谈判项目技术、服务、商务及其他要求

（带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1、采购项目概况

依照国家《计算机信息系统安全保护等级划分准则》、《信息系统安全等级保护基本要求》、《信息系统安全保护等级定级指南》等标准，以及采购人对信息系统等级保护工作的有关规定和要求，对采购人的网络和信息系统进行等级保护。为满足物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个方面基本技术要求进行技术体系建设；为满足安全策略管理制度、安全管理机构和人员、安全建设管理、安全运维管理四个方面基本管理要求进行管理体系建设。采购人通过技术体系建设和管理体系建设，既能满足等级保护的相关要求，又能全方面为采购人的业务系统提供“融合安全、立体防护”的安全保障防御体系，保证信息系统整体的安全保护能力。

3.2、采购内容

3.2.1 标的清单

采购包 1：
采购包预算金额（元）: 3,980,000.00
采购包最高限价（元）: 3,980,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	电视制作边界核心防火墙	1.00	455,500.00	批	工业	是	否	否	否
2	数据库审计系统	1.00	160,000.00	台	工业	否	否	否	否
3	态势感知系统	1.00	380,000.00	套	工业	否	否	否	否
4	威胁分析探针	2.00	360,000.00	套	工业	否	否	否	否
5	漏洞扫描系统	1.00	180,000.00	台	工业	否	否	否	否
6	防病毒系统	1.00	120,000.00	套	工业	否	否	否	否

7	网络管理系统	1.00	250,000.00	套	工业	否	否	否	否
8	服务器安全管理系统	1.00	120,000.00	套	工业	否	否	否	否
9	远程监测服务	1.00	150,000.00	项	工业	否	否	否	否
10	网络安全摆渡系统隔离交换机	1.00	390,000.00	台	工业	否	否	否	否
11	网络安全周边控制设备	1.00	167,500.00	批	工业	否	否	否	否
12	在线多屏编转码平台	2.00	350,000.00	台	工业	否	否	否	否
13	安全管理工作站 1	4.00	120,000.00	台	工业	否	否	否	是
14	安全管理工作站 2	3.00	60,000.00	台	工业	否	否	否	是
15	交换机	2.00	18,000.00	台	工业	否	否	否	否
16	等保评测	3.00	240,000.00	项	软件和信息技术服务业	否	否	否	否
17	安全专家值守及应急处置服务	1.00	300,000.00	项	软件和信息技术服务业	否	否	否	否
18	网络安全能力提升培训服务	1.00	70,000.00	项	软件和信息技术服务业	否	否	否	否
19	系统集成	1.00	89,000.00	项	软件和信息技术服务业	否	否	否	否

3.3、技术参数及要求

采购包 1：

标的名称：电视制作边界核心防火墙

参数性质	序号	技术参数与性能指标
★	1	1、整体性能要求：防火墙吞吐量≥100Gbps，最大并发连接数≥3000万，每秒新建连接数≥100万， IPS吞吐量≥30Gbps，IPSec VPN吞吐量≥40Gbps，SSL VPN吞吐量≥8Gbps，IPSec VPN隧道数≥40000，SSL VPN并发在线用户数≥10000，虚拟防火墙数量≥1000。 2、硬件要求：100G光口≥2个，40G光口≥2个，万兆光口≥20个，配置100G多模万兆光模块≥2个，千兆电口模块≥8个。支持1个独立千兆独立带外管理接口。配置2个交流电源，冗余风扇。支持日志本地存储空间≥1TB SSD。 3、策略管理：支持基于源IP/目的IP，服务类型，应用类型，安全域，时间段等字段进行安全策略规则的配置。支持服务器负载均衡功能。 4、路由功能：支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议，支持SRv6协议；策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级。 5、IPV6：支持IPv6协议栈、IPV6穿越技术、IPV6路由协议；支持IPv6 over IPv4 隧道，6RD隧道。 6、DDoS防护：支持HTTP、HTTPS、DNS、SIP等应用层Flood攻击，支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略。 7、URL过滤：支持URL识别能力和URL地址识别库。 8、入侵防御及病毒防护：系统预定义IPS签名数量≥20000，CVE和CNNVD编号的签名条目数不得少于11000，支持用户自定义签名规则，支持正则表达式。支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护。 9、支持通过telemetry功能，设备通主动向采集器上送设备的接口流量统计、CPU或内存数据等信息。 10、开放RESTCONF，NETCONF等北向接口。 11、供应商所提供的设备如属于《网络关键设备和网络安全专用产品安全认证和安全检查结果》目录中产品，应该由具备资格的机构安全认证合格或者安全检测符合要求，或有效期内的《计算机信息系统安全专用产品销售许可证》复印件。 12、质保要求：五年质保及五年入侵防御、URL过滤、防病毒、应用识别特征库升级服务。
	2	**★一、项目所需设备及技术要求（提供承诺函，格式自拟）** （一）建设目标 1、完善并完成制作系统满足等级保护三级系统建设，同时确保核心业务的安全建设满足评定要求，从而确保成都广播电视台的整体信息化建设符合相关要求并迈向新的台阶。

		2、建立完善的网络安全技术防护体系和安全运维保障。根据信息安全等级保护的要求，建立满足要求的安全技术防护体系，以及后续的网络安全服务和应急技术响应。 3、以成都广播电视台中心机房为核心建设三级安全等保网络体系，实现物理和环境安全的监测和安全防护。 4、制定保障信息管理活动不中断的应急预案。应急预案是安全等级保护的重要组成部分，按可能出现问题的不同情形制定相应的应急措施，在系统出现故障和意外且无法短时间恢复的情况下能确保业务流程持续进行。 （二）安全规划参考以下法律法规和政策标准 1、国家信息安全相关文件： 《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令） 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号） 《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号） 《信息安全等级保护管理办法》（公通字[2007]43 号） 《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861 号） 《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号） 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号） 《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号） 《国家广播电影电视总局令(第 62 号令)》 以及其他相关文件。 2、国家标准： GA/T 1389-2017《信息安全技术网络安全等级保护定级指南》 GB/T 36639-2018《信息安全技术可信计算规范服务器可信支撑平台》 GB/T 36627-2018《信息安全技术网络安全等级保护测试评估技术指南》 GB/T 36635-2018《信息安全技术网络安全监测基本要求与实施指南》 GB/T 36643-2018《信息安全技术网络安全威胁信息格式规范》 GB/T 36958-2018《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 22239-2019《信息安全技术网络安全等级保护基本要求》 GB/T 25070-2019《信息安全技术网络安全等级保护安全设计技术要求》 GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》 GD/J 044-2012《广播电视相关信息系统安全等级保护测评要求》 GD/J 037-2011《广播电视相关信息系统安全等级保护定级指南》

		GD/J 038-2011《广播电视相关信息系统安全等级保护基本要求》 **注：采购文件所引用相关标准文件，如有修订或变更，按最新标准执行。** **★二、其他要求** **1、要求供应商对所投产品电视制作边界核心防火墙、数据库审计系统、态势感知系统、威胁分析探针、漏洞扫描系统、防病毒系统、网络管理系统、服务器安全管理系统、远程监测服务、网络安全摆渡系统隔离交换机、网络安全周边控制设备、安全管理工作站 1、安全管理工作站 2、在线多屏编转码平台、交换机等设备的功能及性能满足招标技术要求。(提供承诺函，格式自拟)** **2、实施要求** 为保证项目按时按质顺利进行，供应商应建立专门的项目管理组，由专人负责。提供详细的项目实施时间表（以天为单位）和各阶段各方人员安排及相关的工作内容；提出完整、合理、可行的项目管理计划，其中包括关于项目进度控制、质量控制、风险控制、文档管理以及与本项目相关的协调工作等的详细描述。 **3、培训要求** 本项目供应商负责对采购人提供技术培训，包括操作人员培训和管理维护人员培训。供应商应提出培训计划，计划包括培训类别、培训项目、人数、时间、地点及培训方式等详细内容，达到使相关人员熟练使用系统的目的。培训前，供应商需编制完成完善的培训材料。 **4、售后服务要求** （1）供应商提供详细的培训计划书； （2）供应商承诺为本项目提供五年整体质保，质保期从项目验收合格开始计算，质保期内每年不少于两次对设备进行现场巡检，出现质量问题，供应商承担维修和更换配件的费用。**（提供承诺函并加盖供应商公章，格式自拟。）** （3）维护响应时间：供应商承诺故障电话响应时间小于 0.5 小时，技术人员在接到通知后 4 小时内到达故障现场，8 小时内完成维修或故障部件更换。**（提供承诺函并加盖供应商公章，格式自拟。）** **★三、商务要求[因平台局限性不能准确表达本项目商务要求，本项目履约过程中涉及的商务要求以此为准，供应商投标时响应本节要求或下列重复要求均可(下列重复要求如:3.4“商务要求”中 3.4.1“交货时间”3.4.4“支付约定”等内容）]** （一）交货时间：合同签订后，90 天内完成供货及安装（采购人可根据项目进展和工作安排，对工期进行适当调整）。 （二）交货地点：采购人指定地点。 （三）付款方式：合同签订且在收到供应商提供的合法有效等额的发票后 5 个工作日内支付合同全款。 **（四）验收标准和方法：** 1、验收组织方式：自行验收。 2、验收主体：采购人。 3、履约验收程序：一次性验收。

		4、履约验收时间：供应商提出验收申请之日起10日内组织验收。 5、技术履约验收内容：按照本项目采购文件中“项目所需设备及技术要求、其他要求”约定执行。 6、商务履约验收内容：按照本项目采购文件中“商务要求”约定执行。 7、验收标准：严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《政府采购需求管理办法》（财库〔2021〕22号）的要求进行验收。 **（五）违约责任** 1、采购人违约责任 （1）采购人无正当理由拒收软硬件、拒付货款的，采购人应向成交供应商偿付拒付货款 5 %的违约金。 （2）采购人未按合同规定的期限向成交供应商支付货款的，每逾期1天采购人向成交供应商偿付欠款额的 1 ‰违约金，但累计违约金总额不超过欠款总额的 5 %。如采购人逾期3个月以上的，成交供应商有权解除合同，由此造成的成交供应商经济损失由采购人承担。 2、成交供应商违约责任 （1）成交供应商所交付的软硬件不符合本合同规定的，采购人有权拒收，同时成交供应商应向采购人支付拒收软硬件部分对应合同金额 10 %的违约金。成交供应商应在得到采购人通知之日起 15 个工作日内采取补救措施。若成交供应商上述期限内所提供的软件仍不符合规定，采购人有权单方面无条件解除合同，但非成交供应商原因导致的情况，成交供应商不承担任何责任。 （2）成交供应商无正当理由未能按本合同规定时间提供软硬件及服务的，每逾期一月向采购人支付合同总金额 2% 的违约金；逾期3个月以上的，采购人有权解除合同，由此造成的采购人经济损失由成交供应商承担。 （3）在成交供应商承诺的或国家规定的质量保证期内（取两者中最长的期限），如经成交供应商 3 次维修，软件仍不能达到合同约定的质量标准、运行效果的，采购人有权要求成交供应商更换为全新合格软件并按本条第（1）款处理，同时，成交供应商还须赔偿采购人因此遭受的损失。 （4）成交供应商保证本合同软件的权利无瑕疵，包括软件所有权及知识产权等权利无瑕疵。如产生了任何的纠纷、索赔或诉讼等，成交供应商除应向采购人返还已收款项中存在权利瑕疵部分对应的合同款项外，还应另按合同总价的 5 %向采购人支付违约金并赔偿因此给采购人造成的一切损失。 3、一方偿付的违约金不足以弥补另一方损失的，还应按另一方损失尚未弥补的部分，支付赔偿金给另一方。 4、双方同意任何一方均不得在本合同期限内及本合同终止后两年内，招聘雇佣任何另一方参与本合同项目实施、咨询、培训及其他服务人员，否则应向另一方支付等同于本合同金额5%的违约金，并赔偿另一方的损失。 （六）包装方式及运输

		1.由供应商负责产品的包装及运输至验收时止。 2.★按照《关于印发<商品包装政府采购需求标准（试行）>、<快递包装政府采购需求标准（试行）>的通知》（财办库〔2020〕123 号）要求，供应商提供的产品包装和快递包装需符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》相关要求。**（提供承诺函并加盖供应商公章，格式自拟。）** ★（七）强制性产品认证 供应商所投产品涉及国家强制认证的（CCC）或前置许可认证的，在投标文件中提供符合国家强制认证（CCC）或前置许可、认证的承诺函件，承诺在供货时一并提供相关许可、认证材料。**（提供承诺函并加盖供应商公章，格式自拟。）** 注意：1、以上内容为本章的实质性要求，不允许有负偏离。 2、本章实质性要求未明确证明材料的，在对应的商务应答表或产品技术参数响应表中应答即可。 3、所有标的涉及的“项目所需设备及技术要求、其他要求、商务要求”等内容，以标的名称：电视制作边界核心防火墙中序号 2“技术参数与性能指标”提到的为准。 4、若谈判文件中其他地方内容存在与 3.3 技术参数及要求内容不一致的，以 3.3 技术参数及要求内容为准。 5、本采购文件所引用相关标准文件，如有修订或变更，按最新标准执行。

标的名称：数据库审计系统

参数性质	序号	技术参数与性能指标
★	1	1、数据库审计系统 SQL 审计处理能力（速率）≥34000SQL/S，≥4TB 磁盘存储空间。标准 2U 机箱，双电源；标配≥6 个千兆自适应电口，1 个 Console 口，支持≥2 个扩展槽位。 2、支持 Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、达梦、人大金仓、南大通用 Gbase。 3、支持内置 SQL 注入、跨站脚本攻击、字段猜测、代码更改等近 500 种风险审计规则库，无需单独配置，直接调用。支持操作语句系列的组合审计规则，可根据某一客体的操作行为序列，连续操作了设定的语句序列时进行规则审计告警。 4、支持白名单管理，根据白名单支持数据库操作命令。 5、同时支持 IPv4 和 IPv6 网络环境下的数据库审计。 6、系统支持评估被保护数据库的整体安全指数； 7、系统支持全库检索、条件检索和关键字检索，快速定位相应的审计会话内容； 8、提供用户界面告警、Syslog 告警、SNMP 告警、邮件告警、短信系

		统、短信猫等多种告警方式； 9、系统内置多种数据类型，可自动检测发现业务环境中数据库对象中包含的数据类型，并进行数据级别的定义。 10、具备《国家信息安全测评信息技术产品安全测评证书》。（提供有效的相关证书复印件或承诺成交后提供该证书）

标的名称：态势感知系统

参数性质	序号	技术参数与性能指标
★	1	1、态势感知平台，含系统软件一套，≥4*GE 管理电口；≥4*USB 接口；1*DB9 Console 接口；冗余电源；≥960G SSD + 12*4TB SATA 存储硬盘。 2、提供远程托管服务平台融合态势感知平台流量，通过云端安全专家团队 7x24 小时持续保障，针对各类威胁事件实时告警监测、深度分析、应急处置完整闭环响应，帮助用户及时感知安全威胁事件，并按周、月出具网络安全态势情况报告。 3、具有威胁感知威胁分析能力，提供从威胁情报比对、应用安全、系统安全和设备安全等业务场景的维度对告警进行攻击带外分析的能力；提供威胁情报维度分析包括但不限于：情报详情、影响资产列表、资产的行为，应用安全的细分维度包括：WEB 安全、数据库安全、中间件安全，系统安全的细分维度包括：暴力破解、弱口令、未授权访问、挖矿行为。 4、提供基于威胁情报的威胁检测能力，检测类型包含 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、其他恶意软件，并可自定义威胁情报； 5、白名单：提供对告警进行加白的能力，加白参数包括受害 IP、攻击 IP、威胁情报、规则、XFF、URL、威胁名称； 支持告警的深度行为分析，行为包括 DNS 解析行为、TCP/UDP 交互行为、WEB 访问行为、传输文件行为；支持以受害资产维度进行分析，分析内容包括失陷状态、受到的攻击类型、威胁级别、处于的攻击阶段、所属的资产分组。 6、支持基于网络请求的语义分析检测，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。 7、告警日志检索溯源能力：提供告警日志检索能力，可基于时间、告警类型、文件 MD5、文件名、文件传输方向、攻击方式、攻击结果、来源/目的所属国、IP 地址、上下行负载等多字段混合搜索。 8、支持与安全终端管理系统，发现威胁事件后支持与安全终端系统控制中心进行指令下发执行终端隔离和扫描操作。 9、终端日志检索溯源能力：提供检索终端 IM 文件传输、邮件附件传输、DNS 访问、 进程、U 盘文件传输等动作的日志，可以及时发现终

		端上存在的异常现象能力，并可结合网络日志及告警日志深挖威胁的攻击全过程； 10、具备大屏展示网络攻击态势能力，大屏展示包括但不限于整体网络风险情况、安全告警总数、攻击次数、攻击 IP 数、受害 IP 资产、攻击态势等，并支持在展示大屏进行分析及溯源取证等工作。 11、所投产品同时支持 IPv4 和 IPv6 网络环境。 12、具备《国家信息安全测评信息技术产品安全测评证书》。（提供有效的相关证书复印件或承诺成交后提供该证书）。

标的名称：威胁分析探针

参数性质	序号	技术参数与性能指标
★	1	1、威胁流量探针两台，网络吞吐≥3G；≥2*GE 流量监听电口；≥2*10GE 流量监听光口（不含光模块）；≥2*GE 管理电口；4*USB 接口；1*DB9 Console 接口；2U 设备；冗余电源；≥4TB SATA 存储硬盘。含系统软件一套； 协议还原能力：提供常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：HTTP、DNS、Smtp、POP3、Imap、Webmail、DB2、Oracle、MySQL、SQL server、Sybase、SMB、FTP、SNMP、Telnet、Nfs 等能力。 2、会话还原能力：提供 TCP/UDP 会话记录、异常流量会话记录、web 访问记录、域名解析、SQL 访问记录、邮件行为、登录情况、文件传输、FTP 控制通道、SSL 加密协商、Telnet 行为、IM 通信等行为描述能力。 3、自定义协议：提供自定义协议和端口，满足特殊场景下的流量抓取。 4、流量过滤：提供流量过滤能力即流量黑、白名单，过滤掉不关注流量或仅接收关注流量。 5、支持基于流量实时 IOC 匹配功能，设备具备主流的 IOC。 6、Webshell 攻击检测能力：提供基于工具特征的 WEBSHELL 检测，实现通过系统调用、系统配置、文件的操作来及时发现威胁；如：中国菜刀、小马上传工具、小马生成器等；提供基于代理程序的攻击检测能力，如 TCP 代理程序、HTTP 代理程序等； 7、支持基于代理程序的攻击检测，如 TCP 代理程序、HTTP 代理程序等。 8、语义分析检测能力：提供基于网络请求的语义分析检测能力，能够将网络请求拆分后从请求头、响应头、请求体、响应体四方面详细展示请求内容，并能提升对未知威胁检测能力。 9、自定义弱口令字典能力：提供支持 HTTP、HTTPS、Telnet、FTP、POP、SMTP、IMAP 等协议的自定义弱口令检测；提供旁路 HTTPS 解密、威胁检测能力。 10、威胁分析探针支持与态势感知平台联动，支持将探针发现的流量发送至态势感知平台进行分析展示。

标的名称：漏洞扫描系统

参数性质	序号	技术参数与性能指标
★	1	1、Web 扫描域名无限制，Web 扫描任务并发数为≥5 个域名。系统扫描 IP 地址最大支持≥1024 个，支持扫描 A 类、B 类、C 类地址。标准 1U 机架式，1T 硬盘，标准配置≥6 个 10/100/1000M 自适应电口，≥4 个千兆光口板卡，≥1 个扩展插槽，2 个 USB 口，1 个 Console 口。 2、具备操作系统、数据库、网络设备等主流系统的漏洞库列表，支持对主流的数据库软件的漏洞检查，支持 Oracle、MySQL、SQL server、DB2 等数据库的安全漏洞检查。 3、支持下发系统扫描、Web 扫描、弱口令扫描任务，扫描目标可以是 IP、域名、URL 的任一格式。 4、支持检测的漏洞数大于 60000 条以上，涵盖漏洞标准包含 CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq6 种，CVSS 覆盖 CVSS2 和 CVSS3 版本。 5、支持 SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP 协议的登录扫描；支持批量导入登录信息、批量登录验证。 6、支持操作系统的配置核查，能够对主流操作系统进行安全配置进行检查，支持 windows、linux、unix 等主流操作系统。 7、支持漏洞数据高级检索及分析，支持按照目标 IP 或 URL、操作系统、MAC 地址、资产评分、漏洞等级、漏洞名称、漏洞类别、漏洞评分、开放端口查看漏洞分布情况，并将检索结果导出。 8、支持 Web 登录扫描，支持 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Session 认证、Digest 认证、SSL，并支持 Web 登陆验证，确保 Web 登录成功。 9、支持至少三种漏洞验证方式如浏览器验证、注入验证、通用验证。 10、支持扫描任务完成后发送告警，告警方式包含邮件告警、短信告警、SNMPtrap 告警、SYSLOG 告警、FTP 告警； 支持 IPv4 和 IPv6 环境的部署和扫描。 11、具备《国家信息安全测评信息技术产品安全测评证书》。（提供有效的相关证书复印件或承诺成交后提供该证书）。 12、在脆弱性扫描能力方面，能够扫描到浏览器漏洞、SMTP/FTP/WEB/DNS/SNMP/RPC 服务的漏洞，能够扫描到 windows 操作系统共享、用户、口令、注册表等漏洞。

标的名称：防病毒系统

参数性质	序号	技术参数与性能指标
★	1	1、配置≥300 点位 Windows 终端的病毒查杀、补丁管理、运维管控的授权，支持 Windows XP/VISTA/WIN7/WIN8/WIN10，包含 3 年升级服务。

		2、控制中心采用 B/S 架构管理端，根据客户端点数的增加支持横向扩展。 3、支持按 CVE 编号查询漏洞，支持按 KB 号查询漏洞，管理员可快速关注高危漏洞，查看漏洞修复情况，如果还有未修复的终端则可立即下发修复任务。 4、管理控制中心当登录账号输入密码错误次数超过锁定阈值后账号将被锁定，同时应支持双因子认证登录方式，提高安全性。 5、客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新。支持设置不同终端类型设置和每批次观察时长。 6、支持终端密码保护功能。 7、支持基于人工智能的安全智能检测引擎，能够有效检测多种类型的恶意软件，通过知名检测机构检测，并且误报率为 0%。 8、病毒防护日志包含：病毒查杀日志、查杀任务日志、攻击防护日志、系统防护日志、按分组、按终端、按时间。 9、支持全部拦截和全屏拦截两种模式，开启弹窗防护功能后自动拦截第三方软件的弹窗。 10、支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录。 11、支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 12、支持对外设进行多维度的放行，包括设备名称、PID/VID、实例路径，通过添加实现例外或加黑。 13、供应商所提供的设备如属于《网络关键设备和网络安全专用产品安全认证和安全检查结果》目录中产品，应该由具备资格的机构安全认证合格或者安全检测符合要求，或有效期内的《计算机信息系统安全专用产品销售许可证》复印件。

标的名称：网络管理系统

参数性质	序号	技术参数与性能指标
★	1	1、管理规模要求：系统应支持大规模设备管理能力，可最多管理 20,000 台网元。 2、管理范围要求：系统应支持多种设备的管理，包括交换机、路由器、防火墙、WLAN、服务器、存储、操作系统、数据库、WEB 应用、摄像头、GPON 设备、微波、超融合、虚拟化、CPE 终端。 3、系统开放性要求：系统提供三种北向接口（SNMP、FTP 及 Restful 接口），可通过北向接口向上层系统提供告警、性能以及资源数据。 系统提供多种远程消息发送能力（短信网关、企业微信、钉钉、短信猫或邮箱服务器）。系统应支持多种南向接口类型，包括 SNMP、STelnet、FTP、SFTP、IPMI、HTTP/HTTPS（REST/Redfish 客户端、服务端）、LwM2M、

		WebSocket、SocketPing、ICMP、WebPing、WebTrace、SSDP 接口，方便管理多种设备类型。 4、拓扑管理要求：支持过滤显示拓扑视图、查看全景图等功能，用户可以及时监控所关注的拓扑节点状态和了解拓扑视图全貌。支持用户在拓扑视图上添加图形、文本和容器等对拓扑对象进行可视化的组织、标记和描述，以方便运维管理。支持刷新、导出拓扑视图，用户可以获取拓扑对象的最新状态，并查找和二次编辑拓扑对象，实现拓扑变化情况可视化管理。 5、故障管理要求：提供多领域、多厂商数据采集能力，包括从下层第三方系统采集网元的告警信息，并将告警集中显示在告警面板中。支持多样化的告警过滤方式，帮助运维人员快速筛选所关注的告警，提高监控效率。支持灵活的告警规则配置，将海量的告警进行关联和压缩，减少告警噪声，实现精准监控。提供紧急、严重、次要、提示四个等级来表达告警的紧急程度，帮助运维人员快速识别告警的重要程度，以采取相应的处理策略。 6、性能管理要求：支持对设备的关键性能指标进行监控，并对采集到的性能数据进行统计，方便用户对设备性能进行管理。支持通过设置不同的性能阈值，生成 4 级不同级别的告警：紧急、重要、次要、提示。支持查看指定设备、指定指标的历史性能数据，以了解设备历史性能趋势。支持监控设备的实时性能数据，了解设备的运行状态，以便确认设备是否存在异常，支持将查询结果导出到 excel 文件。 7、报表管理要求：支持用户拖拽式自定义报表内容，运用钻取、旋转、切片等操作，实现业务数据的灵活展现和统计汇总，提供自助式数据同比、环比、TOPN 等分析功能。支持根据用户设定的周期自动生成报表，可以通过 Email 发送，也可以手动导出 Excel、PDF 格式的报表。 8、网络管理能力要求：至少支持 Cisco、Huawei、H3C、锐捷等厂商的设备管理。要求具备自定义设备的管理能力（至少包括告警参数、性能指标），从而达到对新设备快速管理。支持对设备配置文件管理、设备软件升级、网络质量检查、流量分析功能和 IP 地址管理功能。 9、服务器管理能力要求：支持对服务器名称、IP 地址、在线状态、健康状态、类型、型号、描述、信息刷新时间等基本信息以及电源、风扇、CPU、内存、硬盘、主板、交换板等部件信息进行管理。支持服务器状态监控、性能监控。 10、支持 WLAN 管理支持对接主流规划工具，可快速导入网规数据，仿真楼栋、楼层、障碍物规划，实现信号覆盖可视。支持 WIDS 管理，探测无线网络中的非法设备/客户端、干扰源和攻击，并通过告警通知运维人员。 11、支持存储管理。持存储设备管理的基本信息、性能信息、告警信息、硬盘域/存储池/LUN/文件系统等容量信息，以及控制器/端口等硬件信息的监控。 12、支持视频监控管理。支持以拓扑形式展示域、集群、CloudIVS 和 VCN 的组网结构，能够统一监控视频设备全网的负载情况，保证视频业务稳定运行。 13、本次配置要求：配置网络设备管理许可≥100 个，服务器管理许可

		≥50 个。配置配套的国产化操作系统及数据库。 14、售后服务：提供对应三年软件升级服务。

标的名称：服务器安全管理系统

参数性质	序号	技术参数与性能指标
★	1	1、服务器安全管理具有统一控制端对全网服务器统一集中管理、策略下发、数据分析等； 2、系统具有良好兼容性，支持 windows/linux 主流操作系统及国产化操作系统，包括但不限于以下的操作系统：Windows Server；RedHat；CentOS；Ubuntu；Suse；麒麟、红旗等； 3、配置≥20 个服务器安全加固系统客户端授权； 4、支持自我防护技术，即使客户端被意外关闭，防护依然有效； 5、支持以列表的形式，统一列出 Windows/Linux 服务器基础信息，并在列表中对服务器的关键软硬件进行统计，包括但不限于：CPU 数、CPU 核数、分区数、账户数、软件应用数、web 站点数、web 服务数、web 框架数、数据库数、端口数、网络连接数、启动服务数、安装包数、计划任务数、环境变量数、内核模块数、证书数、注册表数、类库数等。 6、支持与态势感知系统联动，能够将威胁告警发送至态势感知系统进行联动分析，进行告警归并统一展示。 7、服务器安全加固产品支持与态势感知系统联动，支持将服务器告警流量发送给态势感知系统。 8、支持全量资产的关键字及语法搜索，支持检索的语法包括但不限于：服务器资产类、进程资产类、账号资产类、软件应用类、web 资产类、web 服务类、web 框架、数据库类、端口资产类、网络连接类、启动服务类、安装包类、计划任务类、环境变量类、内核类、类库资产类、注册表类、证书资产类进行检索。 9、支持通过自动、手动的任务设置，对局域网内服务器的服务器进行扫描，并自动获取服务器相关信息，包括 MAC 地址、设备类型、未知主机 IP、操作系统、发现方式、首次发现时间等信息。 10、支持通过检测主机 Web 目录下的文件内容，发现 Web 网站中存在的后门文件。 11、支持服务器防火墙功能，可对服务器定制访问策略，支持设置端口的暴露控制规则，支持对服务器的进程外连控制进行规则设置。 12、支持对服务器中复用的相同密码进行检测，可识别出某个密码被哪些服务器、哪个账户、在什么操作系统上进行了复用；支持域控弱口令扫描检测。 13、支持在事件列表的详情中，查看事件的基础信息、检测说明、动态攻击路径信息、资产等信息，并可在详情中以前后翻页的形式连续查看事件；支持对威胁进行日志调查，包括：攻击者 IP、受害者 IP、

		进程主体等，并可自动跳转至日志分析界面进行调查。 14、支持提供文件监控与防护功能，且支持防护模式和监控模式进行切换，需支持指定受保护路径以及例外路径的设置；支持对保护路径内的文件提供文件的读取、写入、重命名、链接、删除、执行、创建等权限控制功能，支持对保护路径内提供例外进程功能。 15、支持提供对 Windows、Linux 操作系统安全加固功能， 支持对 Agent 进行统一管理，包括：Agent 降级，Agent 暂停，Agent 异常重启，Agent 安装的版本、可升级的版本占比情况进行统计，并可对 Agent 版本进行更新和同步，Agent 性能保护。 16、供应商所提供的设备如属于《网络关键设备和网络安全专用产品安全认证和安全检查结果》目录中产品，应该由具备资格的机构安全认证合格或者安全检测符合要求，或有效期内的《计算机信息系统安全专用产品销售许可证》复印件。

标的名称：远程监测服务

参数性质	序号	技术参数与性能指标
★	1	1、提供对威胁感知系统的 7*24 小时远程实时监测，远程托管平台和威胁感知系统实现对接。 2 安全事件通告：服务人员对安全监测发现的安全隐患及事件在服务规定时间内进行通告，同时根据客户需求每日同步安全情况。 3、威胁抑制/阻断：建立工作群，实时推送封禁信息，包括高频攻击源、恶意软件 IOC、内外交互的恶意链接等，可通过安全运营平台对上述情况进行联动封禁，阻止进一步攻击。 4、托管中心平台支持查看客户所受攻击中攻击者地区分布情况，并对外部攻击、横向攻击和外联攻击攻击成功情况和受攻击 IP 失陷数量进行统计展示。 5、平台支持面向客户的安全报告与交付物管理，可导出、下载各类安全报告，包括事件分析报告、周报、月报、应急响应报告等，使得客户能直观查看服务成果。 6、支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等。 7、平台支持查看所有经云端分析专家研判后推送的安全事件工单，呈现该安全事件工单对应的告警详情、研判结论、处置建议及工单流程信息，使安全事件分析处置流程透明化，可跟踪溯源。 8、平台支持对客户资产信息统计展示，包括总资产、重点资产的资产数量变化以及各资产组的资产情况；平台支持对重点监测资产存在风险及修复状态统计展示。 9、支持对具体资产点击跳转至告警页面，查看以该资产 IP 为受害 IP 的告警信息。

		10、托管中心平台要求支持对客户资产信息统计展示，包括总资产、重点资产的资产数量变化以及各资产组的资产情况；平台支持对重点监测资产存在风险及修复状态统计展示。 11、支持对客户资产信息进行录入管理，支持资产的添加、删除、编辑和检索查看，对资产信息的导入和导出操作；支持对资产打标签，且通过标签进行过滤。

标的名称：网络安全摆渡系统隔离交换机

参数性质	序号	技术参数与性能指标
★	1	1、支持高带宽点对点互连；支持在信号传输速率为 8GHz 时，I/O 带宽最高可扩展至 64Gbps。 2、支持满足系统要求的可扩展带宽；支持来自 1-32 PCI Express 通道的多个互连带宽。 3、支持电源管理、热交换、热插拔、数据完整性、高级错误记录和报告、QoS。 4、支持任意 4 点网络安全隔离设备间的文件交换。 2、端口链路速度≥64 Gb/s 。 3、应用系统性能≥6000 MB/s。 4、端口时延≤200ns。 5、PCIE 接口数量≥8。 6、连接线支持 x8 iPass PCI-E 连接线。 7、支持兼容 FST 接口。 8、供应商所提供的设备如属于《网络关键设备和网络安全专用产品安全认证和安全检查结果》目录中产品，应该由具备资格的机构安全认证合格或者安全检测符合要求，或有效期内的《计算机信息系统安全专用产品销售许可证》复印件。

标的名称：网络安全周边控制设备

参数性质	序号	技术参数与性能指标
★	1	1、数字调音台；数量：5 台；通道配置≥9 个；输入混音通道：≥16 个单声道，≥1 个立体声，≥2 个 FX 返送；总线：≥1 个立体声，≥6 个混音，≥2 个 FX，≥2 个矩阵（支持输入到矩阵）。本地 I/O：≥16 个麦克风/线路，≥8 个（XLR）输出；USB：≥18 个输入，≥18 个输出。 2、录音话筒；数量：10 套；生成元件：动圈 N / Dym 磁铁结构；频率响应：(kick 曲线） ≥ 30 Hz - 18000 Hz ；（一般曲线）≥45 Hz - 18000 Hz ；指向性模式：心形；阻抗：150 欧姆平衡；阻抗：≥150

		欧姆平衡； 3、耳机；数量：10 套；功能用途：HiFi 耳机，监听耳机，手机耳机，音乐耳机；连接方式：3.5mm 镀金插头；佩戴方式：头戴式；发声原理：动圈；驱动单元：≥30mm；频响范围≥16-28000Hz；产品阻抗 ≥55 欧姆；灵敏度≥91dB；最大功率 ≥200mW； 4、音箱；数量：10 套；频率响应：≥54Hz－30kHz；功率：双功放系统，LF≥45W，HF≥25W，高性能≥70W；输入接口：XLR 和 TRS phone 型输入口，可接受平衡和非平衡信号。 5、ODA 光盘数据存储介质；数量：20 张；存储容量≥5.5TB；支持一次性写入；100 万次以上读取次数，100 年常温保存期限。

标的名称：在线多屏编转码平台

参数性质	序号	技术参数与性能指标
★	1	1、平台配置：CPU≥2 颗，缓存不低于 64G 内存，配置双电源，不低于 6 个 GBE 端口，暂存空间不低于 200G 企业级 SSD。 2、模块配置：在线多屏编转码平台操作系统，多格式协议及采集接入模块，多格式视频解码模块，多格式音频解码模块，多格式协议及接口输出模块，多格式视频编码模块，多格式音频编码模块，一进多出编转码任务模块，播放预览模块，内容编辑模块，HDR 处理模块，图文包装模块，直播控制模块，收录模块，网络管理与负载均衡模块，用户权限管理模块，日志告警管理模块，时间时区管理模块，任务控制模块，预设管理模块，素材管理模块，信号主备垫切换模块。 3、编转码处理器具有 Icelake 架构及以上架构的处理能力； 4、具有 IPv6 协议进行通信和数据传输，并可以在网管界面上配置。 5、不低于 8 路 SDI 全高清 25 帧 H.264 编转码能力或 4 路全高清 25 帧 H.265 编转码能力或 1 路 4K 25 帧 H.265 编转码能力； 6、输入信源协议需要支持 TS Over UDP、TS Over HTTP、FLV Over HTTP、Apple HLS、Adobe RTMP、RTSP、RTP、ZIXI。 7、输入信源协议需要支持 SRT，支持 Caller、Listener、Rendevzous 三种模式数据接收以及 AES 解密，并支持端口模式和流 Streamid 模式接收 SRT 信源，以满足当前主流传输场景协议需求。 8、支持高清解析度的 AVS+组播信源接入（提供 AVS+高清解码器入网证证明）。 9、支持带 5.1 或 7.1 声道的 Dolby AC-3 或 Dolby E-AC-3 音频的输入文件转码。 10、支持单转码任务内双路信号的备份输入，并能自动切换；主备信号支持从不同的网口接收，在主/备路信号问题时可以在主备信号间自动倒换；主备信号可以支持不同编码格式和不同协议的异构信源。 11、当主信源质量好于备信源时，支持优先使用主信源的机制，若主信源故障切至备信源，一旦主信源恢复，则自动切回主信源，确保最

		优质量生产。 12、支持 TS Over UDP 方式的单播及组播流输出，支持 IGMP v3 协议，IGMP v3 协议输出源地址和 TTL 可配置。 13、支持 1 进多出多屏分发，支持不同编码格式及不同协议的流同时输出。 14、针对事件性直播的 HLS 输出，支持在直播时对 HLS 切片进行保存并重新构建所有切片的索引，当直播结束后可以将保存的切片和索引作为点播素材使用，缩短点播内容上线时间（提供第三方检测机构的检测报告复印件加盖供应商公章或提供承诺函，承诺成交后提供）。 15、支持 H.265 视频编码格式，支持 Profile 包括 Main、Main10，位深包括 8bit、10bit。 16、支持 RAW 视频格式输出，支持对输出视频帧率、分辨率、帧场模式、采样和 HDR 的设置。 17、支持国产化 HDR Vivid 标准，支持高光模式（三通道、单通道、原始通道）、整体亮度、中灰亮度的参数设置。 18、支持单声道、立体声、5.1 和 7.1 声道等编码模式。 19、支持 PQ 曲线输入，Dolby Vision Profile 5 或者 Dolby Vision Profile 8.1 输出（提供国家认可的第三方检测机构的检测报告复印件加盖供应商公章或提供承诺函，承诺成交后提供） 20、支持网管系统统一配置功能，即所有任务可以在网管系统中进行统一配置，包括但不限于创建、删除、复制任务模板、编码模板和图文模板等。 21、网管系统支持邮件报警及语音告警，可在网管系统界面上直接进行邮件相关参数的配置与有效性测试。 22、要求设备兼容市场上主流在线多屏编转码平台和智能收录平台，具备统一管理平台集群转码调度与热备份。**（提供承诺函，格式自拟）**

标的名称：安全管理工作站 1

参数性质	序号	技术参数与性能指标
★	1	1、支持 CPU 颗数：≥2 颗；CPU 内核≥12 核；CPU 频率≥2.1G； 2、内存容量：≥128GB；硬盘转速：7200rpm；硬盘容量：≥8TB；硬盘类型：SATA 企业级； 3、采集卡≥1 张；SDI 视频输入及输出：支持 4 路双向 12bit SD/HD 可独立配置输入或输出接口；SDI 音频输入及输出：支持 16 通道嵌入 SD 和 HD；同步输入：支持三电平或黑场；支持各类 SD 和 HD 的 SDI 格式，最高支持 1080P60。 4、超高清网络非线性编辑系统：超高清上下载软件模块、超高清文件介质上下载软件模块、超高清字幕编辑软件模块、超高清实时上下变换软件模块、超高清专业图像特技软件模块、超高清专业字幕特技软件模块、超高清节目审查软件模块。

		5、支持 VR 编辑，支持创建 VR360°、VR180° 工程，支持 VR 虚拟图文/视频植入；支持植入 VR 字幕、图文或视频，支持可调节植入对象的透视角度和透明度等。

标的名称：安全管理工作站 2

参数性质	序号	技术参数与性能指标
★	1	1、CPU 内核≥16 核； CPU 频率≥2.1G； 显存≥4GB；硬盘容量≥2TB； 2、内存容量≥16GB； 3、硬盘转速≥7200rpm； 4、采集卡≥1 张；SDI 视频输入及输出：支持 4 路双向 12bit SD/HD 可独立配置输入或输出接口；SDI 音频输入及输出：支持 16 通道嵌入 SD 和 HD；同步输入：支持三电平或黑场；支持各类 SD 和 HD 的 SDI 格式，最高支持 1080P60； 5、高清多通道直导播软件；视频文件播放：支持所有流行格式，包括 AVI、MP4、H264、MPEG-2、WMV、MOV 和 MXF；音频文件播放：支持 MP3 和 WAV。音频设备支持：混合多个音频源，例如声卡、ASIO 音频接口和采集卡音频。 高清流媒体编码输出；支持通过 AJA、Blackmagic 和 Bluefish 卡输出到专业录音卡座和监视器；在普通 PC 上进行专业高清制作；以全高清格式实时录制到 AVI、MP4、MPEG-2 或 WMV；内置具有高质量实时色度键的高清虚拟场景；内置音频混音器；实时视频效果；不同的“多视图”预设将多个输入组合为图层，或使用可用的缩放、平移、旋转和裁剪控件自定义每个元素的位置。兼容 NDI 设备发送和接收 NDI 源。

标的名称：交换机

参数性质	序号	技术参数与性能指标
★	1	1、交换容量≥520Gbps，包转发率≥170Mpps，若官网有 A/B 值以最小值为准； 2、24 个 10/100/1000Base-T 以太网端口，4 个万兆 SFP+；支持专用堆叠口，不占用业务口带宽，堆叠带宽（双向）≥ 40Gbps 3、支持 MAC 表项≥32K，支持 IPv4 路由表≥4K，支持 IPv6 路由表≥1K。 4、CPU 和 LSW 要求国产化，推动自主可控。（提供第三方检测机构的

		检测报告复印件加盖供应商公章或提供承诺函，承诺成交后提供） 5、支持防 ARP 攻击、DOS 攻击、ICMP 防攻击、CPU 保护。 6、支持 Telemetry 技术。 注：本次采购的交换机为接入交换机，交换容量<30Tbps，包转发率<10Gpps。

标的名称：等保评测

参数性质	序号	技术参数与性能指标
★	1	1、3 个系统二级等保测评服务； 2、按照网络安全等级保护测评依据《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》、开展测评工作（至少包括以下项目）： （1）安全物理环境测评：物理位置的选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应、电磁防护。 （2）安全通信网络测评：包含网络架构、通信传输、可信验证。 （3）安全区域边界：边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证。 （4）安全计算环境测评：身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。 （5）安全管理中心测评：系统管理、审计管理、安全管理、集中管控。 （6）安全管理制度测评：安全策略、管理制度、制定与发布、审批和修订。 （7）安全管理机构测评：岗位设置、人员配备、授权和审批、沟通和合作、审核和检查。 （8）安全管理人员测评：人员录用、人员离岗、安全意识教育和培训、外部人员访问管理。 （9）安全建设管理测评：安全建设管理测评应当包含：定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择。 （10）安全运维管理测评：环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理。 3、测评服务允许分包（参与测评服务的企业须具备经“公安部第三研究所”认证颁发的《网络安全等级测评与检测评估机构服务认证证书》）。

标的名称：安全专家值守及应急处置服务

参数性质	序号	技术参数与性能指标
★	1	1、服务期限。安全专家服务按人天（每人天指单人服务不低于 8 小时）计算，自合同签订之日起一年内，采购人按实际需要要求安全专家到场服务，总人天不低于 60 天。 2、服务内容 （1）安全值守，在全国两会等重要保障期内，按采购人要求，到现场协助完成网络安全值守及保障工作，并出具值守报告。 （2）应急处置，在发生疑似或确定网络安全事件时，按采购人要求，到现场协助进行风险阻止、事件判断、追踪溯源、系统修复等工作，并出具应急处置报告。 （3）应急演练，协助采购人完成每年不少于两次的应急演练（至少一次为实际操作），应急演练方案由采购人与安全专家共同编制，采购人审核通过后执行，应急演练模拟环境由安全专家负责搭建，所需软硬件设备由采购人提供；应急演练结束后，出具应急演练总结材料。 3、服务要求 （1）提供安全值守、应急处置、应急演练等安全服务。 （2）提供安全值守、应急处置、应急演练等安全服务。 （3）网络安全专家必须严格遵守采购人网络安全、保密相关规定，其背景审查由网络安全服务供应商负责。 （4）对确定或疑似网络安全事件，网络安全服务供应商接到采购人应急处置要求后，必须在规定的时间内指派人员到达现场，一般网络安全事件不超过 4 小时，较大网络安全事件不超过 2 小时，较大网络安全事件不超过 1 小时，特别重大网络安全事件不超过 30 分钟。 （5）网络安全专家执行完相应工作后，必须在规定时间内出具相应的过程报告及结论报告。

标的名称：网络安全能力提升培训服务

参数性质	序号	技术参数与性能指标
★	1	1、服务期限。自合同签订之日起一年，采购人根据实际工作安排，组织人员参与培训。 2、服务内容 （1）网络安全意识培训，培训师资及内容由网络安全服务供应商提供，采购人审核通过后执行，培训场地、人员由采购人组织，培训针对采购人全体在职员工，培训课时不低于 4 课时。 （2）网络安全岗位技术人员资质培训，网络安全服务供应商提供不少于 7 人次 CISP（注册信息安全专业人员）培训。

		（3）网络安全岗位技术人员技能提升培训，网络安全服务供应商提供不少于 4 次培训，培训师资及内容由网络安全服务供应商提供，采购人审核通过后执行，培训场地、人员由采购人组织，培训结束后由采购人、网络安全服务供应商共同组织笔试或机试考试。

标的名称：系统集成

参数性质	序号	技术参数与性能指标
★	1	1、电视制作边界核心防火墙系统、数据库审计系统、态势感知系统、威胁分析探针、漏洞扫描系统、防病毒系统、网络安全摆渡系统隔离交换机、网络安全周边控制设备、在线多屏编转码平台等网络安全系统搭建服务； 2、提供网络管理系统、服务器安全管理系统、超高清网络非线性编辑系统、高清多通道直导播软件等软件部署服务； 3、提供网络安全系统各系统的培训服务； 4、六类网线 20 箱、5 米 LC 光纤跳线 200 对、六类水晶头 20 盒等耗材一批； 5、高朋办公区机房内 30 组机柜及 9 个弱电间、1 个综合配线间、双林办公区内 2 个网络机房的废旧网线、设备、光纤线清理与桥架清理。清理过程中必须依据《广播电视安全播出管理规定》（2021 年修订版全文）国家广播电影电视总局令第 62 号的相关内容严格执行，作为集成商一并负有相同法律责任。高朋办公区废旧设备清理、废旧机柜的拆除至地下室负二层，双林办公区废旧设备清理至综合楼二楼杂物间，并共同完成资产搬迁清点工作； 6、高朋办公网络改造。改造内容如下：将旧办公网络设备与新建办公网络设备重新进行网络规划、改造，实现统一管理；优化现有 WLAN 网络。网络改造所产生的设备采购、综合布线等材料包含在本次报价里面。 7、提供一套支持成都市广播电视台版权中心的确权平台，平台软件源代码、软件所有权和著作权全部属于成都市广播电视台。该平台要求能够实现统一认证，实现免密码登录，获得相应用户权限。登录成功后，能将成都市广播电视台媒资系统内的基础编目信息（媒资 ID、视音频作品内容、作品名称、首次发表日期、作者、封面）提取出来。确权平台上完成作品类型、作品类型说明、作品创造性质、作品归宿、作品完成时间、创作完成地点、发表地点、获得权利方式、著作权人、权利拥有方式、作品创作说明、作品创意、创作经过、权利保证书、证明材料的信息手动填报。自动汇总基础编目信息和手动填报消息后，发送至“斑马中国”相应开放接口完成版权登记“一站式”上传工作。确保所发送信息链路安全、数据安全、网络安全。

3.4、商务要求

3.4.1 交货时间

采购包 1：
自合同签订之日起 90 日

3.4.2 交货地点和方式

采购包 1：
见“3.3 技术参数及要求”

3.4.3 支付方式

采购包 1：
一次付清

3.4.4 支付约定

采购包 1： 付款条件说明： 合同签订且在收到供应商提供的合法有效等额的发票后 ，达到付款条件起 5 日内，支付合同总金额的 100.00%。

3.4.5 验收标准和方法

采购包 1：
见“3.3 技术参数及要求”

3.4.6 包装方式及运输

采购包 1：
见“3.3 技术参数及要求”

3.4.7 质量保修范围和保修期

采购包 1：
见“3.3 技术参数及要求”

3.4.8 违约责任及解决争议的方法

采购包 1：

见“3.3 技术参数及要求”

3.5 其他要求

采购包 1：

见“3.3 技术参数及要求”