第一节 采购清单一览表

序号	分项项目名称	服务内容	数量	单位
1	**业务中台成品软件**			
1.1	业务中台	运维管理平台	1	项
1.2		无人机管理平台	1	项
1.3		融合通信平台	1	项
1.4		视频整合平台	1	项
1.5		设备管理平台	1	项
2	**云服务平台（公有云）成品软件**			
2.1	**云服务平台软件（公有云）**		1	套
3	**云服务平台（专有云）成品软件**			
3.1	**云服务平台软件（专有云）**		1	套
4	**公有云硬件**			
4.1	网络设备	核心交换机	2	台
4.2		业务网交换机	13	台
4.3		千兆电口管理交换机	6	台
4.4		云平台核心交换机	2	台
4.5		外网接入路由器	2	台
4.6		**统一授时服务器**	1	台
4.7	存储设备	分布式存储设备	3	台
5	**专有云硬件**			
5.1	网络设备	参数网 ROCE 交换机	6	台
5.2		业务网交换机	26	台
5.3		云平台核心交换机	2	台
5.4		千兆电口管理交换机	8	台
5.5		核心交换机	2	台
5.6	存储设备	大数据存储服务器	4	台
5.7		分布式块存储	6	台
5.8		分布式对象存储	18	台
5.9	备份设备	备份存储	4	台

6	**公有云安全和密码设备**			
6.1	安全设备	边界区防火墙	2	台
6.2		数据安全交换系统	1	套
6.3		安全运维管理区/办公区防火墙	2	台
6.4		Web 应用防火墙	2	台
6.5		抗 DDoS	2	台
6.6		入侵防御	2	台
6.7		核心交换区流量探针	1	台
6.8		运维区/终端区流量探针	2	台
6.9		网络审计	1	台
6.10		国密堡垒机	1	台
6.11		网络准入	1	台
6.12		数据防泄漏系统	1	台
6.13		VPN 综合安全网关	2	台
6.14		核心交换区边界防火墙	2	台
6.15		云安全管理平台	1	套
6.16		漏洞扫描	1	套
6.17		日志审计	1	套
6.18		堡垒机	1	套
6.19		数据库审计	1	套
6.20		主机安全防护	1	套
6.21		Web 应用防火墙	1	套
6.22		流量探针	1	套
6.23		态势感知平台	1	套
6.24	密码设备	服务器密码机	2	台
6.25		时间戳服务器	1	台
6.26		签名验签系统	1	台
6.27		协同签名系统	1	台
6.28		安全认证网关	1	台
7	**专有云安全和密码设备**			
7.1	安全设备	边界区防火墙	2	台

7.2		数据安全交换系统	1	套
7.3		安全运维管理区/终端区防火墙	2	台
7.4		核心交换区流量探针	1	台
7.5		安全运维管理区/终端区流量探针	2	台
7.6		网络审计	1	台
7.7		国密堡垒机	1	台
7.8		网络准入	1	台
7.9		数据防泄漏系统	1	台
7.10		核心交换区边界防火墙	2	台
7.11		零信任访问控制系统	1	套
7.12		情报板安全管理平台	1	套
7.13		安全可视化管理平台	1	套
7.14		安全智能分析系统	1	套
7.15		云安全管理平台	1	套
7.16		漏洞扫描	1	套
7.17		日志审计	3	套
7.18		堡垒机	3	套
7.19		数据库审计	3	套
7.20		主机安全防护	1	套
7.21		Web 应用防火墙	1	套
7.22		流量探针	1	套
7.23		态势感知平台	1	套
7.24		云数据库审计（部署在政务云）	7	套
7.25		云日志审计（部署在政务云）	7	套
7.26		流量探针（部署在政务云）	7	套
7.27	密码设备	服务器密码机	2	台
7.28		密码服务管理平台	1	套
7.29		时间戳服务器	1	台
7.30		签名验签系统	1	台
7.31		协同签名系统	1	台
7.32		国密设备证书	160	套

7.33		安全认证网关	1	台
7.34		国密 SSL 证书	2	个
7.35		国密浏览器	400	套
7.36		个人数字证书	3400	个
7.37	数据安全	数据分级分类平台	1	套
7.38		数据脱敏系统	1	套
7.39		数据库安全网关	1	套
7.40		API 安全审计系统	1	套
7.41		数据安全管理平台	1	套
7.42		API 安全网关	1	套
8	**机房及通信链路租赁**			
8.1	机柜租赁	8kW 机柜	54	个
8.2		12kW 机柜	15	个
8.3	通信链路租赁	政务外网带宽 300Mbps（不计取租赁费）	1	项
8.4		互联网带宽 3Gbps	1	项
8.5		专网带宽 2.5Gbps	1	项
9	**集成费**			
9.1	软、硬件集成	集成费	1	项

第二节 技术要求

一、项目基本情况

1.项目编号：政府采购编号：豫财招标采购-2025-1641

2.项目名称：河南省智慧交通服务云平台项目—省政务云交通专有域成品软硬件和系统集成

3.建设工期：建设工期总时间不超过 6 个月

4.预算金额：64212300 元，最高限价：64212300 元，分项汇总限价表如下：

序号	名称及类别	预算金额（万元）
（一）	成品软件购置费（政务云交通专有域）	1749.86
1	业务中台	788.86
1.1	运维管理平台	90.00
1.2	无人机管理平台	175.00
1.3	融合通信平台	108.86

序号	名称及类别	预算金额（万元）
1.4	视频整合平台	165.00
1.5	设备管理平台	250.00
2	云服务平台软件	931.00
3	安全软件	30.00
（二）	成品硬件购置费（政务云交通专有域）	3500.2
1	云平台硬件	1730.80
2	安全和密码设备	1769.40
（三）	机房及通信链路租赁	729.90
（四）	集成费	441.27
合计		6421.23

注：（1）本包包含集采部分集成费

（2）投标人应按本采购需求中的《项目采购清单一览表》逐项进行报价，且相应分项汇总金额不得超过上表中的分项汇总限价金额，否则视为无效投标。

5.项目软硬件运维期：自项目竣工验收合格之日起开始计算，成品软硬件免费运维三年；其他免费运维一年。针对本项目提供 7*24 免费售后技术支持服务（包括但不限于版本升级、漏洞修复、故障排除、性能调优、技术咨询等）。

6.采购内容：（1）业务中台成品软件，包括运维管理平台、无人机管理平台、融合通信平台、视频整合平台和设备管理平台。（2）云服务平台软件，包括云服务平台软件（专有云）和云服务平台软件（公有云）。（3）安全软件。（4）云平台硬件包括公有云硬件和专有云硬件。公有云硬件包括网络设备、存储设备。专有云硬件包括网络设备、存储设备、备份设备。（5）安全和密码设备包括公有云的安全和密码设备、专有云的网络安全、密码和数据安全设备。（6）机房及通信链路租赁。（7）对成品软件、云平台硬件、安全和密码设备等内容进行集成。负责在采购人指定地点开发、调试软件，负责相关软硬件购置及安装集成、系统部署及推广应用，并负责培训采购人（含相关用户单位）人员，使所建设的硬件和所部署软件得以正常运行，满足采购人（含相关用户单位）的需要。

二、建设要求

（一）基本要求

1.中标人承担河南省“一轴一廊”交通基础设施数字化转型升级示范通道及网络项目中河南省智慧交通服务云平台项目建设，具体内容包括但不限于：中标人应当完成项目需求调研与确认、软件开发与实施（概要设计、详细设计及编码）、软硬件购置、接口开发、数据资源建设、试运行、培训、

部署及推广应用、验收、升级与售后服务等，使经双方确认的软件和硬件均满足采购人（含相关用户单位）的需要，并正常运行。同时，中标人作为项目总包方，须为所有参与项目的团队提供统一的协同办公服务（例如许可数充足的飞书等平台），确保各项目组信息同步、高效协作。

2.因本项目涉及多家用户单位，中标人应加强与采购人以及各相关用户单位的汇报、沟通、对接，确保项目建成后符合本项目招标文件中技术规格书、报交通运输部备案的《河南省“一轴一廊”交通基础设施数字化转型升级示范通道及网络实施方案》以及经河南省发展和改革委员会批复的《河南省智慧交通服务云平台项目初步设计和投资概算》等全部要求，并应符合交通运输部、河南省相关技术标准、规范及文件要求，最终确保满足交通运输部组织的绩效评价考核各项考评指标要求。

3.中标人应按照采购人制订的数据及业务整合相关标准、规范及要求开展项目建设。

4.中标人采购、开发软件必须遵守国家《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《信息安全技术个人信息安全规范》等有关的法律法规，不得造成采购人因使用该软件出现数据合规风险和承担法律责任。

5.中标人须无条件补足云平台部署所需要的相关资源，包括但不限于服务器硬盘等。

6.本项目为“交钥匙”工程，包括设备采购、运输、安装、集成、测试、试运行、交工验收和竣工验收全过程。投标人投标报价应包含所有费用，包括投标内容深化设计费、设备采购费、运输费、人工费、机械费、制作安装实施费、综合布线所需的光纤、网线及相关辅材费、保险费（含设备、人员等）、成品保护费、材料检测费、材料清场费、测试及试运行费、各类验收费、培训费、质保期内工程产品包换/质量保修/现场组织和协调费、税费、利润、项目措施费、安全文明措施费等工程建设中所需要的一切费用，投标人漏报或不报，招标人将视有关费用包括在工程量清单的其他单价及合价中而不予支付；

投标人应充分理解本次项目建设内容，除额外说明的条目外，本包工程量清单中未明示的、与完成本工程相关的必不可少的材料，包括但不限于实现设备联接所需的光纤、网线及配套辅材等，以及完成本工程所需的相关辅助工作，应视为包含在相关清单条目中。投标人应该根据建设内容进行计算，并作预算报价，施工过程中不予认定；

项目实施全过程中，在招标文件中未明示但因项目需要必不可少的建设内容，应视为含在投标报价清单中，深化设计（详设）时投标人应依据招标文件、初步设计及业主提出的合理需求补充完善，且追加的建设内容不再另行增加费用；

在实际施工中，招标人可以无条件要求投标人更换不符合要求的产品，购进的材料设备与提供的样品不一致时，由投标人无条件退货，如因使用不符合国家标准、行业及各项指标的材料，由此引起的相关费用由投标人承担；

投标人应充分理解本次工程建设内容，必须确保本包相关建设内容实现与本次工程其他各包相关建设内容的正确衔接与整合。

7.中标人须实现本项目建设的交通专有域被省级政务云统一纳管。

（二）功能需求

构建一个高性能、高可用的数据中心环境。硬件设备作为数据中心运行的物理载体，必须包括服务器、存储、网络及安全设备等，并具备为上层所有软件系统与云服务提供必需的计算、存储、网络连通及全方位安全防护的能力，确保形成整个项目的坚实底座。

提供弹性可扩展的云服务。将底层硬件资源池化，并以服务形式按需供给。平台必须提供弹性云主机、云存储、云数据库等关键资源服务，实现资源的灵活调配与高效利用，以支撑整个项目所需的基础资源。

提供统一的业务能力平台。为上层各类业务应用提供标准化、可复用支撑服务的能力，确保业务应用能够快速集成核心功能，实现业务的敏捷开发与稳定运行。

（三）系统性能要求

具体要求详见本采购需求附件。

（四）信创要求

为贯彻国家信息化创新（信创）发展战略，确保本项目在关键技术上的自主可控与安全可靠，本项目要求须全面符合国家信创标准。具体包括：

1.技术路线要求：投标人提供的硬件及成品软件须为符合信创技术路线的产品。

2.产品兼容性：投标人须确保其提供的系统软件、应用软件与中国信息安全测评中心发布的安全可靠测评结果公告内的主流国产基础软硬件具有良好的兼容性。

3.安全可控要求：系统设计应遵循安全可控原则，从数据安全、网络安全、身份认证与访问控制等方面，利用国产化技术体系实现安全增强，确保从底层基础设施到上层应用的全链路安全。

4.实施与交付：中标人应在项目实施、部署、测试及试运行等各个环节，确保所开发的系统完成在国产化环境下的适配、调优与稳定运行，最终交付的系统必须是完整、可用的国产化信息系统。

（五）等保要求

为保障本项目的安全稳定运行，依据《中华人民共和国网络安全法》及国家网络安全等级保护制度，本项目须严格遵循以下要求：

1.定级与备案要求：系统安全保护等级原则上不得低于等保三级（项目一阶段设计所明确的等级）。中标人须协助采购人，依据《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）等国家标准，完成系统的等保定级及备案工作。

2.安全设计与建设要求：中标人须在系统设计与开发阶段，严格依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）中相应等保级别要求，对系统的技术安全（包括安全物理环境、安全通信网络、安全区域边界、安全计算环境）和管理安全（包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理）进行同步规划、同步建设。

3.测评与整改要求：系统开发部署完成后，中标人须配合采购人委托的具有资质的第三方测评机构，对系统进行全面测评。中标人须负责解决测评过程中发现的所有安全问题并进行整改，直至所有系统通过测评。

4.中标人所投机房设施，须在河南省智慧交通服务云平台项目启动网络安全等级保护第三级测评（等保三级）前，确保机房设施完全符合《网络安全等级保护基本要求》第三级标准规定的技术要求与管理要求。**（提供承诺函，格式自拟）**

（六）国密要求

为保障本项目数据传输、存储及应用系统的安全可控，满足国家密码法律法规及商用密码管理要求，本项目在密码技术的应用上须遵循以下规定：

1.算法标准：所有系统必须采用国家密码管理局批准的国产商用密码算法，包括但不限于 SM2、SM3、SM4 等，用于实现系统的身份认证、数字签名、数据加密、完整性保护等安全功能。

2.应用场景：国密算法应用场景包括但不限于传输、存储、身份认证、数字签名等

3.产品与合规要求：所使用的密码产品或内嵌密码技术的模块，原则上应选用具有《商用密码产品认证证书》的产品。

4.评估与整改要求：中标人应配合采购人委托的具有资质的第三方评估机构开展商用密码应用安全性评估工作。中标人须负责解决评估过程中发现的所有安全问题并进行整改，直至所有系统通过评估，并取得国家商用密码管理部门出具的备案证明。

5.中标人所投机房设施，须在河南省智慧交通服务云平台项目启动商用密码应用安全性评估（密评三级）前，确保机房设施完全符合《商用密码应用安全性评估管理办法》（国密局令第 3 号）规定的技术要求与管理要求。**（提供承诺函，格式自拟）**

三、成品软硬件技术规格

投标人需针对技术要求表中加“★”项指标做出实质性响应，不满足为无效投标。

本包所涉及的所有软硬件设备须支持 IPv4 和 IPv6。

技术要求表详见本节第十八条。

（一）成品软件功能要求

（1）运维管理平台

本项目运维管理平台主要由业务应用集成、性能检测、IT 资源整合监控、运维可视化等相关模块构成，具体涉及的软件技术规格参数、功能模块要求、性能指标标准及相关适配兼容要求，详见附件“8.4.2 业务中台建设方案”所列内容。

（2）无人机管理平台

本项目无人机管理平台主要由设备信息管理、权限管理、飞行计划任务管理、数据统计展示管理、无人机养护管理等相关模块构成，具体涉及的软件技术规格参数、功能模块要求、性能指标标准及相关适配兼容要求，详见附件“8.4.2 业务中台建设方案”所列内容。

（3）融合通信平台

本项目融合通信平台主要由在线人数授权、离线消息推送、网络和用户状态监测、视频资源管理、会议参会信息监测等相关模块构成，具体涉及的软件技术规格参数、功能模块要求、性能指标标准及相关适配兼容要求，详见附件“8.4.2 业务中台建设方案”所列内容。

（4）视频整合平台

本项目视频整合平台主要由视频接入管理、视频转发、视频协议转换等相关模块构成，具体涉及的软件技术规格参数、功能模块要求、性能指标标准及相关适配兼容要求，详见附件“8.4.2 业务中台建设方案”所列内容。

（5）设备管理平台

本项目设备管理平台主要由设备接入、设备管理、能力开放等相关模块构成，具体涉及的软件技术规格参数、功能模块要求、性能指标标准及相关适配兼容要求，详见附件“8.4.2 业务中台建设方案”所列内容。

（二）云服务平台软件功能要求

（1）云服务平台软件（公有云）

本项目云服务平台软件（公有云）主要由云平台管理能力、云主机能力、镜像管理能力、云硬盘能力、云网络能力、负载均衡、云安全能力、运维能力、运营能力等云平台相关能力构成，具体涉及的各类型软件技术规格参数、功能模块要求、详细授权数量、性能指标标准及相关适配兼容要求，详见附件“8.2 数字基础设施建设方案”所列内容。

（2）云服务平台软件（专有云）

本项目云服务平台软件（专有云）主要由弹性云主机软件、安全组软件、快照软件、在线迁移软件、裸金属服务软件、弹性伸缩软件、镜像软件、云硬盘软件、对象存储软件、租户网络软件、弹性IP软件、弹性负载均衡软件、事务型关系数据库、云向量数据库、容器服务、云管软件、大数据平台管理软件、MPP数据仓库、算力管理软件等云平台相关软件构成，具体涉及的各类型软件技术规格参数、功能模块要求、详细授权数量、性能指标标准及相关适配兼容要求，详见附件“8.2数字基础设施建设方案”所列内容。

（三）成品硬件技术规格

（1）公有云硬件

本项目公有云区硬件主要由网络设备、存储设备、安全设备、密码设备等硬件设备构成，具体涉及的各类型设备技术规格参数要求、详细配置数量及相关性能指标，详见附件“8.2数字基础设施建设方案”所列内容。

（2）专有云硬件

本项目专有云区硬件主要由网络设备、存储设备、安全设备、密码设备、数据安全等硬件设备构成，具体涉及的各类型设备技术规格参数要求、详细配置数量及相关性能指标，详见附件“8.2数字基础设施建设方案”所列内容。

（四）机房及链路租赁

机房应在郑州市域内，同时满足自然环境、公用工程条件、物理与环境安全，具体涉及的各类型设备技术规格参数要求、详细配置数量及相关性能指标，详见附件“8.10机房及配套工程建设方案”和所列内容。

（五）整体运维服务

须设置以下岗位：设置机房整体运维7*24小时岗位2个，5*8小时岗位2个；设置安全监测及处置7*24小时岗位2个；设置密码运维管理5*8小时岗1个。

工作包括但不限于：配合河南省智慧交通服务云平台项目的其他包中标人进行云资源分配、调整，7×24小时对机房内所有网络设备与安全设备进行常态化管理，确保设备物理状态稳定、基础配置正常；定期监测设备运行指标，包括带宽利用率、端口状态、CPU负载、安全告警等数据；全面分析网络运行状态，必要时进行调整和优化（包含网络故障处理、网络设备调整、网络线路保障等）；实时监测机房动环系统运行状态，并及时处理告警信息；机房基础设施进行常态化安全巡检（包含对供电系统、空调、机房门禁等）发现问题及时处理。7×24小时监测保障云平台的网络和数据安全，实时

监测部署在云平台中的系统的安全隐患风险以及受攻击情况。发生安全事件后及时开展应急处置响应支撑工作，对已经发生的告警信息及安全事件进行分析、协调、处理等工作，追踪事件原因并提供可行性建议

整体运维服务期限自交工验收完成之日起，至项目整体竣工验收后一年。

（六）与河南省智慧交通服务云平台项目其他包之间的关系

本包与河南省智慧交通服务云平台项目其他包之间的关系包括但不限于以下内容：

序号	包名称	包具体内容	关系
1	数据加工处理和中台建设	数据资源规划	本包建设内容纳入数据加工处理和中台建设的数据资源规划
2	数据加工处理和中台建设	数据采集	本包应用系统获取外部数据通过数据加工处理和中台建设的数据采集接口。
3	数据加工处理和中台建设	数据仓库建设	本包产生的数据存储于数据加工处理和中台建设的云平台数据仓库
4	数据加工处理和中台建设	数据治理	本包产生的数据纳入数据加工处理和中台建设的数据治理范围
5	数据加工处理和中台建设	数据资产构建	本包产生的数据资源由数据加工处理和中台建设的完成数据资源编目、指标体系构建、图谱-矩阵绘制。
6	数据加工处理和中台建设	数据建模分析	本包调用数据加工处理和中台建设的数据建模分析功能
7	数据加工处理和中台建设	快搜快查数据准备	本包调用数据加工处理和中台建设的快搜快查功能，本包产生的数据供数据内容归纳与管理和纸质报表报告电子化入库使用
8	数据加工处理和中台建设	数据共享	本包产生的数据由数据加工处理和中台建设的数据共享功能向外共享。
9	数据加工处理和中台建设	数据加工	本包产生的数据供数据加工处理和中台建设的数据加工使用，调用数据加工处理和中台建设的数据加工功能。
10	数据加工处理和中台建设	数据中台	本包产生的数据供数据中台调用，调用数据加工处理和中台建设的数据中台功能

序号	包名称	包具体内容	关系
11	数据加工处理和中台建设	业务中台	本包调用数据加工处理和中台建设的业务中台服务池资源。
12	数据加工处理和中台建设	AI 中台	本包调用数据加工处理和中台建设的 AI 中台功能。
13	数据加工处理和中台建设	AI 大模型适配	本包调用数据加工处理和中台建设的 AI 中台大模型，本包应用开发的模型受数据加工处理和中台建设的 AI 大模型适配功能管理
14	数据加工处理和中台建设	AI 数据需求调研对接和调优测试	本包接受数据加工处理和中台建设的 AI 数据需求调研，并配合调优
15	数据加工处理和中台建设	数据综合管理	本包产生的数据受数据加工处理和中台建设的的数据综合管理
16	运行监测预警服务+集成费	运行监测预警服务	本包为运行监测预警服务包应用系统的正常稳定运行提供基础资源和安全保障。
17	运行监测预警服务+集成费	统一门户	本包建设内容纳入统一门户管理范围，统一 UI 设计，统一授时，统一权限管理；调用业务中台可视化工具；调用业务中台工作流引擎进行工作量配置;纳入业务中台搜索引擎搜索范围，并可调用搜索引擎；调用业务中台算法管理平台功能；为业务中台视频整合平台提供道路运行监测相关视频数据，调用视频整合平台视频资源；调用业务中台融合通信平台功能；软件开发符合业务中台代码通用管理系统要求。
18	道路运输与执法监管+集成费	道路运输与执法监管	本包为道路运输与执法监管包应用系统的正常稳定运行提供基础资源和安全保障。
19	普通公路管理+集成费	普通公路管理	本包为普通公路管理包应用系统的正常稳定运行提供基础资源和安全保障。
20	基础设施监测预警	基础设施监测预警	本包为基础设施监测预警包应用系统的正常稳定运行提供基础资源和安全保障。

序号	包名称	包具体内容	关系
21	地理信息平台+集成费	地理信息平台	本包为地理信息平台的正常稳定运行提供基础资源和安全保障。
22	电子航道图与内河航运综合监管+集成费	电子航道图与内河航运综合监管	本包为电子航道图与内河航运综合监管应用系统的正常稳定运行提供基础资源和安全保障。
23	工程监理	工程监理	本包建设监理由工程监理包执行
24	安全等级保护测评	安全等级保护测评费用	本包安全等级保护测评由安全等级保护测评包执行
25	商用密码应用安全评估	商用密码应用安全评估	本包商用密码应用安全评估由商用密码应用安全评估包执行
26	第三方软件测试	第三方软件测试	本包第三方软件测试由第三方软件测试包执行

（七）详细技术要求

具体要求详见本采购需求附件。

四、系统集成要求

为确保本包对河南省智慧交通服务云平台项目的其他包以及河南省交通运输厅其他业务系统的集成，系统集成包括但不限于以下要求：

1.实现与已建或在建系统平台的软硬件集成、数据对接、部署安装、测试。

2.负责协同并引导其他中标方完成集成，建立统一的基础软硬件服务能力，形成一致的用户体验与业务入口，统一提供为其他中标方硬件设备服务能力，确保系统间的一致性与协同性。

3.负责协调并引导其他中标方完成集成。

4.实现与河南省“一轴一廊”交通基础设施数字化转型升级示范通道及网络项目其他建设任务的软硬件集成、数据对接。

5.中标人应利用本项目的代码通用管理系统对所有定制开发的软件源代码和系统运行必要的第三方插件包进行统一管理，实现源代码及文档托管、源代码自动编译、统一部署集成，并接受代码通用管理系统的权限控制、代码审计和部署监控。中标人在交工验收前应按照采购人要求编制系统部署方案，并在后续迭代过程中持续完善。

6.中标人需负责以下接入及相关具体工作：负责实现所提供的无人机管理平台与包括但不限于河南省普通干线公路无人机设备、交投集团无人机平台的全面对接，根据采购人要求，完成无人机的接入、部署及调试工作，确保所有接入无人机可通过该平台实现有效管理；负责承接河南省普通干线公

路设备、执法站点设备、水路设备的接入实施工作，完成所提供设备管理平台与交投集团物联网平台的对接调试，需提供不少于 130 个标准物模型供各类设备适配使用，并完成不少于 3 万台设备的接入授权配置，保障所有接入设备稳定联网及数据交互；根据采购人要求为视频整合平台完成治超站、执法站点等非国标视频的转码和接入工作；负责将硬件设备兼容性作为云服务平台软件（公有云）与云服务平台软件（专有云）的核心技术指标进行落地实施，全面完成与本期采购及部署的各类硬件设备的适配测试与调试工作，确保软件功能与硬件性能深度匹配，通过优化配置实现系统整体高效运行。

7.中标人应在中标合同签订后 20 日历日内，完成施工图设计，并通过由采购人组织的专家评审。

五、成品软硬件部署要求

（一）成品软件部署要求

（1）部署环境准备

成品软件须部署于招标方指定的国产服务器操作系统环境中，确保版本完全兼容。

部署前需完成基础环境配置，包括安装指定版本的国产数据库、中间件及其他必需的依赖组件。

（2）软件安装与配置

严格遵循部署手册，完成软件安装与组件配置。

根据招标方业务需求，完成系统管理员、核心参数及业务流程的初始化设置。

（3）数据初始化

如涉及历史数据，须制定迁移方案，完成数据清洗、转换与核对，确保数据准确完整。

（4）系统集成

如需与现有其他系统对接，须按招标方规范完成接口配置与联调测试，确保数据互通与功能协同。

（5）安全与权限

部署中须完成系统安全加固，修改默认设置，配置高强度安全策略。

依据招标方组织架构，配置并测试用户角色与操作权限，确保权责清晰。

（6）验收与文档

需交付完整的部署记录、系统架构图及配置说明文档。

提交最终软件介质、授权文件及全套用户管理手册，作为验收依据。

（二）硬件设备安装要求

（1）机柜安装与布局

所有硬件设备必须稳固安装于指定标准机柜内，确保承重均匀分布，机柜整体载荷应符合机房承重设计标准。

设备布局应遵循“重物下置、高热分散”原则，重型设备安装于机柜中下部，高功率、高热密度

设备应分散布置，避免局部过热。

设备间需预留不低于 1U 的垂直空间，确保前后风道畅通，形成冷热通道隔离，满足强制散热要求。正面（进风口）与背面（排风口）不得有线缆、挡板等阻碍气流。

（2）供电与功率管理

设备供电必须接入额定容量匹配的不间断电源（UPS）回路，单相用电设备应均匀分配至不同相位，确保三相平衡。

严格核算单台设备、单机柜及总体的额定功率、峰值功率与典型功耗，确保 UPS 容量、配电回路及 PDU 额定电流留有不低于 30%的冗余。

所有设备应使用标准电源接头，可靠连接至机柜专用电源分配单元（PDU），禁止使用非标转接线或串接插排。双电源设备应分别接入两路独立的 PDU，实现冗余供电。

（3）线缆布放与管理

所有线缆（电源线、网络线、光纤、控制线等）须按类型规范布放，强弱电线缆分离，或采用屏蔽措施避免干扰。

线缆应沿机柜线槽布设，横平竖直，使用尼龙扎带或魔术贴捆扎固定，松紧适度，弯曲半径应符合线缆规范（如光纤不低于直径的 10 倍）。

每条线缆两端均须粘贴唯一、清晰、耐久的标识标签，标签内容应包括本端/对端设备、端口及用途等信息，便于快速识别与维护。

（4）安全与接地

安装过程须严格遵守国家电气安全、机房消防及电磁兼容等相关规范。

所有设备金属外壳、机柜均须可靠接地，接地电阻符合国家标准，确保人员与设备安全，并有效抑制静电与电磁干扰。

（5）安装记录与验收

安装过程中需填写完整安装记录，包括设备上架位置、电源接线图、网络端口分配、IP 地址规划、硬件配置清单及功率测算数据等。

所有记录文档应图文并茂，作为项目竣工验收的必要依据，并纳入后期运维档案。

（三）信创兼容性要求

部件必须与信创云平台完全兼容，如不能完全兼容，则需免费更换原厂其他能完全兼容的部件。

六、培训要求

1.培训要求：

中标人应针对本项目所有软、硬件产品，组建专业的培训团队，明确分工职责，并对采购人（含

相关用户单位）的相关人员开展多批次、多层次、多种形式的培训。具体要求如下：

（1）中标人应保证提供熟悉本项目全部软、硬件产品的培训讲师，其中硬件培训讲师须具备相应产品的技术认证资质。

（2）培训内容必须全面覆盖本项目所涉及的成品软件、服务器、网络设备、安全设备、存储设备以及其他所有硬件产品。

（3）培训应包括但不限于软件操作、系统维护管理、硬件设备操作、日常维护及故障排查等。

（4）中标人应根据采购人需要，提供集中授课、现场指导、模拟演练等多种灵活的培训方式。

（5）中标人须提供完整的软硬件综合培训方案、培训计划与培训教材，所有资料须经监理单位审核并报采购人批准后执行。

2.培训目标

通过系统化培训，确保采购人及相关用户单位人员达到以下目标：

（1）系统管理员

硬件管理员：能够独立完成所有硬件设备的启停、状态监控、日志分析、故障诊断与部件更换；能有效应对硬件类应急事件。

软件管理员：能够独立完成软件的安装、配置、管理、备份、恢复和优化；能够处理软件运行中的常见问题与突发事件，有效解答操作人员的常见疑问。

（2）操作人员

成品软件操作人员：掌握软件系统的业务流程和操作方法，能独立处理日常业务。

硬件设备操作人员：熟悉相关硬件设备的基本操作和注意事项，能正确使用设备并执行简单状态检查。

七、应用推广要求

为了使本项目具有良好的应用推广效果，实现应用系统的建设目标，中标人需：

1.按照采购人及相关用户单位要求编制系统推广应用相关的配套制度，配合采购人及相关用户单位开展应用效果考核等工作。

2.按照采购人及相关用户单位要求做好充分的培训，并根据需要到相关系统应用现场进行指导。

3.系统质保期（免费维护期）内，中标人应在相关系统应用范围内深入推广应用，并采取多种方式指导各级各类用户操作使用，及时解决系统应用过程中出现的各种问题。

八、项目进度要求

1.合同签订之日起6个月内，中标人应当完成软件系统及接口开发、完成软硬件设备的到货验收、数据资源相关建设，完成系统测试、软硬件部署。由中标人组织交工验收，经采购人同意后，进入系

统联调。

2.系统联调满 3 个月，由采购人组织项目初步验收。初步验收通过后进入试运行，试运行不少于 3 个月，试运行后采购人组织竣工验收。

3.项目实施总时间：不超过 22 个月（从合同生效之日起至竣工验收合格）。

4.项目硬件质保期：自项目竣工验收合格之日起开始计算，本项目硬件设备三年免费原厂质保。针对本项目提供 7*24 免费售后技术支持服务（包括但不限于定期巡检、调整优化、维修更换、网络接入、备品备件、设备更换、部件更换、固件版本升级、规则库升级、病毒库升级、特征库升级、漏洞库升级、故障排除、技术咨询等）。

5.项目软件运维期：自项目竣工验收合格之日起开始计算，成品软件免费运维三年；开发软件免费运维一年。针对本项目提供 7*24 免费售后技术支持服务（包括但不限于运行监控、定期巡检、调整优化、使用支持、故障排除、需求管理、备份和恢复、系统迁移、资产管理和配置管理、版本升级、漏洞修复、技术咨询等）。

九、组织机构要求

1.项目实施团队人员

（1）投标人应指派项目负责人 1 名，负责整体项目实施全过程管理和控制各项工作。

（2）投标人应指派技术负责人 1 名，负责项目整体项目实施全过程技术把关。

（3）投标人应指派不少于 20 人的项目团队。

2.项目实施团队人员要求

投标人应提供**项目核心人员一览表**（至少包括姓名、学历、职称及执业资格、拟任职务、是否驻场）。

注：项目团队中的项目负责人、技术负责人、各团队负责人、团队内各分组负责人**均应列为核心人员**。

3.项目驻场要求

为保障项目建设实施过程的高效沟通与衔接，确保项目建设任务高质量如期完成，项目上线试运行前需提供现场服务（地点应在项目实施机房 3 公里以内，由中标人自行选择并承担相关费用），现场服务人员不少于 15 人（核心人员均应驻场），且该驻地包括至少可容纳 20 人办公的办公场所或 1 间不少于 20 人位的会议场所，用于召开例会、调度会、关键节点审查会及各类协调会议等，项目负责人、项目技术负责人、各分组负责人在项目交工验收合格前应全程在项目驻地办公（国家法定节假日除外），其他人员在项目驻地办公要求由采购人根据项目进展及项目建设实际需要确定。

项目初步验收合格后，质保期（免费维护期）结束前，中标人应根据采购人要求至少安排 15 人

提供驻场服务（驻场人员须为项目核心人员，驻场场地由中标人自行提供并承担一切费用，不少于 7 个工位，提供系统运行和使用技术支持，确保系统稳定运行及项目建设目标有效实现。同时，采购人应根据项目运维工作实际需要，安排部分运维人员在相关用户单位提供的其他场地驻场运维。

驻场人员工作时间与采购人一致。

4.团队管理要求

（1）中标人为本项目组成的团队人员及资质应与投标文件保持一致。如果在合同履行过程中采购人发现有团队成员不符合招标文件规定的，中标人应无条件更换为符合招标文件规定的人员。

（2）本项目交工验收前，中标人原则上不得变更项目团队人员。中标人更换项目团队成员的，采购人将按照如下方式处理：

①中标人非因意外情况及不可抗力事件导致而变更项目核心人员的，须经采购人书面同意，采购人从合同总金额中扣除人民币拾万元（100000 元）/人次的违约金；中标人未经采购人书面同意擅自更换核心人员的，采购人从合同总金额中扣除人民币贰拾万元（200000 元）/人次的违约金，给采购人造成损失的，中标人还须全额赔偿采购人损失。

②中标人变更项目团队其它人员的，须经采购人书面同意；中标人未经采购人书面同意擅自更换的，采购人从合同总金额中扣除人民币捌万元（80000 元）/人次的违约金，给采购人造成损失的，中标人还须全额赔偿采购人损失。

（3）中标人项目组应建立项目调度制度，定期举行工地例会，汇报项目计划执行情况和解决项目执行过程中存在的困难和问题。

（4）日常考勤及处理：

①采购人委托监理单位负责对中标人驻场项目组成员进行日常考勤，及时向采购人项目联系人报告，考勤情况须写入监理周报。

②中标人驻场项目组成员请假半天及半天以上须履行请假手续，否则以旷工论处。

③中标人驻场项目组成员旷工的，采购人从合同总金额中扣除人民币壹仟元（1000 元）/人次的违约金。同一人累计旷工超过 3 次的（含 3 次），采购人要求中标人以同等或更高资历条件的人员替换该旷工人员。

十、质量保证及运维要求

1.中标人应保证系统的开发、实施及维护满足采购人需求，完全符合合同规定质量、技术和性能的要求。所有第三方技术或产品必须得到合法地使用授权。

2.质保期（免费维护期）：质保期（免费维护期）从竣工验收合格之日起计算。质保期（免费维护期）内，中标人应当保证接到通知后 10 分钟内响应，30 分钟内赶到现场提供服务。以上质保期（免

费维护期）如涉及费用均包含在合同价中。在质保期（免费维护期）内，中标人应当免费为采购人提供上门系统维护服务，如有质量问题，中标人应予以免费更换、修改、维修。质保期（免费维护期）内中标人有义务向采购人免费提供软件系统的最新技术和软件升级版本，满足新的业务需求。

3.在质保期（免费维护期）内，如发现系统有潜在设计缺陷或维护服务措施不当，采购人有权退货或向中标人索赔，或者要求中标人限期整改。

4.中标人应保证按照招标文件要求实现采购人所有开发、实施、测试、培训、验收和维护工作。

5.中标人必须严格遵守《中华人民共和国产品质量法》，并完整地履行质保期（免费维护期）内的免费现场维修服务承诺。

6.由于产品技术性能或服务响应不及时到位给采购人造成损失或不良影响的，中标人应赔偿采购人损失。

7.在质保期结束之后，采购人可要求中标人继续提供日常维护支持服务，并支付相应的维护服务费，中标人应提供优惠收费，具体由双方另行商定。

十一、违约与赔偿责任

1.在本合同履行中，因出现在现有技术水平和条件下难以克服的技术困难，导致中标人开发失败或部分失败的，采购人有权单方解除合同，中标人应当赔偿由此给采购人造成的全部损失，中标人损失赔偿额不超过本合同的总金额。

2.在本合同履行过程中，中标人若出现或凭其判断可能出现无法克服的技术困难，并可能致使开发失败或者部分失败的情形时，应当及时通知采购人并采取适当措施减少损失。没有及时通知并采取适当措施，采购人有权单方解除合同，给采购人造成损失的，中标人应当赔偿采购人的全部损失，中标人赔偿额不超过本合同的总金额。

3.中标人未能履行本合同约定，安装未经双方确认的应用软件，必须主动迅速停用或更换软件，并承担停用及更换的费用，赔偿相关损失。如果中标人在采购人指定的日期前仍不更换软件，采购人有权单方解除合同，停止向中标人付款，中标人还应赔偿由此给采购人造成的全部损失。

4.质保期（免费维护期）内，中标人未能履行本合同约定，不能按时完成软件的升级工作或未能按约提供维修或维护服务，中标人每次需按照合同总额的千分之三（3‰）支付违约金。

5.因中标人原因造成采购人数据丢失、泄露的，中标人应承担相应的赔偿及法律责任。

6.因中标人原因（包括但不限于系统功能未实现、性能不达标、数据错误、交付延迟等）导致河南省智慧交通服务云平台项目在2025年度、2026年度交通运输部组织的数字化转型升级绩效评价考核中扣分，造成河南省未获得全额中央财政资金补助的，**按以下方式处理：**

中标人按“**中标人原因扣分值/厅本级总扣分值×厅本级未获取资金金额**”承担损失，中标人损

失赔偿额不超过合同总金额，该金额**直接从合同应付款项中扣除**。中标人有异议的，可在采购人明确损失赔偿额后 10 个工作日内提出申辩，由**采购人复核并出具最终认定意见**。

7.中标人需遵守项目监理有关规范，如有违约，将按照该办法的相关要求进行处理。

8.合同履行过程中，如中标人出现违约行为，中标人同意采购人在应付款项中直接扣除相应违约金。中标人违约金的承担方式不影响发票开具，中标人向采购人开票金额仍以合同约定的应付款为准。

9.本项目所称采购人的损失既包括直接损失，也包括期待利益等间接损失及可能发生的诉讼费、保全费、律师费等实现债权的费用。

十二、保密要求

中标人应按规定严格做好保密工作，未经采购人许可，在本合同有效期间及有效期结束后，中标人不得将合同执行过程中获悉的任何资料及数据擅自复印、修改，或向第三方透露、转让、提供版权或所有权，不得向任何第三方提供本项目信息系统的源程序，否则中标人应承担由此引起的法律后果及经济赔偿责任。

十三、知识产权归属

1.中标人向采购人提交的河南省智慧交通服务云平台项目应用软件开发成果的知识产权，以及中标人为河南省智慧交通服务云平台项目应用软件开发之目的在开发过程中新形成的专利、计算机软件、技术诀窍、秘密信息、技术资料和文件的知识产权均归采购人单独所有（中标人在本合同签署之前已经拥有的知识产权和中标人按照本合同约定使用的第三方的知识产权除外）。

2.除非采购人书面同意，中标人不得以任何方式向第三方披露、转让和许可有关的技术成果、计算机软件、技术诀窍、秘密信息、技术资料、文件等。

3.除本项目开发工作需要之外，未得到采购人的书面许可，中标人不得以任何方式商业性地利用上述资料和技术。

4.采购人委托中标人开发的本单位本项目产品升级后新产生的知识产权仍归采购人所有。

5.双方确定，采购人有权使用中标人按照本合同约定提供的研究开发成果进行后续改进。由此产生的具有实质性或创造性技术进步特征的新的技术成果及其权利归属，由采购人享有。

6.中标人利用研究开发经费所购置与研究开发工作有关的设备、器材、资料等财产，归采购人所有。

7.中标人有权在完成本合同约定的研究开发工作后，利用该项研究开发成果（不包括软件系统中的用户信息和各类数据）进行后续改进。由此产生的具有实质性或创造性技术进步特征的新的技术成果，归中标人所有。

8.双方完成本合同项目的主要研究人员享有在有关技术成果文件上写明技术成果完成者的权利

和取得有关荣誉证书、奖励的权利。

十四、验收要求

1.验收依据

（1）国家、省有关法律、法规，以及国家、省关于信息系统建设的有关标准、规范、办法及文件等。

（2）报交通运输部备案的《河南省“一轴一廊”交通基础设施数字化转型升级示范通道及网络实施方案》。

（3）经批准的项目可行性报告及其批复文件。

（4）经批准的一阶段设计和投资概预算报告及批复文件。

（5）项目招投标文件、合同文件、设计文件、施工图设计文件、设备和软件技术说明书以及项目结、决算有关资料。

（6）监理单位提供的有关验收规范。

2.验收组织

中标人应配合监理单位做好验收收尾、资料准备等工作。项目验收工作由包括采购人上级主管部门、采购人、监理单位、用户单位、测评单位、专家和中标人等在内的项目验收组来完成。

（1）验收分为交工验收、初步验收和竣工验收。

（2）交工验收由中标人组织，并出具交工验收报告。

（3）初步验收由采购人组织，并出具初步验收报告。

（4）竣工验收由采购人上级有关部门组织。

3.交工验收

（1）中标人自检合格后向监理单位提交交工验收申请。

（2）监理单位组织审查中标人提出的交工验收申请和交工验收方案。

（3）中标人组织采购人、监理单位等对项目的工程、技术、功能、财务和档案等进行验收，合格后形成交工验收报告。

4.初步验收

（1）交工验收后，系统试运行满 3 个月后，中标人向采购人提交初步验收申请。

（2）采购人组织审查中标人提出的初步验收申请和初步验收方案。

（3）采购人根据需要组织单项验收，形成单项验收报告。

（4）采购人组织第三方功能、性能、安全测评并出具测评报告。

（5）采购人组织等级保护测评及备案。

（6）经采购人审核确认后出具《数据接入认定书》《部署交付确认书》。

（7）采购人组织对项目的工程、技术和档案等进行验收，合格后形成初步验收报告。

（8）第三方测试（测评）合格，不免除中标人因产品质量问题而应承担的赔偿责任。

（9）若第三方测试（测评）不合格，中标人应在采购人要求的时间内完成整改并重新申请验收，整改费用由中标人承担，逾期未通过验收的，中标人应承担逾期违约责任。

5.档案验收

为规范本项目档案管理工作，确保项目档案的完整性、准确性、系统性和安全性，为系统的长期运维和审计追溯提供可靠依据，本项目档案的整理及验收需满足如下要求：

（1）归档范围与质量要求：中标人负责从合同签订、项目调研、设计、开发、测试、培训、试运行、推广应用、验收到运维移交全过程中产生的，具有保存价值的各类文件材料（包括但不限于纸质、电子、声像等不同载体）的收集、整理与编制工作。归档文件材料必须齐全、完整、签章完备，其质量应符合国家及河南省关于档案案卷构成的相关要求。

（2）整理标准与规范性要求：项目档案管理必须严格遵循《政务信息化项目档案管理规范》（DB43/T 1889-2020）以及河南省档案行政主管部门发布的现行相关法规、标准与文件要求。

（3）专项验收要求：中标人须全程配合档案专项验收各项工作，直至本项目档案通过采购人上级有关档案主管部门组织的正式验收，并取得验收通过的正式意见或批复文件。

（4）中标人须提供河南省智慧交通服务云平台项目所有包档案文件存放场所。

6.竣工验收

（1）竣工验收条件

①项目建设已全部完成，交工验收合格后系统正常运行 6 个月内；

②完成结算审核和财务决算审计；

③档案文件整理齐全，通过档案验收；

④中标人对工程质量自检合格，并出具自检报告；

⑤经第三方软件测评、等级保护测评、密码安全评估合格，并出具测评/评估报告。

⑥系统能完全满足相关用户使用需求，并由用户出具意见为合格（或满意）的书面用户使用报告。

项目竣工验收具体条件根据采购人上级有关部门文件要求及竣工验收组织部门的相关要求确定。

（2）项目满足上述竣工验收条件后，中标人提交竣工验收申请。

（3）由采购人上级有关部门组建竣工验收委员会。

（4）竣工验收委员会须对竣工验收的先期基础性工作进行检查，重点检查项目建设、设计、监理、施工、招标采购、档案资料、预算执行和财务决算等情况，提出评价意见和建议。

（5）竣工验收委员会基于评价意见出具竣工验收报告。

7.中标人成果交付

中标人在双方组织的各项阶段性验收过程中，应当根据本合同要求免费向验收组提供完整的验收资料。中标人所有提交的文档必须符合采购人要求的文档规范。

十五、费用支付

1.银行保函

合同签订后2个工作日之内，中标人向采购人提供合同总金额100%的银行保函，保函时效不低于6个月。若中标人无法在限定时间内开具银行保函，资金被财政收回导致无法支付，后果由中标人自行承担。采购人在收到银行保函后支付等额项目条款。

2.支付条件及支付额度

其他条款以合同签订为准。

3.支付单位：河南省交通运输调度指挥中心。

4.支付程序：合同签订后，中标人应配合采购人办理备案。每次付款前，中标人应将发票和相关支付材料交采购人，采购人通过国库集中支付网支付合同款。

5.采购人不向项目合同约定的收款账户外的任何其他账户办理付款手续，中标人确需变更收款账户信息的，应当提交其法定代表人签字并加盖财务专用章的证明材料，并征得采购人书面同意。

6.采购人付款前，中标人应当向采购人出具符合要求的相应正式发票。如中标人未按时出具发票或出具发票不符合要求的，采购人可相应顺延付款时间，且不视为违约，无需承担任何违约责任。

7.本合同款项的支付均使用财政资金，因财政资金未到位或财政支付流程等原因导致付款延迟的，不视为采购人违约，采购人无需承担任何违约责任。

十六、转包和分包

1.中标人不得以任何形式将合同转包、转让。

2.除本招标文件中明确同意分包且中标人在其投标文件中明确响应分包的本项目非主体、非关键性工作外，中标人不得将合同的其他任何工作内容分包给他人。

3.中标人违反本条规定的，采购人有权单方解除合同，并要求中标人支付本合同总价款百分之二十（20%）的违约金，给采购人造成损失的，中标人还应赔偿采购人全部损失。

十七、其他要求及相关约定

见本招标文件第四章《政府采购合同》

十八、技术要求表

1.公有云安全软件

序号	设备类别及名称	技术规格	单位	数量
1.1	云安全管理平台	★1.性能指标：满足本项目安全设备设施的纳管； 2.功能指标： ▲下一代防火墙、Web 应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）等安全能力。 ▲云安全管理平台内置云安全中心，能够汇总展示资产面临的安全风险。 云安全管理平台支持多级架构设置云安全区域，并将管理员与区域进行关联，可按照云安全区域选择虚拟安全组件，管理员拥有对应区域内的设备设施管理、工单管理等权限。 ★3.永久授权，三年原厂维保服务。	套	1
1.2	漏洞扫描	★1.性能要求：授权可并发扫描 IP 数≥64 个；支持 Web 应用、操作系统、网络设备、数据库及安全基线配置的全面扫描； 2.功能指标： ★具备超过 200000 条漏洞特征的知识库，与国际及国内主流漏洞标准兼容； ▲支持弱口令扫描，允许用户自定义密码字典与扫描策略； ▲全面覆盖 SQL 注入、XSS、命令执行、文件包含、反序列化等 OWASPTOP10 核心 Web 漏洞检测； 支持生成漏洞扫描报告； ★3.永久授权，三年原厂维保服务。	套	1
1.3	日志审计	★1.性能要求：日志处理性能≥2000EPS；支持日志源类型≥100 种； 2.功能指标： ★支持 Syslog、SNMP、Agent 等多种日志采集方式； ★内置不少于 5000 种日志解析规则，覆盖主流网络、安全及服务器设备； ▲支持日志的标准化、范式化及自定义解析； ▲具备智能日志分析能力； ▲支持实时日志检索、统计报表、关联分析及异常行为检测； 可对潜在安全威胁进行挖掘与可视化展示； ★3.永久授权，三年原厂维保服务。	套	1

序号	设备类别及名称	技术规格	单位	数量
1.4	堡垒机	★1.性能要求：授权管理资产数≥600 个；支持并发字符会话数≥600； 2.功能指标： ★支持系统管理员、部门管理员、运维员、审计员等多角色精细权限划分； ▲支持旁路部署 ★支持 B/S 架构管理； ▲可基于用户、资产、协议等条件设置访问控制策略，并对高危命令进行实时告警或阻断； ▲支持 SSH、Telnet、RDP、VNC 等协议的 H5 化运维，无需安装本地客户端； ★支持 Oracle、MySQL、SQLServer、达梦、人大金仓等主流数据库的协议代理与操作审计； ★提供完整的会话录屏、命令记录及操作回溯功能； ★3.永久授权，三年原厂维保服务。	套	1
1.5	数据库审计	★1.性能要求：支持数据库实例数≥32 个；SQL 语句处理性能≥20000 条/秒； 2.功能指标： ★全面支持达梦、金仓、高斯等国产数据库及国外主流数据库的协议解析与行为审计； ▲支持基于 SQL 注入、漏洞攻击、数据泄露、违规操作等内置规则进行实时风险检测与告警； ▲具备精细化的访问控制策略，可基于客户端 IP、数据库账号、工具、时间等多维度设置审计规则； ▲支持全量 SQL 记录，捕获并分析语句内容、执行状态、影响行数等详细信息； 提供智能日志分析界面，支持多维度钻取查询与可视化筛选； 支持通过 Syslog 等标准协议将审计日志外送至第三方平台； ★3.永久授权，三年原厂维保服务。	套	1
1.6	主机安全防护	★1.性能指标：支持≥500 台云虚拟机的安全防护。 2.功能指标： ▲提供统一的中央管理控制台，实现策略统一下发、资产状态监控与安全事件集中响应； ▲支持网络访问控制，可按照 IP、端口、协议设置精细化网络策略； ★具备主机级文件传输监控与访问控制能力，支持黑白名单机制； ▲集成病毒查杀与恶意代码防护功能，支持全盘扫描、快速扫描及自定义扫描任务； ▲提供高级威胁防护能力，可检测并阻断无文件攻击、内存攻击等新型威胁； ▲支持安全基线检查与自动化合规评估；具备样本上报与威胁情报联动能力； ★3.永久授权，三年原厂维保服务。	套	1

序号	设备类别及名称	技术规格	单位	数量
1.7	Web 应用防火墙	★1.性能要求：HTTP 防护流量≥500Mbps；HTTP 最大并发连接数≥50000；HTTP 每秒新建连接数≥4000； 2.功能指标： ★支持对 SQL 注入、XSS、Webshell 等 Web 攻击的检测与防护； ★支持 CC 攻击防护； ★支持自定义安全策略与黑白名单； ★具备完整的攻击日志记录与审计功能； ★3.永久授权，提供三年原厂维保服务和规则库的升级授权。	套	1
1.8	流量探针	★1.性能要求：应用层吞吐量≥1Gbps； 2.功能指标： ★支持检测 Web 攻击、恶意文件、暴力破解、漏洞利用、数据泄露等多种网络威胁； ★利用沙箱、异常行为分析等手段，有效发现 APT 攻击、0day 漏洞利用及未知恶意代码； ▲支持对加密流量进行解析与检测，精准定位异常主机与攻击源； ▲支持流量溯源，关联原始流量包与攻击上下文； ★3.永久授权，三年原厂维保服务。	套	1
1.9	态势感知平台	★1.性能指标：全流量分析≥5Gbps、威胁检测模式≥10Gbps，数据采集和处理性能≥1.5wEPS； 2.功能指标： ▲实现实体间网络互访关系的多级分析，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级分析，支持威胁关系的自动拓展； ▲支持人工录入、流量自动发现、扫描发现等资产数据接入方式；流量自动发现方式能自动识别资产类型，如 Web 服务器、DNS 服务器、邮件服务器、FTP 文件服务器等多种类型资产，支持 web 业务系统发现；支持批量确认流量发现的资产；支持提供资产同步标准化接口，支持第三方通过自定义设置同步数据源进行资产同步； ▲自动化编排支持通过图形化界面拖拽编辑自定义剧本，编排的组件，包括标准动作、设备动作、决策、脚本、人工任务、并行节点和等待节点； ★应对网络、主机和 Web 应用等的运行状态、常见漏洞、各种攻击行为和异常行为等进行实时监测。 ▲平台能够支持针对 IP、域名、会话进行封堵，支持主机隔离、流量牵引等方式联动设备进行封堵。 ▲应建立包括资产态势、威胁态势、漏洞态势、攻击态势、事件态势等在内的安全态势评估体系，并对其进行评估。 ▲数据检索支持多种检索模式；检索语句支持快速保存，保留检索语句历史记录；支持统计指标、规则模型、关	套	1

序号	设备类别及名称	技术规格	单位	数量
		联模型、情报模型，对实时数据进行分析与告警。 ★支持集群化部署。 ★3.永久授权，三年原厂维保服务。		

2.公有云安全硬件

序号	设备类别及名称	技术规格	单位	数量
2.1	边界区防火墙	★1.核心芯片：国产化 CPU; ★2.性能要求：网络层吞吐量≥40Gbps，应用层吞吐量≥10Gbps，最大并发连接数≥800 万，每秒新建连接数≥40 万； ★3.硬件规格：标准机架式设备。千兆电口≥4 个，万兆光口≥4 个（满配光模块）； 4.功能指标： ▲支持入侵防御及病毒防护； 支持 IPSec/SSLVPN; ▲支持安全域划分及基于地址、应用、服务、时间等多维度的访问控制策略； ▲支持实时威胁检测与日志审计； ▲具备策略路由及网络地址转换能力； ★5.可靠性：支持双机热备，双冗余电源; ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权	台	2
2.2	数据安全交换系统	整体要求：包含数据交换前置机、数据交换后置机、安全隔离网闸 ★1.性能要求：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★2.规格要求：提供标准化的跨网数据交换接口，包括但不限于：文件交换、数据库交换、消息交换、请求服务接口、音视频代理接口等；支持基于文件特征、文件内容、文件名、病毒检测、URL 过滤、命令方法、信令动作、媒体流格式等多维度的安全检查策略。 3.数据交换前置机： ★核心芯片：国产化 CPU; ★性能指标：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★硬件规格：标准机架式设备;≥6 个千兆电口，≥2 个千兆光口（满配光模块），≥2 个扩展槽。 功能指标：交换平台前置机，通过网络安全隔离、协议剥离与重组、访问控制、内容过滤和安全认证等技术，实现边界网络和协议安全隔离，使跨网跨域业务数据和应用协议得到高安全性、可控性和可管理性。提供文件交换、数据交换、接口服务交换、消息交换、协议转换、病毒防护、访问控制、高可用集群、日志审计等功能模块。 4.数据交换后置机：	套	1

序号	设备类别及名称	技术规格	单位	数量
		★核心芯片：国产化 CPU； ★性能指标：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★硬件规格：标准机架式设备;≥6 个千兆电口，≥2 个千兆光口（满配光模块），≥2 个扩展槽。 功能指标：交换平台后置机，通过网络安全隔离、协议剥离与重组、访问控制、内容过滤和安全认证等技术，实现边界网络和协议安全隔离，使跨网跨域业务数据和应用协议得到高安全性、可控性和可管理性。提供文件交换、数据交换、接口服务交换、消息交换、协议转换、病毒防护、访问控制、高可用集群、日志审计等功能模块。 5.安全隔离网闸。 ★核心芯片：国产化 CPU； 安全隔离网闸-外网端：标准机架式设备；≥6 个千兆电口，≥2 个万兆光口（满配光模块）；冗余电源； 安全隔离网闸-内网端：2U 机架式设备；≥6 个千兆电口，≥2 个万兆光口（满配光模块）；冗余电源； ★6.可靠性：冗余电源; ★7.三年原厂维保服务。		
2.3	安全运维管理区/办公区防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐量≥10Gbps，应用层吞吐量≥2Gbps，最大并发连接数≥200 万，新建连接数≥6 万； ★3.硬件规格：标准机架式设备。千兆电口≥4 个，万兆光口≥4 个（满配光模块）； 4.功能指标： ▲支持入侵防御及病毒防护； 支持 IPSec/SSLVPN； ▲支持多维度的安全策略及访问控制； ▲支持实时威胁检测与日志审计； ▲具备策略路由及网络地址转换能力； ★5.可靠性：支持双机热备，冗余电源; ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权	台	2
2.4	Web 应用防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：HTTP 吞吐量≥20Gbps；HTTPS 吞吐量≥8Gbps；每秒事务处理数≥14000； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥2TB；万兆光口≥4 个（满配光模块）	台	2

序号	设备类别及名称	技术规格	单位	数量
		4.功能指标： ▲支持对 SQL 注入、XSS、Webshell 等 Web 攻击的检测与防护； ▲支持 CC 攻击防护； ▲支持自定义安全策略与黑白名单； 具备完整的攻击日志记录与审计功能； ★5.可靠性：双机热备，冗余电源； ★6.三年原厂维保服务和 web 应用防护规则库的升级授权		
2.5	抗 DDoS	★1.核心芯片：国产化 CPU； ★2.性能要求：处理能力≥10Gbps； ★3.硬件规格：标准机架式设备；千兆电口≥4 个；万兆光口≥4 个（满配光模块） 4.功能指标： ▲支持对各类 Flood 攻击、CC 攻击及混合型 DDoS 攻击进行流量清洗； ▲支持攻击源指纹学习与自动封禁； ▲具备实时流量监控与清洗报表功能； ★5.可靠性：冗余电源； ★6.三年原厂维保服务	台	2
2.6	入侵防御	★1.核心芯片：国产化 CPU； ★2.性能要求：攻击防护性能≥20Gbps；最大并发连接数≥1000 万；每秒新建连接数≥20 万； ★3.硬件规格：标准机架式设备；千兆电口≥4 个；万兆光口≥4 个（满配光模块）； 4.功能指标： ▲集成防病毒功能； ▲支持对漏洞利用、蠕虫、木马、SQL 注入等攻击的深度检测与主动防御； 支持安全策略自定义； ▲具备完整的安全事件日志与报表功能； ★5.可靠性：支持双机热备，冗余电源； ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权。	台	2
2.7	核心交换区流	★1.核心芯片：国产化 CPU；	台	1

序号	设备类别及名称	技术规格	单位	数量
	量探针	★2.性能要求：网络层吞吐率≥20Gbps； ★3.硬件规格：标准机架式设备；内存≥32GB；硬盘≥960GB；千兆电口≥4 个；万兆光口≥4 个（满配光模块）； 4.功能指标： ★支持全流量分析与元数据提取； ★能够检测恶意文件、Web 攻击及 APT 攻击； ★支持失陷主机发现与资产识别； ★具备流量回溯与安全事件调查能力； ★5.可靠性：冗余电源； ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权。		
2.8	运维区/终端区流量探针	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐率≥1Gbps； ★3.硬件规格：标准机架式设备；内存≥8GB；硬盘≥960GB；千兆电口≥4 个；万兆光口≥4 个（满配光模块）； 4.关键功能： ★支持全流量分析与元数据提取； ★能够检测恶意文件、Web 攻击及 APT 攻击； ★支持失陷主机发现与资产识别； ★具备流量回溯与安全事件调查能力； ★5.可靠性：冗余电源； ★6.三年原厂维保服务和规则库升级	台	2
2.9	网络审计	★1.核心芯片：国产化 CPU； ★2.性能要求：吞吐量≥10Gbps； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥2TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持对网络应用协议和内容的识别与审计； ★支持文件传输行为审计； ★支持会话记录与行为回溯； ★具备完备的日志存储、检索与报表功能；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★5.可靠性：冗余电源； ★6.三年原厂维保服务和规则库升级；		
2.10	国密堡垒机	★1.核心芯片：国产化 CPU； ★2.性能要求：授权管理资产数≥3000 个；支持并发字符会话数≥2000； ★3.硬件规格：标准机架式设备；内存≥32GB；硬盘≥4TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）；内置国密卡,支持国密算法； 4.功能指标： ★支持运维操作全会话审计与录屏回放； ★支持主流数据库及远程协议代理； ★支持基于角色的精细权限划分与授权审批流程； ★具备完善的账号管理与口令策略； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。	台	1
2.11	网络准入	★1.核心芯片：国产化 CPU； ★2.性能要求：处理并发流量≥1600Mbps；支持终端授权数≥1000； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥1TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持 802.1X、Portal、端口镜像等多种接入控制方式； ★支持终端安全状态检查与动态授权； ★具备终端身份识别与行为审计功能； ★5.可靠性：冗余电源； ★6.三年原厂维保服务；	台	1
2.12	数据防泄漏系统	★1.核心芯片：国产化 CPU； ★2.性能要求：整机吞吐≥5Gbps ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥1TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持基于内容的敏感数据识别与监控；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★支持对邮件及文件传输行为进行审计与阻断； ★支持数据泄露风险分析与报表展示； ★具备灵活的响应策略与处理流程； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。		
2.13	VPN 综合安全网关	★1.核心芯片：国产化 CPU； ★2.性能要求：SSL 最大加密吞吐率≥1.5Gbps，最大并发 SSL 用户数≥10000，最大并发 SSL 用户数≥10000，提供≥1000 人授权； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥960GB；千兆电口≥6 个；千兆光口≥4 个（满配光模块）；内置国密卡或国密芯片，支持 SM2、SM3、SM4 算法； 4.功能指标： ★支持 IPsec/SSL/L2TPVPN； ★支持国密算法； ▲支持数字证书认证与精细的访问控制策略； ★具备完整的 VPN 隧道监控与用户审计功能； ★5.可靠性：支持双机热备，冗余电源； ★6.三年原厂维保服务。	台	2
2.14	核心交换区边界防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐量≥100Gbps；应用层吞吐量≥25Gbps；最大并发连接数≥800 万；每秒新建连接数≥40 万； ★3.硬件规格：标准机架式设备；双冗余电源；千兆电口≥4 个；万兆光口≥4 个（满配光模块）；业务接口扩展槽位≥1 个,100Gbps 光口≥4（满配光模块）； 4.功能指标： ▲集成入侵防御系统与防病毒引擎； 支持 IPSec/SSLVPN； ▲实现精细化的安全域划分与隔离； ▲提供基于源/目的地址、MAC 地址、应用、服务、时间等多维度的访问控制策略与包过滤能力；	台	2

序号	设备类别及名称	技术规格	单位	数量
		★5.可靠性：支持双机热备，冗余电源； ★6.三年原厂维保服务。		

3.公有云密码硬件

序号	设备类别及名称	技术规格	单位	数量
3.1	服务器密码机	★1.核心芯片：国产化 CPU； ★2.性能要求：SM1/SM4 加解密速率≥2.8Gbps；SM2 密钥对生成≥29000 对/秒；SM2 签名≥29000 次/秒；SM2 验签≥65000 次/秒；SM3 杂凑速率≥2.8Gbps； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； 4.关键功能： ★提供数据加解密、数字签名/验签、密钥全生命周期管理、消息认证等完备的密码服务； ★全面支持国密 SM1/SM2/SM3/SM4 算法及国际 RSA/AES/SHA/DES/3DES 等通用算法； ★提供 B/S 模式的图形化管理系统，实现设备监控、用户管理、策略配置与安全审计； ★支持密钥的生成、存储、备份、恢复与归档管理； ★具备高安全性的密钥存储机制与严格的访问控制策略； ★5.可靠性：冗余电源；关键部件采用高可靠设计； ★6.三年原厂维保服务；须具有商用密码产品认证证书。	台	2
3.2	时间戳服务器	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备，内存≥16GB，硬盘≥500GB；千兆电口≥2 个； ★3.性能要求：SM2 时间戳签发效率≥27000 次/秒；SM2 时间戳验证效率≥21000 次/秒； 4.功能指标： ★实现对各类电子数据的签发时间戳功能，支持多种时间戳格式，支持文件时间戳功能； ★5.三年原厂维保服务.须具有商用密码产品认证证书。	台	1
3.3	签名验签系统	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3 性能要求：SM2P1 签名性能≥80000 次/秒；SM2P1 验签性能≥30000 次/秒；SM2P7 签名性能≥20000 次/秒；SM2P7 验签性能≥40000 次/秒；SM3 摘要速率≥1Gbps； 4.功能指标： ★为信息系统提供基于数字证书的数字签名与验证服务，保障数据完整性、不可否认性及身份真实性； ★支持多种数字签名格式；支持 SM2/RSA 签名密钥、SM4 对称密钥的生成与管理； ★支持证书请求文件的生成与下载；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★支持应用实体管理与密钥、证书关联绑定； ★提供完善的密钥生命周期管理及安全审计日志； ★5.三年原厂维保服务，须具有商用密码产品认证证书。		
3.4	协同签名系统	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能指标：支持软件部署，提供 C/S 身份认证服务，协同签名≥4000 次/秒，密钥请求并发为 1000 次/s 4.功能指标： ★实现终端用户基于数字证书与移动端协同的强身份鉴别，完成多因子认证； ★采用协同签名技术，服务端与终端各持私钥分量，协同运算生成完整签名，全程不重构完整私钥； ★支持密钥安全分割与存储； ★提供标准的 API 接口供业务应用集成； ★5.三年原厂维保服务，须具有商用密码产品认证证书。	台	1
3.5	安全认证网关	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能要求：最大加密吞吐量≥1400Mbps；最大并发连接数（SM2/RSA 双向）≥50000；最大新建连接数（SM2 双向）≥5000；最大新建连接数（RSA 双向）≥12000； 4.功能指标： ★采用数字证书为应用系统提供用户管理、强身份鉴别、单点登录、传输加密、访问控制和安全审计服务； ★全面支持 SM2、SM3、SM4 等国密算法及 RSA 等国际通用算法； ★支持 CA 证书的全生命周期管理，包括导入、发布、删除及状态监控； ▲支持发布根证书、签名证书与加密证书； ▲支持清除管理后台敏感数据缓存，提升系统安全性； ▲提供基于角色和策略的精细访问控制； ★具备完备的安全审计功能，记录用户登录、资源访问及管理操作等日志； ★4.三年原厂维保服务，须具有商用密码产品认证证书。	台	1

4.云服务平台（公有云）成品软件

	序号	设备类别及名称	技术规格	单位	数量
云服务平台软件(公有云)	1	云平台管理能力	▲1.提供云主机、存储、网络、安全、容器、中间件、数据库、运营和运维等功能。 ★2.云平台管理服务器支持分别基于鲲鹏、飞腾、海光CPU部署，计算节点支持基于鲲鹏、飞腾、海光CPU部署。 ▲3.云管理平台支持软SDN，实现与硬件设备解绑。 ▲4.支持云主机弹性伸缩功能；。 ★5.按照一套并配备云平台物理机节点数量或CPU颗数的授权（永久授权，三年原厂技术支持）。	套	1
	2	云主机能力	★1.支持云主机在线扩容CPU/内存等。 ★2.支持云主机全生命周期管理和维护。 ▲3.支持为云服务器指定IP地址创建云主机。 ▲4.支持云主机按宿主机、机架物理拓扑的调度能力。 ▲5.支持对云主机实例设置标签。 ▲6.支持云主机高可用（宕机迁移）。 ▲7.支持用户通过VNC方式远程访问云主机。	套	1
	3	镜像管理能力	★1.支持对云主机的系统盘和数据盘创建整机镜像模板。 ▲2.支持将本地镜像文件上传至云平台作为自定义或共享镜像使用。 ▲3.在运维平台中可查看当前镜像列表及相关信息。	套	1
	4	云硬盘能力	★1.支持在线扩展容量，扩容期间无需关闭虚拟机。 ★2.支持磁盘的创建、删除、卸载、扩容、挂载、查询等功能。 ▲3.支持分布式EC或三副本数据冗余保护，三副本模式下，数据三副本支持分布在不同位置。 ▲4.分布式块存储服务支持在线切换EC纠删码高容量模式。 ▲5.分布式块存储支持定时快照、手动快照等多盘崩溃处理机制。 6.支持使用国密算法加密，对云盘中的数据或云盘进行加密。 ★7.配置不少于90TB的可用容量授权（永久授权，三年原厂技术支持）。	套	1
	5	云网络能力	★1.支持用户创建自己的专有网络。 ▲2.支持在控制台上针对VPC地址新增CIDR地址段的扩容。 ▲3.支持创建NAT网关，支持SNAT和DNAT配置。	套	1

			▲4.支持不同 VPC 间互通。 ▲5.支持为负载均衡、弹性公网 IP、NAT 网关和 VPC 物理专线，进行租户实例化诊断。		
	6	负载均衡	★1.七层负载均衡模式下支持配置域名或者 URL 转发策略，将来自不同域名或者 URL 的请求转发给不同的云服务器处理。 ▲2.支持为负载均衡实例设置黑名单或白名单等访问控制策略。 ▲3.负载均衡支持为监听实例设置 QOS。 ▲4.负载均衡支持 TCP/UDP/HTTP 健康检查方式。 ▲5.负载均衡支持多集群，实现基于租户集群隔离。 ★7.配置一套弹性负载均衡软件授权（永久授权，三年原厂技术支持）。	套	1
	7	云安全能力	★1.安全组规则配置时支持指定多个不连续的多个端口范围;支持安全组添加实例时显示 ip 和实例名称。 ▲2.支持云主机网络防 ARP 欺骗。 ▲3.支持进行安全组规则检测。 ▲4.安全组规则支持设置优先级，规则支持允许和拒绝的策略。	套	1
	8	运维能力	★1.云平台运维控制台支持对云管理平台多个维度运维能力 ★2.提供统一设备管理能力，统一管理包括数据中心存储、服务器、网络设备（路由器、交换机、防火墙）。	套	1
	9	运营能力	★1.提供基础数据、资源数据的概览展示。	套	1
	10	云管软件服务要求	★1.所投云平台应持有第三方机构出具的代码检测报告，代码自研率应超过 90%。 ★2.所投云平台应提供软件著作证书。 ★3.提供原厂安装服务，三年原厂维保服务。 ★4.供应商承诺中标后提供培训材料、产品手册、培训视频等相关内容。 ★5.服务有效期内供应商提供原厂级的软件更新服务。	套	1

5.公有云业务中台成品软件

序号	软件名称及类别	性能指标	单位	数量
5.1	运维管理平台	★支持监控 CPU / 内存 / 磁盘等≥30 类硬件指标，设备离线、硬件故障、软件异常响应时间≤2s，数据采集频率核心设备≤5 s；普通设备≤30s。 ★业务应用集成：通过管理协议，自动发现信息系统之间的 TCP 调用和业务系统下 IT 资源间依存关系，模型化呈现关系的构成。 ★性能检测：系统能够提供对用户访问体验和后台系统性能的全面量化和关联分析，以帮助快速识别和解决系统瓶颈。 ★IT 资源整合监控：包括中间件、数据库、服务器、网络流量、用户数据关联、性能波动分析等 IT 资源进行整合监控，实现一体化运维管理。 ★运维可视化：提供一整套数据可视化展示功能，包括 IT 基础设施、多系统关联、数据调用关系等。 ★授权：满足本项目专有云和公有云所有设备的授权需求。	项	1
5.2	无人机管理平台	★支持不少于 5000 路无人机接入的授权。 ▲最大并发接入无人机数≥500 架。 ★设备兼容性覆盖率≥98%，任务下发响应时间≤2s。 ★设备信息管理：具备对无人机基本信息的增加、删除、修改、导入功能。 ★责任人员管理：具备监管单位信息、业务人员信息管理，进行分组管理。 ★飞行计划任务管理：结合不同地市公路基础设施分布的实际情况，进行无人机飞行计划的新增、编辑、删除、上报和飞行计划任务管理。 ★数据统计展示管理：进行统计数据的汇总，飞行数据展示和设备使用情况展示，生成各种图。 ★无人机养护管理：实现照片信息的上传，巡检养护业务功能需完善增加无人机设备巡检养护信息。	项	1
5.3	融合通信平台	★增加 2000 个在线人数授权，支持离线消息推送，用户状态、会议状态监测、网络测速等功能。 ★离线消息推送：建立从云端到终端的消息推送通道，通过集成推送服务向客户端应用实时推送消息。 ★在线人数授权：新增 2000 个在线用户数。结合节点扩容支持 2000 用户同时使用。 ★网络、用户状态监测：通过报表形式展示用户的在线状态情况，增加网络测速功能，用于监测网络状况 ★会议参会信息监测：会议画面输出页面中，能够实时查看当前会议参会人的网络异常情况。	项	1
5.4	视频整合平台	★具备视频资源管理、视频接入管理、视频转发、视频协议转换等功能。 ★视频资源管理：提供所有视频资源情况概览，为满足现有需求，需增加 5 套转发节点，满足 1000 路视频并发需求。	项	1

		★视频接入管理：含 2000 路视频管理授权，将全省具备接入条件的 144 个超限监测站、执法点视频以及其他非国标协议的视频接入省级视频平台。 ★视频转发：提供高并发的流媒体转分发、标准协议能力开放、集群管理、动态扩展媒体节点功能。 ★视频协议转换：对符合标准协议的设备直接接入，对不符合标准协议的设备进行转换后接入。支持协议标准化、多级联网、调阅查看等功能		
5.5	设备管理平台	★满足 20000 台设备接入需求。 ★设备接入：支持多网络接入、多协议接入、多种接入模式、设备安全接入，设备接入模块具备证书管理、自定义协议、协议管理、设备网关等功能。 ★设备管理：设备生命周期管理：提供 API 实现设备的创建、删除、修改、查询等操作。 ▲设备管理模块主要包含设备注册中心、物模型、产品管理、设备管理、网关设备、地理位置以及固件升级。同时具备规则引擎配置，可对设备告警、规则实例进行相关配置操作。 ▲能力开放：IoT 平台提供统一的 API 接入网关，对外开放 RestfulAPI 接口，使能行业应用快速构建物联网解决方案。应用管理主要包含 OpenAPI、数据 API、API 调用统计以及用户管理实现分权分域查看。	项	1

6.公有云存储设备

序号	设备类别及名称	技术规格	单位	数量
6.1	**分布式块存储**	★1.核心芯片：国产化 CPU； ★2.计算性能：计算性能：配置 2 颗 CPU，每颗物理核数≥32 核且支持超线程，每颗主频≥2.5GHz，每颗 CPU 线程数≥64；或配置 2 颗 CPU，每颗物理核数≥48 核，每颗主频≥2.6GHz； ★3.内存配置：内存≥512GB，内存规格不低于 DDR4； ★4.存储配置：系统盘≥2 块 480GB SSD，纠删码或三副本可用容量≥30TB SSD； ★5.网络配置：≥2 块双端口 25G 以太网光口网卡（满配光模块），≥1 个带外管理口； ★6.可靠性：支持端口绑定，冗余电源、冗余风扇； ★7.三年原厂维保服务。整机为信创产品，须提供信创操作系统。	**台**	**3**

7.公有云网络设备

序号	设备类别及名称	技术规格	单位	数量
7.1	核心交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥25Tbps，包转发率≥19200 Mpps； ★3.接口：配置≥14 个 100GE 光口(满配光模块），≥12 个 25GE 光口(满配光模块），独立业务槽位≥4 个； ★4.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★5.三年原厂维保服务。	台	2
7.2	业务网交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥8Tbps，包转发率≥2000Mpps； ★3.接口：≥48 个 25G 以太网光口（满配光模块），≥8 个 100GE 以太网光口（满配光模块）； ★4.可靠性：支持 BFD 技术，实现路由协议的快速故障检测机制，支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★5.三年原厂维保服务。	台	13
7.3	千兆电口管理交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥670Gbps，包转发率≥200Mpps； ★3.接口：≥48 个千兆电口，≥6 个万兆以太网光口（满配光模块）； ★4.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★5.三年原厂维保服务。	台	6
7.4	云平台核心交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥800Tbps，包转发率≥230000Mpps； ★3.架构：独立业务槽位≥4 个，独立主控槽位≥2 个，独立交换网槽位≥6 个； ★4.接口：≥36 个 100G 以太网光口（满配光模块），≥8 个万兆以太网光口（满配光模块）； ★5.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★6.三年原厂维保服务。	台	2
7.5	外网接入路由器	★1.核心芯片：CPU、芯片均须为国产化芯片； ★2.性能要求：交换容量≥480Gbps，包转发率≥200Mpps； ★3.架构：≥2 个独立主控板，≥8 个业务槽位； ★4.接口：≥8 个万兆以太网光口（满配光模块），≥8 个千兆电口；	台	2

		★5.可靠性：支持 BFD 技术，实现路由协议的快速故障检测机制，冗余电源； ★6.三年原厂维保服务。		
7.6	**统一授时服务器**	★1.整机形态：标准机架设备； ★2.网络接口：不少于 2 个 25GE 光口（满配光模块），不少于 2 个 USB 接口，不少于 1 个 VGA 口，不少于 1 个串口； ★3.授时功能：提供纳秒级时间同步精度； ★4.时间源：同时支持北斗、CDMA、IRIG-B 码，智能切换并跟踪各时间源； ★6.性能指标：NTP 请求量不小于 14000 次/秒;客户端容量不小于 80000。	台	1

8.专有云安全成品软件

序号	设备类别及名称	技术规格	单位	数量
8.1	云安全管理平台	★1.性能指标：满足本项目租户安全设备设施的纳管； 2.功能指标： ▲下一代防火墙、Web 应用防火墙、堡垒机、综合漏洞扫描、数据库审计、日志审计、主机安全（EDR）等安全能力； ▲云安全管理平台内置云安全中心，能够汇总展示租户资产面临的安全风险，支持直接对安全风险进行响应处置； ▲云安全管理平台支持以通用授权许可的方式激活虚拟安全组件； ▲云安全管理平台支持多级架构设置云安全区域，并将租户、管理员与区域进行关联，租户可按照云安全区域选择虚拟安全组件，管理员拥有对应区域内的租户管理、设备设施管理、工单管理等权限； ▲支持安全代运维功能。 ★3.永久授权，三年原厂维保服务。	套	1
8.2	漏洞扫描	★1.性能要求：授权可并发扫描 IP 数≥64 个；支持 Web 应用、操作系统、网络设备、数据库及安全基线配置的全面扫描； 2.功能指标： ★具备不少于 200000 条漏洞特征的知识库，与国际及国内主流漏洞标准兼容； ★支持弱口令扫描，允许用户自定义密码字典与扫描策略； ★全面覆盖 SQL 注入、XSS、命令执行、文件包含、反序列化等 OWASPTOP10 核心 Web 漏洞检测； ▲支持智能流量控制； ▲可生成详尽的漏洞扫描报告，包含风险等级、详细描述及修复建议； ★3.永久授权，三年原厂维保服务。	套	1
8.3	日志审计	★1.性能要求：日志处理性能≥2000EPS；支持日志源数量≥100 个； 2.功能指标： ★支持 Syslog、SNMP、Agent 等多种日志采集方式； ★内置不少于 5000 种日志解析规则，覆盖主流网络、安全及服务器设备； 支持日志的标准化、范式化及自定义解析； ★具备基于分词算法的智能日志分析能力；	套	3

序号	设备类别及名称	技术规格	单位	数量
		▲支持实时日志检索、统计报表、关联分析及异常行为检测； 可对潜在安全威胁进行挖掘与可视化展示； ★3.永久授权，三年原厂维保服务。		
8.4	堡垒机	★1.性能要求：授权管理资产数≥600 个；支持并发字符会话数≥300； 2.功能指标： ★支持系统管理员、部门管理员、运维员、审计员等多角色精细权限划分； ▲支持旁路部署与 B/S 架构管理； ★可基于用户、资产、协议等条件设置访问控制策略，并对高危命令进行实时告警或阻断； ★支持 SSH、Telnet、RDP、VNC 等协议的 H5 化运维，无需安装本地客户端； ★支持 Oracle、MySQL、SQLServer、达梦、人大金仓等主流数据库的协议代理与操作审计； ★提供完整的会话录屏、命令记录及操作回溯功能； ★3.永久授权，三年原厂维保服务。	套	3
8.5	数据库审计	★1.性能要求：支持数据库实例数≥32 个；SQL 语句处理性能≥20000 条/秒； 3.功能指标： ★全面支持达梦、金仓、高斯等国产数据库及国外主流数据库的协议解析与行为审计； ★支持基于 SQL 注入、漏洞攻击、数据泄露、违规操作等内置规则进行实时风险检测与告警； ▲具备精细化的访问控制策略，可基于客户端 IP、数据库账号、工具、时间等多维度设置审计规则； ▲支持全量 SQL 记录，捕获并分析语句内容、执行状态、影响行数等详细信息； ▲提供智能日志分析界面，支持多维度钻取查询与可视化筛选； ★支持通过 Syslog 等标准协议将审计日志外送至第三方平台； ★3.永久授权，三年原厂维保服务。	套	3
8.6	主机安全防护	★1.性能指标：支持≥500 台云虚拟机的安全防护； 2.功能指标： ▲提供统一的中央管理控制台，实现策略统一下发、资产状态监控与安全事件集中响应； ★支持基于微隔离技术的网络访问控制，可按照 IP、端口、协议设置精细化网络策略； ★具备主机级文件传输监控与访问控制能力，支持黑白名单机制； ★集成病毒查杀与恶意代码防护功能，支持全盘扫描、快速扫描及自定义扫描任务；	套	1

序号	设备类别及名称	技术规格	单位	数量
		★提供高级威胁防护能力，可检测并阻断无文件攻击、内存攻击等新型威胁； ★支持安全基线检查与自动化合规评估； ★具备样本上报与威胁情报联动能力； ★3.永久授权，三年原厂维保服务。		
8.7	Web 应用防火墙	★1.性能要求：HTTP 防护流量≥500Mbps；HTTP 最大并发连接数≥50000；HTTP 每秒新建连接数≥4000； 2.功能指标： ▲支持对 SQL 注入、XSS、Webshell 等 Web 攻击的检测与防护； ▲支持 CC 攻击防护； ▲支持自定义安全策略与黑白名单； 具备完整的攻击日志记录与审计功能； ★3.永久授权，提供三年原厂维保服务和规则库的升级授权。	套	1
8.8	流量探针	★1.性能要求：应用层吞吐量≥1Gbps； 2.功能指标： ★基于全流量分析技术，深度检测 Web 攻击、恶意文件、DGA 域名、暴力破解、漏洞利用、数据泄露等多种网络威胁； ★利用沙箱、异常行为分析等手段，有效发现 APT 攻击、0day 漏洞利用及未知恶意代码； ★支持对加密流量进行解析与检测；具备智能告警降噪与事件聚合能力，通过实体行为分析精准定位异常主机与攻击源； ▲支持一键下钻溯源，关联原始流量包与攻击上下文； ★3.永久授权，三年原厂维保服务。	套	1
8.9	态势感知平台	★1.性能指标：全流量分析≥5Gbps、威胁检测模式≥10Gbps，数据采集和处理性能≥1.5wEPS； 2.功能指标： ▲实现实体间网络互访关系的多级钻取，支持通过端口、协议、异常访问类型、攻击链等过滤关联关系，支持实体间网络互访关系的多级钻取； ▲支持人工录入、流量自动发现、扫描发现等资产数据接入方式；流量自动发现方式能自动识别资产类型，如 Web 服务器、DNS 服务器、邮件服务器、FTP 文件服务器等多种类型资产，支持 web 业务系统发现；支持批量确认流量发现的资产；支持提供资产同步标准化接口，支持第三方通过自定义设置同步数据源进行资产	套	1

序号	设备类别及名称	技术规格	单位	数量
		同步； 自动化编排支持通过图形化界面拖拽编辑自定义剧本，编排的组件，包括标准动作、设备动作、决策、脚本、人工任务、并行节点和等待节点； ▲应对网络、主机和 Web 应用等的运行状态、常见漏洞、各种攻击行为和异常行为等进行实时监测。 ▲平台能够支持针对 IP、域名、会话进行封堵，支持主机隔离、流量牵引等方式联动设备进行封堵。 ▲应建立包括资产态势、威胁态势、漏洞态势、攻击态势、事件态势等在内的安全态势评估体系，并对其进行评估。 ▲支持智能检索语句分析，支持检索语句的中文、英文，支持逻辑运算符与字段值的自动提示补全；检索语句支持快速保存，保留检索语句历史记录；支持统计指标、规则模型、关联模型、情报模型，对实时数据进行分析与告警。 ▲集群化部署。 ★3.永久授权，三年原厂维保服务。		
8.10	云数据库审计（部署在政务云）	★1.性能指标：支持的数据库实例个数≥32 个；SQL 处理能力≥20000 条/秒； ★2.功能指标： ★支持国产数据库：DM、GBase、KingBase、GuassDB 等 ★支持 SYSLOG 方式进行审计数据外送，外送审计数据内容包括（源 IP、源端口、客户端 MAC、数据库用户名、数据库实例名等会话信息，SQL 语句或参数、记录发生事件、返回结果集、操作类型、影响行数等语句详细信息）。 ★具有内置规则，规则类型有 sql 注入、账号安全、数据泄露和违规操作等。 ★支持基于客户端 IP、数据库账号、客户端工具、MAC 地址、操作系统用户、主机名、时间配置访问规则，支持基于 SQL 注入规则、漏洞攻击规则、账号安全规则、数据泄露规则、违规操作规则进行安全审计，覆盖国内外主流数据库类型。 ★支持日志查询时分析筛选能力，根据查询条件自动分析出存在的数据库账号、客户端 IP、客户端工具、操作系统用户名、服务端 IP、操作类型、数据库名/实例名、表名、主机名、执行状态、执行时长、影响行数等，并支持在以上各个维度中灵活筛选分析。 ★3.永久授权，三年原厂维保服务。	套	7

序号	设备类别及名称	技术规格	单位	数量
8.11	云日志审计（部署在政务云）	★1.性能指标：日志源≥100，日志处理能力≥2000EPS； 2.功能指标： ★支持 syslog 日志接收转发。 ★支持在目标主机上安装 Agent 程序，采集日志。 ★内置不少于 5000 解析规则，支持不少于 5000 设备类型日志进行解析（标准化、归一化），解析规则支持自定义。 ▲支持分词算法的日志解析能力和动态激活与调整的日志解析能力。 ▲能够按照预定义的策略对指定日志源的日志进行收集、转换和筛选，支持日志查询、统计报表，可对潜在危害、异常行为、关联事件进行分析，可针对日志数据进行分析挖掘，展示日志信息中的风险状况。 ★3.永久授权，三年原厂维保服务。	套	7
8.12	流量探针（部署在政务云）	★1.性能指标：应用层吞吐量≥1Gbps； 2.功能指标： ▲支持利用网络流量分析技术、异常访问定位技术、基于 Web 的攻击检测技术、恶意文件分析技术及云端的高级分析技术来综合分析检测发现 APT 攻击。 ▲支持使用深度威胁检测技术，对 APT 攻击行为进行检测，相对于仅依靠特征检测的传统安全设备设施，可发现 0day 漏洞利用、未知恶意代码等高级攻击行为，能检测到传统安全设备无法检测的攻击，为用户提供更高级的安全保障； ▲支持检测 WEB 攻击、恶意文件攻击、远程控制、WEB 后门访问、行为分析、DGA 域名请求、SMB 远程溢出攻击、弱口令、拒绝服务攻击、隧道通信、暴力破解、挖矿、恶意工具利用、扫描行为、漏洞利用、邮件社工攻击、ARP 欺骗、密码明文形式传输等行为。 支持自动对系统告警事件降噪收敛处理，以基于实体的事件分类方式，将异常客户端 IP、安全事件发生次数进行排序展示。 ★3.永久授权，三年原厂维保服务。	套	7

9.专有云安全硬件

序号	设备类别及名称	技术规格	单位	数量
9.1	边界区防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐量≥40Gbps，应用层吞吐量≥10Gbps，最大并发连接数≥800 万，每秒新建连接数≥40 万； ★3.硬件规格：标准机架式设备。千兆电口≥4 个，万兆光口≥4 个（满配光模块）； 4.功能指标： ▲支持入侵防御及病毒防护； 支持 IPSec/SSLVPN； ▲支持安全域划分及基于地址、应用、服务、时间等多维度的访问控制策略； ▲支持实时威胁检测与日志审计； ▲具备策略路由及网络地址转换能力； ★5.可靠性：支持双机热备，双冗余电源； ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权。	台	2
9.2	数据安全交换系统	整体要求：包含数据交换前置机、数据交换后置机、安全隔离网闸 ★1.性能要求：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★2.规格要求：提供标准化的跨网数据交换接口，包括但不限于：文件交换、数据库交换、消息交换、请求服务接口、音视频代理接口等；支持基于文件特征、文件内容、文件名、病毒检测、URL 过滤、命令方法、信令动作、媒体流格式等多维度的安全检查策略。 3.数据交换前置机： ★核心芯片：国产化 CPU； ★性能指标：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★硬件规格：标准机架式设备;≥6 个千兆电口，≥2 个千兆光口（满配光模块），≥2 个扩展槽。 功能指标：交换平台前置机，通过网络安全隔离、协议剥离与重组、访问控制、内容过滤和安全认证等技术，实现边界网络和协议安全隔离，使跨网跨域业务数据和应用协议得到高安全性、可控性和可管理性。提供文件交换、数据交换、接口服务交换、消息交换、协议转换、病毒防护、访问控制、高可用集群、日志审计等功能模块。 4.数据交换后置机：	套	1

序号	设备类别及名称	技术规格	单位	数量
		★核心芯片：国产化 CPU； ★性能指标：吞吐量≥10Gbps；最大并发连接数≥150 万；系统延迟≤1ms； ★硬件规格：标准机架式设备;≥6 个千兆电口，≥2 个千兆光口（满配光模块），≥2 个扩展槽。 功能指标：交换平台后置机，通过网络安全隔离、协议剥离与重组、访问控制、内容过滤和安全认证等技术，实现边界网络和协议安全隔离，使跨网跨域业务数据和应用协议得到高安全性、可控性和可管理性。提供文件交换、数据交换、接口服务交换、消息交换、协议转换、病毒防护、访问控制、高可用集群、日志审计等功能模块。 5.安全隔离网闸。 ★核心芯片：国产化 CPU； 安全隔离网闸-外网端：标准机架式设备；≥6 个千兆电口，≥2 个万兆光口（满配光模块）；冗余电源； 安全隔离网闸-内网端：2U 机架式设备；≥6 个千兆电口，≥2 个万兆光口（满配光模块）；冗余电源； ★6.可靠性：冗余电源; ★7.三年原厂维保服务。		
9.3	安全运维管理区/终端区防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐量≥10Gbps，应用层吞吐量≥2Gbps，最大并发连接数≥200 万，新建连接数≥6 万； ★3.硬件规格：标准机架式设备，千兆电口≥4 个，万兆光口≥4 个（满配光模块）； 4.功能指标： ▲支持入侵防御及病毒防护； 支持 IPSec/SSLVPN； ▲支持多维度的安全策略及访问控制； ▲支持实时威胁检测与日志审计； ▲具备策略路由及网络地址转换能力； ★5.可靠性：支持双机热备，冗余电源； ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权。	台	2
9.4	核心交换区流量探针	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐率≥20Gbps；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★3.硬件规格：标准机架式设备；内存≥32GB；硬盘≥960GB；千兆电口≥4 个；万兆光口≥4 个（满配光模块）； 4.功能指标： ★支持全流量分析与元数据提取； ★能够检测恶意文件、Web 攻击及 APT 攻击； ★支持失陷主机发现与资产识别； ★具备流量回溯与安全事件调查能力； ★5.可靠性：冗余电源； ★6.三年原厂维保服务和入侵及防病毒规则库的升级授权。		
9.5	安全运维管理区/终端区流量探针	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐率≥1Gbps； ★3.硬件规格：标准机架式设备；内存≥8GB；硬盘≥960GB；千兆电口≥4 个；万兆光口≥4 个（满配光模块）； 4.关键功能： ★支持全流量分析与元数据提取； ★能够检测恶意文件、Web 攻击及 APT 攻击； ★支持失陷主机发现与资产识别； ★具备流量回溯与安全事件调查能力； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。	台	2
9.6	网络审计	★1.核心芯片：国产化 CPU； ★2.性能要求：吞吐量≥10Gbps； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥2TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持对网络应用协议和内容的识别与审计； ★支持文件传输行为审计； ★支持会话记录与行为回溯； ★具备完备的日志存储、检索与报表功能；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★5.可靠性：冗余电源； ★6.三年原厂维保服务。		
9.7	国密堡垒机	★1.核心芯片：国产化 CPU； ★2.性能要求：授权管理资产数≥3000 个；支持并发字符会话数≥2000； ★3.硬件规格：标准机架式设备；内存≥32GB；硬盘≥4TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）；内置国密卡或国密芯片,支持国密算法； 4.功能指标： ★支持运维操作全会话审计与录屏回放； ★支持主流数据库及远程协议代理； ★支持基于角色的精细权限划分与授权审批流程； ★具备完善的账号管理与口令策略； ★5.可靠性：冗余电源； ★6.三年原厂维保服务，须具有商用密码产品认证证书。	台	1
9.8	网络准入	★1.核心芯片：国产化 CPU； ★2.性能要求：处理并发流量≥1600Mbps；支持终端授权数≥1000； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥1TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持 802.1X、Portal、端口镜像等多种接入控制方式； ★支持终端安全状态检查与动态授权； ★具备终端身份识别与行为审计功能； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。	台	1
9.9	数据防泄漏系统	★1.核心芯片：国产化 CPU； ★2.性能要求：整机吞吐≥5Gbps；； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥1TB；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★支持基于内容的敏感数据识别与监控；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★支持对邮件及文件传输行为进行审计与阻断； ★支持数据泄露风险分析与报表展示； ★具备灵活的响应策略与处理流程； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。		
9.10	核心交换区边界防火墙	★1.核心芯片：国产化 CPU； ★2.性能要求：网络层吞吐量≥100Gbps；应用层吞吐量≥25Gbps；最大并发连接数≥800 万；每秒新建连接数≥40 万； ★3.硬件规格：标准机架式设备；双冗余电源；千兆电口≥4 个；万兆光口≥4 个（满配光模块）；100GB 光口≥4 个（满配光模块） 4.功能指标： ▲集成入侵防御系统与防病毒引擎； 支持 IPSec/SSLVPN； ▲实现精细化的安全域划分与隔离； ▲提供基于源/目的地址、MAC 地址、应用、服务、时间等多维度的访问控制策略与包过滤能力； ★5.可靠性：支持双机热备，冗余电源； ★6.三年原厂维保服务。	台	2
9.11	零信任访问控制系统	★1.核心芯片：国产化 CPU； ★2.性能要求：授权用户数≥1000 个； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥960GB；千兆电口≥2 个； 4.功能指标： ★支持多因子认证与持续风险监测； ★支持动态访问授权与网络隐身； ★具备统一的策略管理中心与用户行为分析能力； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。	套	1
9.12	情报板安全管理平	★1.核心架构：国产化 CPU；	套	1

序号	设备类别及名称	技术规格	单位	数量
	台	★2.性能要求：授权管理资产数≥6500 个； ★3.硬件规格：标准机架式设备；内存≥64GB；硬盘≥8TB；千兆电口≥2 个； 4.功能指标： ▲集中采集与关联分析各类 IoT 安全设备、终端安全设备产生的安全日志与事件； ★实现物联网资产的自动发现、识别、注册与全生命周期管理； ★具备物联网设备的安全策略统一下发、运行状态实时监测与异常行为感知分析能力； ▲支持动态绘制网络资产 IP 地址分布地图与物理/逻辑网络拓扑； ★提供资产安全风险评估、漏洞生命周期管理及合规性检查功能； ★具备统一的安全事件告警管理与应急处置流程； ★支持与全省各地市的普通公路、高速公路情报板进行适配对接； ★5.可靠性：冗余电源；支持数据本地备份与恢复； ★6.三年原厂维保服务。		
9.13	安全可视化管理平台	★1.核心架构：国产化 CPU； ★2.性能要求：全流量分析性能≥5Gbps；威胁检测性能≥10Gbps；数据采集处理性能≥15000EPS； ★3.硬件规格：标准机架式设备；内存≥256GB；硬盘≥48TB；冗余电源；千兆电口≥4 个；万兆光口≥2 个（满配光模块）； 4.功能指标： ★提供统一的网络安全态势可视化总览与运维管控界面； ★支持对全网流量、安全日志、运维告警、系统资源等多维度数据的实时采集、关联分析与监控展示； ★具备资产自动发现与画像功能，集中展示资产信息、安全状态、关联威胁及管理属性； ▲支持安全事件的一键调查与取证分析，实现事件与原始日志、流量数据的快速关联回溯； ▲支持网络安全监测、数据安全监测、安全风险评估、渗透测试、漏洞扫描、重要时期网络安全保障等能力； ★具备对已经发生的告警信息及安全事件进行分析、协调处理、保护资产等能力； ★提供自定义报表、安全大屏、策略统一下发等运维管理功能； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。	套	1
9.14	安全智能分析系统	★1.核心架构：国产化 CPU；	套	1

序号	设备类别及名称	技术规格	单位	数量
		★2.性能要求：推理速度≥30 字符/秒；支持并发处理请求数≤20 个；具备与外部算力平台对接能力； ★3.硬件规格：标准机架式设备；CPU≥2 颗*12 核；GPU 总显存≥240GB；内存≥128GB；硬盘≥32TB；万兆光口≥2 个（满配光模块）； 4.功能指标： 集成安全领域大模型，提供智能问答、逻辑推理、报告生成等 AI 能力； ▲支持自定义智能体及智能体工作流的创建与管理； ★具备识别敏感数据泄露与 API 安全风险功能； ★具备自动化分析安全告警，输出攻击定性、载荷解读与处置建议功能； ★具备多源日志关联分析，自动构建攻击链并生成调查结论功能； ★具备深度检测各类 Web 攻击与恶意代码功能； ★具备监测与分析内部运维操作风险功能等； ▲提供统一的模型管理、知识库管理与系统配置界面； ★5.可靠性：冗余电源； ★6.三年原厂维保服务。		

10.专有云密码软件

序号	设备类别及名称	技术规格	单位	数量
10.1	密码服务管理平台	★1.性能指标：支持软件部署，采用国产化软硬件环境，系统最大密钥容量≥1000 万个；SM2 最大密钥获取速率≥790TPS；SM4 最大密钥获取速率≥840TPS；SM2 最大密钥生成速率≥340TPS；SM4 最大密钥生成速率≥560TPS； 2.功能指标： ★提供统一的密码服务能力，包括密钥管理、数据加解密、数字签名/验签、安全通道、协同签名等； ★实现对云服务器密码机、签名验签服务器等多种密码资源的统一虚拟化管理与动态分配； ★支持基于多租户的密钥与运算安全隔离； ★具备完善的密钥全生命周期管理、证书管理及密码策略管理能力； ★提供对平台服务、密码资源、设备运行状态的实时监控与统计分析看板； ★支持对各类密码安全设备的集中配置与集群管理； ▲实时监控密码使用风险，管理密码设备、证书及秘钥生命周期管理（密钥生成、分发、存储、使用、更新、归档、备份、恢复和销毁等），提供加密、认证等技术支撑； ★3.三年原厂维保服务。	套	1
10.2	国密设备证书	★1.性能指标：以数字证书的方式，提供身份鉴别功能，含 CA 证书； ★2.功能指标：支持 SM1、SM2、SM3、SM4 国密算法； 3.功能指标： 提供身份认证、数据加解密、安全存储等功能； ★4.接口：提供标准的安全中间件（PKCS#11、SKF、CSP）以及 API 接口； ★5.每套证书包含 1 张设备身份 CA 证书，提供为期 3 年的证书有效期及相应的技术服务支持。	套	160
10.3	国密 SSL 证书	★1.性能指标：使用国密算法和安全协议，为网站访问提供数据机密性、完整性保护；支持通配域名，提供双证书（V1+DV）； 2.功能指标： ▲支持 SM2/RSA 双证书部署； ▲具备浏览器自适应加密能力，自动为国密浏览器启用国密算法 HTTPS 加密，为国际通用浏览器启用 RSA 算法 HTTPS 加密； ▲全面兼容各类主流浏览器及移动终端访问；	个	2

序号	设备类别及名称	技术规格	单位	数量
		★3.提供为期3年的证书有效期及相应的技术服务支持。		
10.4	国密浏览器	★1.性能指标:为终端设备提供支持国密算法的浏览器,支持SM2/SM3/SM4/SM9等国密算法及RSA/AES/SHA等国际算法; 2.功能指标: ★提供国密算法通信能力，实现与国密SSL证书的自动适配; ▲支持数字证书及CRL管理; ▲提供SSL/TLS安全传输协议支持，包括单向及双向认证; ▲具备安全策略管控、历史记录清理等安全增强功能; ★3.提供为期3年的软件功能授权及相应的技术服务支持。	套	400
10.5	个人数字证书	★1.性能指标：基于智能密码钥匙（USB-Key）的数字证书，支持SM1/SM2/SM3/SM4国密算法; 2.功能指标: ▲为个人用户提供基于数字证书的身份认证、数据加解密、数字签名等安全功能; ▲提供标准安全中间件及API接口供应用系统集成; ★3.每套包含信创版USB-Key介质1个，内置个人CA证书1张，提供为期3年的证书有效期及相应的技术服务支持。	个	3400

11.专有云密码硬件

序号	设备类别及名称	技术规格	单位	数量
11.1	服务器密码机	★1.核心芯片：国产化 CPU； ★2.性能要求：SM1/SM4 加解密速率≥2.8Gbps；SM2 密钥对生成≥29000 对/秒；SM2 签名≥29000 次/秒；SM2 验签≥65000 次/秒；SM3 杂凑速率≥2.8Gbps； ★3.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； 4.关键功能： ★提供数据加解密、数字签名/验签、密钥全生命周期管理、消息认证等完备的密码服务； ★全面支持国密 SM1/SM2/SM3/SM4 算法及国际 RSA/AES/SHA/DES/3DES 等通用算法； ★提供 B/S 模式的图形化管理系统，实现设备监控、用户管理、策略配置与安全审计； ★支持密钥的生成、存储、备份、恢复与归档管理； ★具备高安全性的密钥存储机制与严格的访问控制策略； ★5.可靠性：冗余电源；关键部件采用高可靠设计； ★6.三年原厂维保服务；须具有商用密码产品认证证书。	台	2
11.2	时间戳服务器	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能要求：SM2 时间戳签发效率≥27000 次/秒；SM2 时间戳验证效率≥21000 次/秒； 4.功能指标： ★实现对各类电子数据的签发时间戳功能，支持多种时间戳格式，支持文件时间戳功能； ★5.三年原厂维保服务，须具有商用密码产品认证证书。	台	1
11.3	签名验签系统	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能要求：SM2P1 签名性能≥80000 次/秒；SM2P1 验签性能≥30000 次/秒；SM2P7 签名性能≥20000 次/秒；SM2P7 验签性能≥40000 次/秒；SM3 摘要速率≥1Gbps； 4.功能指标： ★为信息系统提供基于数字证书的数字签名与验证服务，保障数据完整性、不可否认性及身份真实性； ★支持多种数字签名格式； ★支持 SM2/RSA 签名密钥、SM4 对称密钥的生成与管理；	台	1

序号	设备类别及名称	技术规格	单位	数量
		★支持证书请求文件的生成与下载； ★支持应用实体管理与密钥、证书关联绑定； ★提供完善的密钥生命周期管理及安全审计日志； ★5.三年原厂维保服务，须具有商用密码产品认证证书。		
11.4	协同签名系统	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能指标：支持软件部署，提供 C/S 身份认证服务，协同签名≥4000 次/秒，密钥请求并发为 1000 次/s； 4.功能指标： ★实现终端用户基于数字证书与移动端协同的强身份鉴别，完成多因子认证； ★采用协同签名技术，服务端与终端各持私钥分量，协同运算生成完整签名，全程不重构完整私钥； ★支持密钥安全分割与存储； ★提供标准的 API 接口供业务应用集成； ★5.三年原厂维保服务，须具有商用密码产品认证证书。	台	1
11.5	安全认证网关	★1.核心芯片：国产化 CPU； ★2.硬件规格：标准机架式设备；内存≥16GB；硬盘≥500GB；千兆电口≥2 个； ★3.性能要求：最大加密吞吐量≥1400Mbps；最大并发连接数（SM2/RSA 双向）≥50000；最大新建连接数（SM2 双向）≥5000；最大新建连接数（RSA 双向）≥12000； 4.功能指标： ★采用数字证书为应用系统提供用户管理、强身份鉴别、单点登录、传输加密、访问控制和安全审计服务； ★全面支持 SM2、SM3、SM4 等国密算法及 RSA 等国际通用算法； ★支持 CA 证书的全生命周期管理，包括导入、发布、删除及状态监控； ▲支持发布根证书、签名证书与加密证书； ▲支持清除管理后台敏感数据缓存，提升系统安全性； ★提供基于角色和策略的精细访问控制； ★具备完备的安全审计功能，记录用户登录、资源访问及管理操作等日志； ★4.三年原厂维保服务，须具有商用密码产品认证证书。	台	1

12.专有云数据安全

序号	设备类别及名称	技术规格	单位	数量
12.1	数据分级分类平台	★1.性能指标：不限制数据库实例； 2.功能指标： ★提供完整的结构化数据分类分级解决方案，包含自动化分类分级、人工校验打标、结果纠错等全流程管理； 深度融合大模型能力，显著提升数据识别准确率和分类效率； ★具备完善的分类分级规则库管理功能，支持内置规则库在线升级和自定义规则灵活配置； ▲集成数据源资产管理、数据库安全评估、API 接口安全管理等核心模块，实现数据安全治理闭环； ★3.交付成果：调研路网运行监测预警项目涉及重要系统的业务条线，梳理业务部门对应的关键业务流程以及业务活动，分析各业务流程涉及的关键敏感数据服务。含数据源资产管理、分类分级管理、数据库安全评估、系统数据安全管理、API 接口、数据安全展示等。完成交付数据安全分类分级规范的制订，交付《数据安全分类分级指南》《数据安全分类分级管控策略》《数据安全分类分级逻辑框架》《数据资产分类分级清单表》； ★4.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。	套	1
12.2	数据脱敏系统	★1.性能指标：不限制数据库实例； 2.功能指标： ★提供数据脱敏处理能力，支持在单个任务中完成复杂的数据脱敏流程； ▲具备脱敏任务监控和管理功能，支持任务定时调度和实时控制； ▲内置数据对比引擎，可对生产数据与测试数据、脱敏前后数据进行多维度差异分析； ★支持灵活的黑白名单策略配置，确保关键数据的正确处理； ★提供脱敏分析报告； ★3.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。	套	1
12.3	数据库安全网关	★1.性能指标：不限制数据库实例数； 2.功能指标： 支持数据库隐身技术，防止漏洞扫描； ▲支持反向代理模式部署； ★提供数据库协议控制、攻击防护、安全审计、统计分析等功能； ★支持基于运维资产、对象、人员、时间等多维度的访问控制；	套	1

序号	设备类别及名称	技术规格	单位	数量
		★支持全部数据库的安全防护与策略更新； ★3.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。		
12.4	API 安全审计系统	★1.性能指标：网络吞吐量 ≥ 5Gbps；支持接口数量无限制； 2.功能指标： ★提供 API 打标策略管理，支持基于请求方式、URL、请求头、请求体、响应码等多维度配置； ★具备 API 接口数据审计能力，可准确识别敏感数据和文件传输行为； ★支持基于 IP、账号、API 组合等多重因素的行为风险监测与配置； ★具备风险事件溯源分析功能，可追溯客户端信息、访问方式等详细信息； 支持实时风险监测和预警； ★3.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。	套	1
12.5	数据安全管理平台	★1.性能指标：支持 IPv4、IPv6 数据信息采集； 2.功能指标： ★提供智能告警聚合和自动化规则生成能力，支持自定义规则模型配置； ▲实现数据流动全过程可视化，构建完整的数据链路图谱； ★具备威胁追溯能力，可还原攻击路径和手法； 支持业务数据可视化建模，通过拖拽方式构建数据流转拓扑； ▲提供工单管理流程，支持流程和内容的全面自定义； ▲实现数据资产敏感级别统计和分析，依据行业标准进行数据安全风险评估； ★3.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。	套	1
12.6	API 安全网关	★1.性能指标：HTTP 吞吐量 ≥ 7Gbps；每秒业务请求数 ≥ 21000 TPS；最大 HTTP 并发连接数 ≥ 10 万，不限制接口数量； 2.功能指标： ★支持精准的流量控制和限速管理，支持多种限流策略灵活配置； ▲具备智能敏感数据识别能力，支持根据业务场景选择适用的脱敏算法； ▲提供细粒度的 API 安全策略管理，支持针对特定 API 和调用者配置请求/响应脱敏规则； ★确保 API 通信的安全性和合规性，防止数据泄露和未授权访问； 3.三年原厂维保服务，支持国产化环境部署，支持软件或硬件交付。	套	1

13.专有云备份硬件

序号	设备类别及名称	技术规格	单位	数量
13.1	备份存储	1.备份一体机硬件模块： ★CPU：配置 2 颗 CPU，单 CPU 主频≥2.5GHz，支持 64 位指令集，核心数≥(C86，16 核；ARM，24 核)； ★内存：≥512GB，内存规格不低于 DDR4； ★硬盘：系统盘≥2 块 960G SSD； ★网络接口：≥4*1GE 电口，≥4*25GE 光口（满配光模块）； ★配置国产化操作系统。 2.软件授权要求： ★配置不少于 256TB 定时实时备份后端容量永久授权，不限制被保护客户端数量； ★提供满足本项目所需要的灾备管理软件、高可用灾备管理软件、数据库灾备管理软件、数据副本管理软件、系统迁移软件和永久授权。 3.功能要求： ★为数据提供定时、实时保护能力，支持对目录和文件对象进行持续数据保护功能，可以恢复数据到任意时间点； ★为业务提供应急和接管能力； ★为提升数据或系统恢复效率，支持挂载恢复功能、可以实现副本数据和系统挂载和恢复使用。 4.提供原厂安装服务，三年原厂维保服务。	台	4

14.专有云存储设备

序号	设备类别及名称	技术规格	单位	数量
14.1	大数据存储服务器	★1.核心芯片：国产化 CPU； ★2.计算性能：配置 2 颗 CPU，单 CPU 主频≥2.5GHz，支持 64 位指令集,核心数≥(C86,32 核;ARM,48 核)； ★3.内存配置：内存≥384GB，内存规格不低于 DDR4； ★4.存储配置：系统盘≥2 块 480GB SSD，数据盘：≥12 块 8TB HDD，缓存盘：≥2 块 1.92TB SSD；≥1 块独立阵列卡（支持 4GB 缓存，支持 RAID0/1/5），采用存算分离架构，提供分布式存储软件授权； ★5.网络配置：≥2 块双端口 25G 以太网光口网卡（满配光模块）；≥1 个带外管理口； ★6.可靠性：支持端口绑定，冗余电源、冗余风扇； ★7.三年原厂维保服务。整机为信创产品，须提供信创操作系统。	台	4
14.2	分布式块存储	★1.核心芯片：国产化 CPU； ★2.计算性能：配置 2 颗 CPU，单 CPU 主频≥2.5GHz，支持 64 位指令集,核心数≥(C86,32 核;ARM,48 核)； ★3.内存配置：内存≥512GB，内存规格不低于 DDR4； ★4.存储配置：系统盘≥2 块 480GB SSD；数据盘：纠删码或三副本可用容量≥30TB SSD，≥1 块独立阵列卡（支持 4GB 缓存，支持 RAID0/1/5） ★5.网络配置：≥2 块双端口 25G 以太网光口网卡（满配光模块）；≥1 个带外管理口； ★6.可靠性：支持端口绑定，冗余电源、冗余风扇； ★7.三年原厂维保服务。整机为信创产品，须提供信创操作系统。	台	6
14.3	分布式对象存储	★1.核心芯片：国产化 CPU； ★2.计算性能：配置 2 颗 CPU，单 CPU 主频≥2.5GHz，支持 64 位指令集，核心数≥(C86,32 核;ARM,48 核)； ★3.内存配置：内存≥512GB，内存规格不低于 DDR4； ★4.存储配置：系统盘≥2 块 960GB SSD，缓存盘：≥2 块 1.92TB SSD，数据盘：≥36 块 20TB SATA；≥1 块独立阵列卡（支持 4GB 缓存，支持 RAID0/1/5）； ★5.网络配置：≥2 块双端口 25G 以太网光口网卡（满配光模块）；≥1 个带外管理口； ★6.可靠性：支持端口绑定，冗余电源、冗余风扇； ★7.三年原厂维保服务。整机为信创产品，须提供信创操作系统。	台	18

15.专有云网络硬件

序号	设备类别及名称	技术规格	单位	数量
15.1	参数网 ROCE 交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥25Tbps，包转发率≥10200Mpps； ★3.关键特性：支持 RoCE 功能； ★4.接口：≥64 个 200G 以太网光口或 32 个 400G 以太网光口（满配光模块）； ★5.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源、冗余风扇； ★6.三年原厂维保服务。	台	6
15.2	业务网交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥8Tbps，包转发率≥2000Mpps； ★3.接口：≥48 个 25G 以太网光口（满配光模块），≥8 个 100GE 以太网光口（满配光模块）； ★4.可靠性：支持 BFD 技术，实现路由协议的快速故障检测机制，支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★5.三年原厂维保服务。	台	26
15.3	云平台核心交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥800Tbps，包转发率≥230000Mpps； ★3.架构：独立业务槽位≥4 个，独立主控槽位≥2 个，独立交换网槽位≥6 个； ★4.接口：≥36 个 100G 以太网光口（满配光模块），≥8 个万兆以太网光口（满配光模块）； ★5.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★6.三年原厂维保服务。	台	2
15.4	千兆电口管理交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥670Gbps，包转发率≥200Mpps； ★3.接口：≥48 个千兆电口，≥6 个万兆以太网光口（满配光模块）； ★4.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★5.三年原厂维保服务。	台	8
15.5	核心交换机	★1.核心芯片：CPU、交换/转发芯片均须为国产化芯片； ★2.性能要求：交换容量≥1900Tbps，包转发率≥460000Mpps； ★3.架构：独立业务槽位≥8 个，独立主控槽位≥2 个，独立交换网槽位≥4 个；	台	2

		★4.接口：≥12 个 100G 以太网光口（满配光模块），≥96 个万兆以太网光口（满配光模块），≥48 个千兆电口； ★5.可靠性：支持链路聚合，支持环路检测、支持抑制广播风暴，冗余电源； ★6.三年原厂维保服务。		

16.云服务平台（专有云）成品软件

	序号	功能类别及名称	技术规格	单位	数量
云服务平台软件(专有云)	1	弹性云主机软件	★1.支持云主机在线扩容 CPU/内存等，无需重启即可生效。 ▲2.支持云主机全生命周期管理和维护。 ▲3.支持为云服务器指定 IP 地址创建云主机，支持配置 IPv6/IPv4 双栈网络，云主机实例可自动获取 IP 地址进行内网通信。 ▲4.支持云主机按宿主机、机架物理拓扑的调度能力。控制台上调度策略支持亲和与反亲和。 ▲5.支持对云主机实例设置标签，支持管理员根据云主机名称、私有 IP、弹性 IP、ID、运行状态、标签等条件快速查找目标云主机。 6.支持云主机高可用（宕机迁移）。 ▲7.支持用户通过 VNC 方式远程访问云主机。 8.云服务器在开启 DPDK 同时支持完整的虚拟机特性。	项	1
	2	安全组软件	★1.安全组规则配置时支持指定多个不连续的多个端口范围；支持安全组添加实例时显示 ip 和实例名称。 ▲2.支持云主机网络防 ARP 欺骗。 ▲3.安全组规则支持设置优先级，规则支持允许和拒绝的策略。	项	1
	3	快照软件	★1.支持虚拟机极速快照启用后可生成快照并可立即投入使用，打完快照后可快速回滚虚拟机。 ▲2.支持设置自动快照策略。	项	1
	4	在线迁移软件	★1.支持在控制台选择多台云主机热迁移，自定义云主机热迁移任务。	项	1
	5	裸金属服务软件	★1.支持查询裸机实例，支持根据实例名称、IP 地址信息检索裸机实例。 ▲2.支持裸机实例告警检测，查询告警信息可按筛选条件检索。 ▲3.支持对添加的裸金属实例进行资源集中监控的能力。 ▲4.支持裸机实例的创建、查询、下线、启动、删除、停止、重新启动等操作。支持设置网络 VPC、专有网络 IP 地址，支持设置 root 登录密码、重新安装操作系统等配置信息。 ▲5.支持裸机镜像管理，支持公共镜像和自定义镜像。支持公共镜像和自定义镜像导出。 ★6.支持物理机接入 VPC 网络并分配 VPC IP 地址，可以与 VPC 内资源互访，以及与外部网络互访。	项	1

	序号	功能类别及名称	技术规格	单位	数量
			▲7.具备裸机托管能力，支持查看托管实例的 cpu、内存、已使用、可使用的使用率数据指标。 ★8.支持管理多种 CPU 架构裸金属，包括但不限于飞腾、鲲鹏、海光等处理器服务器。		
	6	弹性伸缩软件	★1.支持弹性伸缩功能，根据业务的需求和策略，自动调整计算资源大小。 ▲2.支持指定待伸缩云主机实例的配置信息，包括但不限于实例规格、镜像、系统盘、数据盘等。 ▲3.支持用户定时执行伸缩规则。	项	1
	7	镜像软件	★1.支持对云主机的系统盘和数据盘创建整机镜像模板，创建的镜像包含用户的业务数据。 ▲2.支持将本地镜像文件上传至云平台作为自定义或共享镜像使用。 ▲3.在运维平台中可查看当前镜像列表及相关信息。	项	1
	8	云硬盘软件	★1.支持在线扩展容量；云硬盘在线扩容不停业务。 2.支持磁盘的创建、删除、卸载、扩容、挂载、查询等功能。 ▲3.支持分布式 EC 或三副本数据冗余保护，三副本模式下，数据三副本支持分布在不同位置。 4.分布式块存储服务支持在线切换 EC 纠删码高容量模式或支持跨资源池迁移。 ▲5.分布式块存储支持定时快照、手动快照等多盘崩溃处理机制。 ★6.配置不少于 180TB 的可用容量授权（永久授权，三年原厂维保服务）。	项	1
云服务平台软件(专有云)	9	对象存储软件	★1.支持对象的上传、下载、删除、复制，获取对象的元数据、创建多段上传任务。 ▲2.支持生命周期管理、定义和管理存储空间内所有对象或对象的某个子集的生命周期、变更容量和变更归属。 ▲3.支持客户端或服务器端加密功能。 4.分布式对象存储服务支持切换 EC 纠删码高容量模式。 ▲5.分布式对象存储租户侧支持实时日志在线查询；支持分钟级的访问、租户运维和性能监测。 ★6.配置不少于 9PB 的可用容量授权（永久授权，三年原厂维保服务）。	项	1
	10	租户网络软件	★1.支持用户创建自己的专有网络，同时支持自定义配置 IP 地址、子网、路由表。支持不同 VPC 之间的安全隔离。 ▲2.支持在控制台上针对 VPC 地址新增 CIDR 地址段的扩容。 3.支持创建 IPv4 NAT 网关，支持 SNAT 和 DNAT 配置。	项	1

	序号	功能类别及名称	技术规格	单位	数量
			4.支持不同 VPC 间互通。 ▲5.支持为负载均衡、弹性公网 IP、NAT 网关和 VPC 物理专线，进行租户实例化诊断。 ▲6.租户网络具备 DNS 功能，支持内网权威域名管理和解析；支持 IPv6 域名解析服务。		
	11	弹性 IP 软件	★1.弹性 IP 支持与多种类型的云资源进行绑定，包括但不限于：云主机、负载均衡、网卡等。用户可以在需要时将弹性 IP 绑定到所需的资源上，在不需要时将其解绑，并且可以释放不再使用的弹性 IP。	项	1
	12	弹性负载均衡软件	▲1.七层负载均衡模式下支持配置支持 UDP、TCP、HTTP、HTTPS 等多种请求转发给不同的云服务器处理。 ▲2.支持为负载均衡实例设置黑名单或白名单等访问控制策略。 ▲3.负载均衡支持为监听实例设置 QOS，且已有的监听 QOS 策略支持在线修改。 4.负载均衡支持 TCP/UDP/HTTP 健康检查方式。支持健康检查，自动隔离异常状态的后端应用服务器。 ▲5.负载均衡支持 IPv6，支持挂载 IPv4 或 IPv6 的后端应用服务器。 ▲6.负载均衡支持多集群。 ★7.配置一套弹性负载均衡软件授权（永久授权，三年原厂维保服务）。	项	1
云服务平台软件(专有云)	13	事务型关系数据库	▲1.分布式数据库兼容 MySQL 协议和语法，支持平滑扩容、服务升降配、读写分离和分布式事务等特性，具备分布式数据库全生命周期的运维管控能力。 ▲2.分层监控体系：提供实例级、数据库级、存储级分层监控指标。 ▲3.提供实例级、数据库级的备份恢复能力，实例备份支持自动备份与手动备份，备份方式包括快速备份与一致性备份。 ▲4.提供分布式数据库无间断平滑扩容功能，扩容进度支持可视化跟踪。 ▲5.提供分布式数据库的全局增量日志服务。 ▲6.提供分布式数据库的全局一致性备份，支持主动创建备份。 ★7.配置≥13 台物理机授权或≥624 物理核授权（永久授权，三年原厂维保服务）。	项	1
	14	云向量数据库	▲1.支持向量分析，衡量非结构化数据之间的相似度，实现非结构化数据（如图片、语音、文本）的高性能检索分析。 ▲2.支持地理信息系统 PostGIS。	项	1

	序号	功能类别及名称	技术规格	单位	数量
			▲3.支持对数据表常用的操作，包括：创建表、删除表、修改表名、增加列、删除列、更改列名等。 4.支持集群节点 CPU 和内存利用率、当前总链接数、IO 吞吐量、磁盘空间资源监控与告警。 ★5.配置 2 套向量型数据库授权（永久授权，三年原厂维保服务）。		
	15	容器服务	★1.容器集群检测能力，可辅助定位集群中出现的问题，提供 Pod 和节点检测。可收集节点和 Pod 信息并识别其中的异常。 ▲2.支持 Pod 资源参数动态修改，支持在不重启 Pod 的情况下，修改 CPU、内存等资源规格参数。 ▲3.支持容器镜像加速能力，支持按需加载镜像数据来显著提升应用分发及容器启动的效率。 ▲4.容器控制节点支持扩容和移除。	项	1
云服务平台软件(专有云)	16	云管软件	★1.支持查看所有云主机列表，以及实例所在的物理机和集群详情。支持根据云主机实例 ID、IP 地址查找云主机。 ★2.支持启动、停止、重启、迁移云主机。 ▲3.支持查询并查看云硬盘详情、卸载目标云主机上的云硬盘、查看操作日志、创建快照和查看快照。 ▲4.支持自定义可开通的云主机规格。 ▲5.提供数据中心存储、服务器等硬件设备的统一管理。 ▲6.提供定义配置服务能力，支撑定义授权用户、云产品服务的可用规格，管控申请、变更与释放操作。 7.应支持对国产通用算力和智能算力芯片的资源管理。 ★8.按照一套并配备云平台物理机节点数量或 CPU 颗数的授权（永久授权，三年原厂维保服务）。	项	1
	17	大数据平台管理软件	▲1.大数据计算平台支持在不同维度，包括 cpu 高负载、内存高负载、硬盘高负载、读写高负载、网络抖动等故障扰动情况下，满足功能的连续性。 ▲2.支持智能存储，利用数据冷热不均的特性对数据进行分层，基于数据访问热度、调整数据存储在 ssd、3 副本或低冗余的归档模式下进行高效数据压缩存储。 ▲3.实时计算提供完善的开发套件，提供 DDL 自动生成、数据预览功能。	项	1

	序号	功能类别及名称	技术规格	单位	数量
			▲4.提供各类底层信息展示，包括流量、资源、性能等指标。 ★5.配置不少于 24 节点管理授权（永久授权，三年原厂维保服务）。		
云服务平台软件(专有云)	18	MPP 数据仓库	▲1.采用 MPP 架构，提供大规模并行处理数据仓库服务，存储和计算能力可水平扩展，支持 PB 级数据的在线分析和离线 ETL 任务处理。 ▲2.支持对数据表常用的操作，包括：创建表、删除表、修改表名、增加列、删除列、更改列名等。 ▲3.支持集群节点 CPU 和内存利用率、当前总链接数、IO 吞吐量、磁盘空间资源监控与告警。 ▲4.支持当基表中的数据发生变化时，能够即时反映数据变化。 ▲5.支持对经常使用或复杂的查询 SQL 具备查询优化能力，支持构建流批一体的实时数仓 ★6.配置不少于 8 节点管理授权（永久授权，三年原厂维保服务）。	项	1
	19	算力管理软件	▲1.将 GPU 资源统一纳管并形成统一算力集群，实时监控硬件状态和计算负载。支持 GPU 与 CPU 等异构资源协同调度，支持虚拟化和容器化。 ▲2.支持将 GPU 算力节点接入云平台网络，方便云内入网与其他云内服务通信。支持租户专有网络管理。 ★3.配置不少于 96 个 GPU 卡授权,不少于 8 节点 ROCE 网络运维 SDN 授权（永久授权，三年原厂维保服务）。	项	1
	20	云管软件服务要求	★1.为确保平台自主可控，所投云平台应持有第三方机构出具的代码检测报告，代码自研率应超过 90%。 ★2.为确保云平台持续演进性，所投云平台应提供软件著作证书。 ★3.为确保平台稳定性，提供原厂安装服务，三年原厂维保服务。 ★4.供应商承诺中标后提供培训材料、产品手册、培训视频等相关内容。 ★5.服务有效期内供应商提供原厂级的软件更新服务。	项	1

本项目核心产品：公有云安全硬件-国密堡垒机

注：1.根据中华人民共和国财政部令第87号--《政府采购货物和服务招标投标管理办法》规定，第三十一条 使用综合评分法的采购项目，提供核心产品相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下投标的，按一家供应商计算，评审后得分最高的同品牌供应商获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会按照招标文件规定的方式确定一个供应商获得中标人推荐资格，招标文件未规定的采取随机抽取方式确定，其他同品牌供应商不作为中标候选人。

2.本项目未办理进口产品手续，不接受原装进口产品。进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品。**若所投产品为在中国境内生产的外国品牌，供应商应自行提供证明材料或承诺书，证明其所投产品不属于进口产品。**