

合同编号：SFZX-2025-051

# 省级视频云联网监测系统公有云资源 及传输网络租用（2025-2026 年度）

## 合 同 书

采购人（甲方）：陕西省高速公路收费中心

供应商（乙方）：中电信数智科技有限公司

采购人（甲方）：陕西省高速公路收费中心

统一社会信用代码：12610000737971805P

地址：陕西省西安市未央区未央路 208 号

联系人：赵妍

联系电话：029-86250115

供应商（乙方）：中电信数智科技有限公司

统一社会信用代码：91110000710928807K

地址：北京市海淀区复兴路 33 号 13 层东塔 13 层 1308 室

联系人：王瑞昕

联系电话：15399130828

双方根据《中华人民共和国政府采购法》及实施条例、《中华人民共和国民法典》和甲方采购项目有关规定，为确保甲方采购项目的顺利实施，甲、乙双方在平等自愿原则下签订本合同，并共同遵守如下条款：

### **第一条 服务内容及要求**

**（一）服务内容：**为落实部省视频联网要求，租用云运营商提供的平台服务层和基础服务层成熟资源，为省级视频云平台业务服务提供基础支撑。

1. 租用公有云资源及配套网络安全产品，服务周期为11个月；
2. 租用省中心至省级视频云平台传输链路，服务周期为11个月；
3. 提供部署迁移测试服务，云网资源开通部署、对接调试、性能测试、应用系统及数据迁移、安全保障以及日常维护巡查等。
4. 系统测评服务：对省级视频云联网监测系统进行检测，并提供权威第三方出具的检测报告。

## **(二) 服务要求**

### **1. 基本功能要求**

#### **(1) 总体要求**

云平台要在满足功能及性能要求的情况下，基于标准开源产品，国产化自研产品优先，保证系统性能提升在技术先进性方面的可延续性。

为满足部平台、公众用户对调取视频传输时延的要求，并考虑后期维护成本及便利性，并能减少对骨干通信网带宽的占用，公有云平台宜采取就近部署原则。支持通过以太网云专线从视频上云汇集点上传视频图像到云平台。应提供监控性能、并发控制等工具，由数据库管理员统一负责授权访问数据库及网络管理，实现数据安全防护。可弹性扩容，支持多处理器、多服务器的水平扩展。具有强的容错能力、错误恢复能力、错误记录及预警能力。支持存储关系型数据和对象型数据。支持网格计算和资源的虚拟化。支持主流的网络协议。

#### **(2) 云主机**

提供多种类型的弹性云主机，可满足不同的使用场景。用户可以根据业务需求自行定义弹性伸缩策略，通过可视化控制台配置定时或者周期性的监控策略。支持不同虚拟机反亲和性硬件隔离部署。支持反亲和性组或硬件隔离组。单个云主机在创建时支持设置多个网卡，并且可以设置不同的 IP 地址。支持系统盘、数据盘备份和恢复，支持实时备份，支持周期性快照，出现数据丢失时恢复至任意时间点。应支持利用省中心现有北斗授时设备进行时间同步。

#### **(3) 对象存储**

存储应采用多副本保存技术。存储可用性不低于 99.99%。

#### **(4) 数据库服务器**



应根据应用服务软件需求，安装各类主流数据库类型及版本，即开即用。应提供用于数据操作的标准应用程序编程接口（API），提供高 IO 存储类型，满足数据库读写的高性能要求。应提供监控性能、并发控制等工具，由数据库管理员统一负责授权访问数据库及网络管理，实现数据安全防护。实例采用主备架构，两个实例位于不同服务器，自动同步数据。主实例不可用时，系统会自动将数据库连接切换至备实例。可弹性扩容，支持多处理器、多服务器的水平扩展。多个用户操作同一条记录时，任何情况下读、写互不影响。支持数据库闪回技术，支持库级、表级、行级的回滚技术。支持基于共享存储的真正应用集群系统。支持数据分区优化的大数据量处理功能。具有强的容错能力、错误恢复能力、错误记录及预警能力。支持存储关系型数据和对象型数据。支持网格计算和资源的虚拟化。支持主流的网络协议。支持同构、异构数据源的访问，包括文件数据源。支持 SAS 作为数据库的二级缓存。

#### **（5）内容分发网络（CDN）**

加速节点资源丰富，提供至少 10 万级并发能力。涵盖了电信、联通、移动、教育网等主流运营商，以及多家中小型运营商。保证将用户请求精准调度至最优边缘节点，提供了有效且稳定的加速效果。支持全网 HTTPS 安全传输，网站防盗链等高级安全控制功能。接入方式简单快速，提供自助化的域名配置。支持多种可定制配置项，包括自定义防盗链、缓存策略、HTTPS 等。方便进行统计分析、日志管理、自定义缓存策略。CDN 需为视频直播加速。

#### **（6）公有云平台安全要求**

公有云平台安全保护等级高于二级（含），由云服务商结合自身云资源配置提供安全防护措施，并在本项目实施完成后出具省级云平



台独立的网络安全等级保护测评报告（不低于等保二级），应至少包含以下服务：

- (1) 安全通信网络。
- (2) 安全区域边界，包括云防火墙、边界防护、访问控制、入侵防范、恶意代码防范等。
- (3) 安全计算环境，身份鉴别与访问控制，脆弱性扫描等。
- (4) 安全管理中心，包括日志审计、流量采集、安全威胁分析等内容。
- (5) 安全管理方案，由云服务商结合自身云资源配置提供具体的安全管理方案及工具，并提供相应的服务。
- (6) 密码应用安全方案，应具备：集中化密钥管理，统一密码服务集成，国密算法全面应用，高可用的分布式部署等功能。

## **2. 基本性能要求**

### **(1) 公有云资源**

**云主机：**云主机间通信带宽不少于 10Gbps，且云主机内网地址需为 20.62.1.0/24。

①省级云平台部署 31 台云主机实现平台对接、流媒体发布、客户端应用和运行监测管理功能，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU32 核，内存 128GB，系统盘 50GB，数据盘 200GB，高 IO 性能。

②省级云平台同时部署 9 台云主机实现宏观事件分析及其他服务应用，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU32 核，内存 128GB，系统盘 50GB，数据盘 200GB，高 IO 性能。

③省级云平台另部署 11 台云主机实现基于高码流视频的微观交通识别功能，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU64 核，内存 256GB，GPU：4\*NVIDIA A10，显存 4\*24GB，系统盘 50GB，数据盘 200GB，高 IO 性能。

④省级云平台另部署 1 台云主机执行系统升级维护、系统巡检、数据备份等操作，云主机配置不低于：

X86 计算（或同等标准架构平台），CPU16 核，内存 64GB，系统盘 50GB，数据盘 200GB，高 IO 性能。

⑤陕西高管通部署 1 台云主机实现业务负载均衡应用配置，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU32 核，内存 32GB，系统盘 1TB，高 IO 性能。

⑥陕西高管通 2 台云主机实现部署业务应用服务，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU32 核，内存 32GB，系统盘 1TB，高 IO 性能。

⑦陕西高管通 1 台云主机实现数据库备份，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU4 核，内存 8GB，系统盘 1TB，数据盘：8TB，高 IO 性能。

⑧陕西高管通 1 台云主机实现执行陕西高管通系统升级维护、系统巡检、数据备份等操作，每台云主机配置不低于：

X86 计算（或同等标准架构平台），CPU16 核，内存 16GB，系统盘 500GB，数据盘：2TB，高 IO 性能。

## **面向对象存储**

采用云供应商提供的对象存储服务对截图单独进行存储，存储应采用多副本保存技术，存储可用性不低于 99.99%。存储容量不低于 20TB。采用云供应商提供的对象存储服务对陕西高管通事件图像、视频图像、业务文件等非结构化数据单独进行存储，存储应采用多副本保存技术，存储可用性不低于 99.99%。存储容量不低于 80TB。

存储桶需能够存储达到数亿级别的小文件。单月 API 请求写入需达到数亿余次，系统应能高效处理高频率的写入请求。

**文件存储：**不低于 2TB。

## **数据库服务器**

省级视频云平台数据库服务器 2 台，应采用主流硬件设备，硬件指标不低于 CPU 和内存：16 核 64GB；存储：SAS 500GB，含软件。提供 REDIS 8G 主备实例，实例采用主备架构，两个实例位于不同服务器。

陕西高管通数据库服务器 2 台，应采用主流硬件设备，硬件指标不低于 CPU 和内存：32 核 128GB；存储：SAS 3TB，超高 IO，含软件。提供 REDIS 16G 主备实例，实例采用主备架构，两个实例位于不同服务器。

## **互联网弹性出口带宽（EIP）**

省级云平台互联网弹性出口带宽租用云供应商提供的服务，上、下行带宽对等，不可与其他业务共用，且具备 60 个及以上独立互联网公网固定 IP 地址，保证每台云主机及负载均衡可单独配置一个公网 IP，至少有 4 个 EIP 配置弹性负载均衡功能。网络带宽不低于 6Gbps。

## **CDN 加速服务**



CDN 流量在流媒体服务上通过动态调度算法，高并发情况下调度 CDN 启用分发功能，提供至少 10 万级并发能力，CDN 流量包不低于 1PB。CDN 需为视频直播加速。

### **VPN 服务**

传输带宽为 5Mbps，对接部级云平台，不少于 50 连接数，满足全省全量摄像机同时控制。

**NAT 网关：**要求连接数  $\geq 10000$ 。

### **算力服务**

通过公有云 GPU 云主机提供算力服务，调用 Deepseek 等大模型能力进行高速公路视频应用定制服务。

## **(2) 安全防护**

乙方应结合自身云资源配置，提供省级云平台的网络安全保障措施，应符合网络安全等级保护不低于二级要求，出具省级云平台的等级保护测评报告。至少包括以下内容：

### **云堡垒机**

1 台，对云主机、云数据库、网络设备等的运维权限、运维行为进行管理和审计的服务。

### **云防火墙**

1 套，以虚拟主机形态，提供高性价比的云安全部署方案。提供高可用性（HA）、入侵防御（IPS）、病毒过滤（AV）、服务质量保证（QoS）等丰富功能。需能够透传客户端真实 IP。

### **日志审计**

1 套，通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息。

## **漏洞扫描**

57 套，提供主机系统漏洞发现、web 漏洞扫描、开放端口扫描、弱口令检测及配置脆弱性检测，并对扫描检测结果进行分析、形成报告，由专家提供解读及指导服务，方便管理员对主机的安全进行检查和分析，及时修复漏洞、提高系统安全防护能力。

## **DDOS 流量防护**

1 套，针对互联网服务器在遭受大流量的攻击后导致服务不可用的情况下，采用远端截流、近源清洗的方式实现流量压制。需能够透传客户端真实 IP。

## **威胁感知**

57 套，同步国家权威威胁情报源，通过对海量攻击数据的持续分析，提供漏洞情报、威胁发现、事件告警、攻击溯源、风险可视等能力，帮用户发现并看见风险，实现全生命周期安全运营。主要可实现感知安全态势、风险与实践告警、漏洞与基线检查等功能。

## **WAF**

1 套，为网站提供安全防护的服务。通过多维度防御策略，为网站拦截 SQL 注入、XSS 跨站、命令&代码注入、敏感文件访问、恶意爬虫等 Web 类型的攻击，保障您的业务安全稳定运行。需能够透传客户端真实 IP。

## **云硬盘备份**

不低于 9TB，针对云主机的系统盘、数据盘提供的备份服务。可对存储重要数据的磁盘进行备份，并在云主机磁盘故障、用户误删数据、遭到黑客攻击等情况下，将备份的数据快速恢复到源盘，最大限度保证用户数据的安全性。

## **服务器安全卫士**

57 套，功能涵盖资产清点、弱口令检测、软件漏洞检测、防暴力破解、Web 后门、反弹 shell 检测等，对云主机进行安全监测和防护，监测数据以报告的形式定期发送给用户，并对入侵等高危情况进行实时邮件通知。

### **(3) 省中心至省级视频云平台传输链路**

省收费中心至省级云平台传输链路采用以太网专线的方式实现和省级云平台链接，并采用双线路负载均衡方式连接，单个线路带宽为 3Gbps，总共 2 个线路，共计 6.0Gbps 带宽。提供从省中心到云资源池站点的二层以太网专线服务，提供接口标准为以太网接口或 E1 接口。要求链路畅通率（可用率）指标  $\geq 99.99\%$ ，承诺平均故障修复时间  $\leq 4$  小时，时延  $\leq 25\text{ms}$ 。

### **(4) 部署迁移测试服务**

组织省级视频云联网监测系统维护单位配合完成云网资源开通部署、对接调试、性能测试、应用及数据迁移、安全保障以及日常维护巡查等。配合采购人开展重点时段网络安全保障及项目相关信息、表格收集整理工作。

### **(5) 系统测评服务**

对省级视频云联网监测系统的协议符合性、运行稳定性、系统可靠性进行检测，并提供权威第三方出具的检测报告。

## **3. 交付要求**

乙方应于 2025 年 8 月 9 日前完成所有云资源、专用网络等服务内容开通，完成应用系统与数据迁移、调试对接使具备使用条件，并向中心出具开通运行、上线申请等书面交付报告，双方确认签章并以此确定服务期起始时间。

## **4. 资产要求**



乙方应在合同服务期开始后 1 个月内梳理所提供云服务的资产台账、网络拓扑、配置信息等提交甲方，并在服务时间到期前 1 个月根据情况进行更新并提交纸质资料。

## **5. 其他要求**

**(1) 保密要求：**项目实施过程中所收集、产生的所有与本项目相关的文档、资料，包括文字、图片、表格、数字等各种形式所有权均归属甲方，乙方必须对所涉及到的内容保密，乙方及服务人员应按要求签署保密协议。

**(2) 网络安全要求：**乙方具备健全的网络安全服务体系，具有网络安全隐患排查、完善加固、预警监测、应对攻击等服务能力，配备具有相关技术能力的网络安全专职人员，为本项目提供漏洞检测、策略配置、加固整改、安全监测、应急处置等保障措施，确保系统安全稳定运行。乙方未发生过重大网络安全事件，按照要求签署网络安全责任协议。

## **第二条 服务地点、时间、人员**

**(一) 服务地点：**甲方指定地点

**(二) 服务时间：**乙方为甲方提供的服务期限：为期 11 个月，2025 年 8 月 10 日-2026 年 7 月 9 日（2025 年 8 月 10 日前所有资源开通调试完成、应用系统与数据完成迁移并正常运行）。

**(三) 服务人员要求：**人员配置要求必须满足服务要求。

## **第三条 服务费用及支付方式**

1. 合同总额（含税）为人民币：贰佰柒拾玖万元整（小写 ¥2,790,000.00 元（含税价））。乙方为履行本合同而发生的所有费用均包含在合同总额中，甲方不再另行支付其他任何费用。

2. 合同签订且服务期开始后15个工作日内支付合同总额的65%(乙方须提供同等金额的银行保函),即人民币壹佰捌拾壹万叁仟伍佰元整,人民币小写1813500.00元;剩余合同总额的35%按月支付(乙方应按季度向甲方提交阶段服务报告),前10个月的每月服务费为合同总额的3.2%,即人民币捌万玖仟贰佰捌拾元整,人民币小写:89280.00元,在每月结束后15日内支付当月服务费;最后1个月的服务费,为合同总额的3.0%,即人民币捌万叁仟柒佰元整,人民币小写:83700.00元,在服务期满并验收合格后15个工作日内进行支付。

3. 乙方须于付款前10日内向甲方出具合法有效的合同全额增值税普通发票,甲方进行支付结算。乙方未提供发票的,甲方有权迟延付款,并不承担违约责任。

4. 甲乙双方各自承担因执行合同所发生的银行费用。

5. 付款方式: 银行转账

甲方开票信息:

名称: 陕西省高速公路收费中心

开户行: 中国银行股份有限公司西安边家村支行

账号: 103207335625

乙方收款账户信息:

账户名称: 中电信数智科技有限公司

开户行: 广发银行股份有限公司北京太阳宫支行

账号: 9550880244109000130

#### **第四条 甲乙双方权利和义务**

##### **(一) 甲方的权利和义务**

1. 甲方有权指派专门人员或者单位对乙方的工作进行全程监督管理,甲方认为不合理的部分有权下达整改通知书,并要求乙方限期

整改;

2. 甲方应按合同约定向乙方支付服务费用,如乙方服务未达到合同要求,甲方有权拒付未达到要求部分的款项,对甲方造成的经济损失,甲方有权要求乙方进行经济赔偿;

3. 甲方有权要求乙方提供与相关服务内容有关的相关信息;

4. 甲方有权得到符合合同要求的所有服务;

5. 乙方完成所有协议约定内容后,甲方根据项目实施情况出具的客观公正的书面用户验收意见;

6. 国家法律、法规所规定由甲方承担的其它责任。

## (二) 乙方的权利和义务

1. 合作过程中乙方应指派专门的业务负责人负责合作事项的全程沟通及协调工作;

2. 乙方应遵守甲方有关合作事项的各项管理规定,及时报告工作进度,在规定时间内完成相应工作;

3. 甲方在工作质量、工作进度、工作内容等方面提出意见及建议,乙方应及时响应并有效改进,乙方应配合甲方或甲方组织的对本合同履行情况的监督与检查,对于甲方指出的问题,应及时作出合理解释或予以纠正;

4. 不得转包、分包;

5. 乙方为甲方提供7x24业务咨询及故障处理服务,当服务内容和  
服务要求内的设备发生故障时,乙方应及时采取有效措施排除故障,  
恢复正常运行,服务期内云平台、链路及相应服务正常使用率不低于  
99%;

6. 服务期满后,乙方应无条件返还甲方向其提供的文件、资料并向甲方移交本系统的全部相关资料,同时乙方应当自留一份完整的项



目档案并予以妥善保存。

7. 国家法律、法规所规定由乙方承担的有关责任。

## **第五条 违约责任**

1. 交付违约责任：乙方如不能按时依照合同约定提供相应服务并完整交付的，每逾期一日的，乙方应按照合同总价款的万分之一向甲方支付违约金；乙方逾期一个月仍无法按合同要求提供服务或提供虚假材料，或质量不能满足技术要求的，甲方有权解除合同，甲方解除合同的，乙方应按照本合同总价款的10%向甲方支付违约金。

2. 网络安全违约责任：

乙方应做到以下要求：

(1) 彻底清理系统隐患。全面排查清理系统网络安全隐患，确保中高危隐患彻底清零。

(2) 全面摸清现网资产。全面摸清系统资产，形成资产台账，定期维护更新资产，确保资产信息准确。

(3) 彻底消除口令问题。定期开展口令隐患排查，严格系统密码存储管理，确保口令问题彻底消除。

(4) 及时升级安装补丁。定期开展漏洞扫描、渗透测试等工作，及时升级系统存在漏洞的软件，安装最新补丁和杀毒软件，确保系统软件升至最新版本。

(5) 强化系统监测能力。充分利用现有监测平台或借助第三方监测手段做好软件/设备状态监测，及时感知并处置异常网络安全行为，确保系统安全运行。

(6) 加强系统安全防护。选用技术能力强、安全业务精湛、经验丰富、责任心强的人员做好系统安全防护，采取切实有效的措施，能够及时发现系统异常攻击行为，做好系统安全防守。

(7)做好日常管理工作。完善运维机制，规范运维程序，形成运维记录，做好设备日常巡检、加强意识技能培训开展安全专项服务、备份系统数据配置、做好监测预警处置等日常网络安全工作。

若乙方因上述(1)至(7)条款落实不到位，造成部、省、公安、中心等有关部门通报时，发现并通报1次，每发生一次乙方应向甲方支付违约金5000元；造成网络安全事件时，将按照国家，部、省、中心网络安全相关规定，根据造成的实际损失、影响，上报有关部门同时进行责任追究。

3. 乙方若违反本协议的任何一款，视为乙方违约；因乙方违约造成甲方损失的，由乙方承担全部的损失赔偿责任，包括但不限于直接经济损失及甲方因此开支的交通费、公证费、鉴定费、诉讼费、仲裁费、律师费、保全费、保全保险费等一切费用。

4. 乙方应支付给甲方的违约金，甲方有权在任意一笔应支付给乙方的款项中予以扣除而无需征得乙方同意。

## **第六条 争议的解决**

1. 合同一经签订，不得擅自变更、中止或者终止合同。对确需变更、调整或者中止、终止合同的，应按规定履行相应的手续。

2. 双方在协议履行过程中所发生的一切争议，双方应本着友好的原则协商、调解解决。协商、调解未果，任何一方均可向甲方所在地人民法院即西安市未央区人民法院起诉。

3. 双方一致同意若因本合同项下争议以诉讼方式解决纠纷时，人民法院及甲乙双方向各方送达相关法律文件的送达地址为本合同列明的地址，法律文书到达时，无论是否签收，都视为送达完成。

## **第七条 验收条款**

乙方所提供服务应遵循中华人民共和国及地方的有关法律规定，达到甲方使用要求，由甲方组织验收。

1. 验收依据：（1）竞争性磋商文件；（2）磋商响应文件；（3）合同文本；（4）国家有关的验收标准及规范。

2. 验收标准：服务期满后，乙方应完成过程资料整理并形成服务总结，书面通知甲方进行验收。甲方在接到申请并核验资料齐全后15个工作日内，组织会议，对乙方提供服务情况进行验收，并形成验收意见。

## **第八条 免责条款**

1. 由于甲方造成的任何数据丢失、机密外泄，乙方不承担任何责任。

2. 因不可抗力导致甲乙双方或一方不能履行或不能完全履行本合同项下有关义务时，甲乙双方相互不承担违约责任。但如遇有不可抗力的一方或双方应于不可抗力发生后15日内将情况告知对方，并提供有关部门的证明。在不可抗力影响消除后的合理时间内，一方或双方应当继续履行合同。

## **第九条 合同生效及其他**

1. 本合同经甲乙双方负责人、法定代表人或授权代表签字并加盖公章后生效；

2. 本合同中所带的附件，具备合同本身同样的法律效力；

3. 本合同一式捌份，其中，甲方肆份，乙方肆份。均具有同等法律效力。

4. 本合同未尽事宜，双方以补充合同完善。

5. 合同签约地：西安市未央区未央路208号。



(以下无正文)

甲方：陕西省高速公路收费中心  
(盖章)

负责人(授权代表): 略红

签订日期: 2025 年 6 月 25 日

乙方：中电信数智科技有限公司  
(盖章)

法定代表人(授权代表):

签订日期: 2025 年 6 月 25 日

李忠

## 附件1

## 租用资源服务清单

| 序号   | 设备(主、材)名称     | 单位 | 数量 | 备注                                                                                                                 |
|------|---------------|----|----|--------------------------------------------------------------------------------------------------------------------|
| 一    | 公有云资源租赁       |    |    | 租用期限为期 11 个月                                                                                                       |
| 1    | 省级云平台         |    |    |                                                                                                                    |
| 1.1  | 云主机           | 台  | 31 | 部署平台对接、流媒体发布、客户端应用和运行监测管理功能, X86 计算(或同等标准架构平台), CPU32 核, 内存 128GB, 系统盘 50GB, 数据盘 200GB, 高 IO 性能                    |
| 1.2  | 云主机           | 台  | 9  | 部署宏观事件分析及其他服务应用, X86 计算(或同等标准架构平台), CPU32 核, 内存 128GB, 系统盘 50GB, 数据盘 200GB, 高 IO 性能                                |
| 1.3  | 云主机           | 台  | 11 | 部署基于高码流视频微观交通分析应用, X86 计算(或同等标准架构平台), CPU64 核, 内存 256GB, GPU: 4*NVIDIA A10, 显存 4*24G, 系统盘 50GB, 数据盘 200GB, 高 IO 性能 |
| 1.4  | 云主机           | 台  | 1  | 执行系统升级维护、系统巡检、数据备份等操作, X86 计算(或同等标准架构平台), CPU16 核, 内存 64GB, 系统盘 50GB, 数据盘 200GB, 高 IO 性能, Windows Server 系统        |
| 1.5  | 云主机           | 台  | 1  | 陕西高管通负载均衡主机。32 核 32G 系统盘: 1TB, 高 IO。                                                                               |
| 1.6  | 云主机           | 台  | 2  | 陕西高管通业务应用主机。32 核 32G 系统盘: 1TB, 高 IO。                                                                               |
| 1.7  | 云主机           | 台  | 1  | 陕西高管通数据备份主机, 4 核 8G 系统盘: 1TB 数据盘: 8TB, 高 IO                                                                        |
| 1.8  | 云主机           | 台  | 1  | 陕西高管通 windows 远程运维主机, 16 核 16G 系统盘: 500GB 数据盘: 2TB, 高 IO 性能, Windows Server 系统                                     |
| 1.9  | 面向对象存储 (20TB) | 项  | 1  | 存储视频截图, 多副本保存技术, 存储可用性不低于 99.99%。存储桶需能够存储达到数亿级别的小文件。单月 API 请求写入需达到数亿余次, 系统应能高效处理高频率的写入请求。                          |
| 1.10 | 面向对象存储        | 项  | 1  | 提供面向对象存储 80TB, 存储陕西高管通                                                                                             |

|      |                          |   |    |                                                                                                              |
|------|--------------------------|---|----|--------------------------------------------------------------------------------------------------------------|
|      | (80TB)                   |   |    | 非结构化数据。存储桶需能够存储达到数亿级别的小文件。单月 API 请求写入需达到数亿余次，系统应能高效处理高频率的写入请求。                                               |
| 1.11 | 文件存储 (2TB)               | 项 | 1  |                                                                                                              |
| 1.12 | 数据库服务器                   | 台 | 1  | CPU16 核，内存 64GB，存储 SAS 500GB，含软件。实例采用主备架构，两个实例位于不同服务器。                                                       |
| 1.13 | 数据库服务器                   | 台 | 1  | 一主两备架构，32 核 128G 内存，数据盘 3TB，超高 IO。存储陕西高管通结构化数据                                                               |
| 1.14 | 数据库服务器                   | 台 | 1  | 提供 REDIS 8G 主备实例                                                                                             |
| 1.15 | 数据库服务器                   | 台 | 1  | 提供 redis 主备架构，16G 内存。用于陕西高管通业务数据缓存。                                                                          |
| 1.16 | 互联网弹性出口带宽 (EIP) (6Gb ps) | 项 | 1  | 不可与其他业务共用，且具备 60 个及以上独立互联网固定 IP 地址(原则上每台云主机可分配一个 EIP)。至少有 4 个 EIP 配套有负载均衡功能。                                 |
| 1.17 | CDN 加速服务(1PB)            | 项 | 1  | 用户视频直播加速 CDN 流量包 (高并发时采用 CDN 分发功能)                                                                           |
| 1.18 | VPN 服务 (5Mbps)           | 项 | 1  | 对接部级云平台，不少于 50 连接数                                                                                           |
| 1.19 | NAT 网关                   | 台 | 1  | 内外网地址映射，连接数不少于 10000                                                                                         |
| 2    | <b>网络安全保障</b>            |   |    | 云服务商应结合自身云资源配置，提供省级云平台的网络安全保障措施，应符合网络安全等级保护不低于二级要求，出具省级云平台的等级保护测评报告。                                         |
| 2.1  | 云堡垒机                     | 台 | 1  | 对云主机、云数据库、网络设备等的运维权限、运维行为进行管理和审计的服务。                                                                         |
| 2.2  | 云防火墙                     | 套 | 1  | 以虚拟主机形态，提供高性价比的云安全部署方案。提供高可用性(HA)、入侵防御(IPS)、病毒过滤(AV)、服务质量保证(QoS)等丰富功能。需能够透传客户端真实 IP。                         |
| 2.3  | 日志审计                     | 套 | 1  | 通过主被动结合的方式，实时不间断地采集用户网络中各种不同厂商的安全设备、网络设备、主机、操作系统、以及各种应用系统产生的海量日志信息。                                          |
| 2.4  | 漏洞扫描                     | 台 | 57 | 提供主机系统漏洞发现、web 扫描、开放端口扫描、弱口令检测及配置脆弱性检测，并对扫描检测结果进行分析、形成报告，由专家提供解读及指导服务，方便管理员对主机的安全进行检查和分析，及时修复漏洞、提高系统安全防护能力。需 |



|     |           |    |    |                                                                                                                 |
|-----|-----------|----|----|-----------------------------------------------------------------------------------------------------------------|
|     |           |    |    | 能够透传客户端真实 IP。                                                                                                   |
| 2.5 | DDOS 流量防护 | 项  | 1  | 针对互联网服务器在遭受大流量的攻击后导致服务不可用的情况下,采用远端截流、近源清洗的方式实现流量压制。                                                             |
| 2.6 | 威胁感知      | 套  | 57 | 同步国家权威威胁情报源,通过对海量攻击数据的持续分析,提供漏洞情报、威胁发现、事件告警、攻击溯源、风险可视等能力,帮用户发现并看见风险,实现全生命周期安全运营。主要可实现感知安全态势、风险与实践告警、漏洞与基线检查等功能。 |
| 2.7 | WAF       | 套  | 1  | 为网站提供安全防护的服务。通过多维度防御策略,为网站拦截 SQL 注入、XSS 跨站、命令&代码注入、敏感文件访问、恶意爬虫等 Web 类型的攻击,保障您的业务安全稳定运行。需能够透传客户端真实 IP。           |
| 2.8 | 云硬盘备份     | TB | 9  | 针对云主机的系统盘、数据盘提供的备份服务。可对存储重要数据的磁盘进行备份,并在云主机磁盘故障、用户误删数据、遭到黑客攻击等情况下,将备份的数据快速恢复到源盘,最大限度保证用户数据的安全性。                  |
| 2.9 | 服务器安全卫士   | 套  | 57 | 功能涵盖资产清点、弱口令检测、软件漏洞检测、防暴力破解、Web 后门、反弹 shell 检测等,对云主机进行安全监测和防护,监测数据以报告的形式定期发送给用户,并对入侵等高危情况进行实时邮件通知。              |
| 二   | 租用专用网络    |    |    | 租用期限为 11 个月。                                                                                                    |
| 1   | 省中心以太网专线  |    |    |                                                                                                                 |
| 1.1 | 3Gbps 带宽  | 项  | 1  | 省中心至省级云平台以太网专线,双线路负载均衡。链路畅通率达到 99.99%以上。                                                                        |
| 1.2 | 3Gbps 带宽  | 项  | 1  |                                                                                                                 |
| 三   | 部署测试迁移    | 项  | 1  | 提供资源开通部署、对接调试、性能测试、应用及数据迁移、安全保障以及日常维护巡查等服务。                                                                     |
| 四   | 系统测评服务    | 项  | 1  | 对省级云平台的协议符合性、运行稳定性、系统可靠性进行检测,并提供权威第三方出具的检测报告。                                                                   |

## 附件 2

# 网络安全责任协议

陕西省高速公路收费中心（以下简称“甲方”）委托中电信数智科技有限公司（以下简称“乙方”）进行省级视频云联网监测系统公有云资源及传输网络租用（2025-2026年度）服务，为加强信息系统网络安全管理工作，保障系统安全稳定运行，按照《中华人民共和国网络安全法》规定，网络安全等级保护及部、省网络安全有关要求，结合《陕西省高速公路收费中心信息系统网络安全管理办法》，经甲乙双方友好协商，签订本网络安全责任协议：

### 第一条 术语定义

- 1、本协议甲方关键岗位为系统管理员、安全管理员、审计管理员。
- 2、本协议乙方关键岗位为参与系统设计、开发、测试、运维等系统全生命周期的所有相关人员。

### 第二条 总体要求

双方要贯彻落实网络安全法律法规，认真执行交通运输部、省委省政府、省交通运输厅和甲方的网络安全规章制度，落实网络安全责任，把网络安全工作纳入重要工作，明确网络安全关键岗位人员及职责，开展关键岗位人员背景审查，与关键岗位人员签订网络安全责任书和保密协议，共同保障系统安全稳定运行。

### 第三条 建设要求

- 1、新建、升级改造的系统，乙方提供的硬件、软件和服务，要符合国家法律、行政法规的规定以及强制性国家标准要求，并通过权威机构的安全认证。

2、新建、升级改造的系统或现有系统新增功能上线前，乙方要委托具有网络安全相关专业能力的机构进行安全检测，安全检测要至少包括系统部署环境评估、安全漏洞扫描、基线配置核查、渗透测试、代码安全审计五方面内容，出具安全检测报告，向甲方报送安全检测报告并提供系统资产清单（所有运行需要使用的软件、插件、进程、IP、端口等）后，系统或新增功能方可正式上线。

3、乙方要严格按照软件工程规范、系统安全需求进行业务应用系统设计开发，不得在程序代码中植入后门、隐蔽信道和恶意代码，同时要关闭高危端口，与业务无关的端口、进程和服务。

#### **第四条 服务要求**

1、乙方要制定完善网络安全服务规范，建立更新系统资产台账，形成系统网络拓扑图，清理已被替换的老旧系统、未关停的测试系统、废弃无用系统等“僵尸系统”，确保资产信息全面准确。

2、乙方要定期开展系统网络安全意识教育和专业技能培训，提升工作人员网络安全意识和技能，从事甲方安全服务人员要具备漏洞检测、策略配置、加固整改、安全监测等技术能力，能够熟练使用网络安全常见产品和工具。

3、乙方要定期开展漏洞扫描、配置核查、渗透测试等系统自查行动，建立漏洞隐患清单，彻底消除口令问题，严格密码存储管理要求，确保中高危隐患清零。

4、乙方要保存系统基础配置信息，留存的系统相关日志不少于六个月，并定期对日志进行审计分析，严格控制运维工具使用，规范日常运维操作行为，形成运维过程相应表单记录。

5、乙方要及时清理离职离岗人员权限，按照最小化原则进行账号授权，及时升级安装最新补丁和杀毒软件，确保系统软件升至最新



版本。

6、乙方要加强系统介质管理，严格介质使用要求，杜绝专网设备违规外联，严格边界访问控制，定期核查优化安全策略。

7、乙方要严格落实国家和行业对数据和个人信息保护相关要求，建立数据访问管理清单，做好数据备份存储工作，定期检查数据有效性，采取脱敏处理及存储加密等安全措施，确保个人信息安全。

8、乙方要加强系统安全风险预警响应，积极利用已有监测方式、第三方监测手段或自行开发的脚本，做好系统异常行为监测，及时处置告警信息，确保系统正常运行。

### **第五条 责任追究**

若乙方未落实本网络安全责任协议内容或因防护不当、未及时发现攻击行为，造成部、省、公安、网信等有关部门通报，发现并通报1次，扣除服务费5000元；造成网络安全事件时，将按照国家、部、省、甲方等网络安全相关规定，根据造成的实际损失、影响，上报有关部门，同时进行责任追究。

### **第六条 争议解决**

双方友好协商解决本协议中的争议。协商不成的，任何一方都有权向甲方所在地人民法院即西安市未央区人民法院提起诉讼。

### **第七条 法律适用、协议文本及效力和变更**

1、本协议适用中华人民共和国的法律。

2、本协议未尽事宜按国家有关法律法规、行业和甲方有关规定执行。

3、本协议的任何修改必须经过双方协商一致，并以书面方式确认方为有效。

4、本协议经双方法定代表人、负责人或授权代表签字并加盖单

位公章后生效。

(以下无正文,为双方签章处)

甲方: 陕西省高速公路收费中心

乙方: 中电信数智科技有限公司

(盖章)

(盖章)

负责人(授权代表):

路红

法定代表人(授权代表):

李忠

日期: 2025 年 6 月 25 日

日期: 2025 年 6 月 25 日

## 保 密 协 议

甲方与乙方签订《省级视频云联网监测系统公有云资源及传输网络租用（2025-2026年度）》合同。为了在项目实施的过程中，使甲乙双方的保密信息、知识产权和相关的合同信息不受到侵害。为此甲、乙双方在履行本协议时，均应遵守《中华人民共和国保守国家秘密法》和《反不正当竞争法》等法律规定，并严格按照以下条款定开展工作：

### 一、保密内容

1、乙方需要保密内容：乙方在履行合同的过程中所获悉的甲方提供的系统信息资产台账、系统网络拓扑信息、系统配置信息、系统运行的数据等，以及经甲方声明需要保密信息。

2、甲方需要保密内容：乙方在服务中使用的流程、方法以及乙方声明需要保密的其他信息。

### 二、保密信息的使用

1、甲方应指定专门的项目协调人员配合乙方工作，乙方在履行合同过程中如需了解或获取甲方相关资料或信息，应向甲方项目协调人员索取。

2、甲方项目协调人员应做好保密信息管理及调研情况的记录工作，乙方应予以配合。

3、乙方可按以下方式获取信息：书面、交付项目、启动信息存取（如存在数据库中的信息）。

### 三、保密的范围

1、乙方只在本项目需要时才能使用甲方提供的秘密信息。乙方应将甲方提供信息的使用限制在与本项目有关的人员、保密协议签署



者范围内。

2、甲方应将乙方在本项目中使用到的流程和方法等技术信息限制在与本项目有关的人员、保密协议签署者范围内。

#### **四、保密义务**

- 1、未经许可不得获取对方与本次工作无关的秘密信息；
- 2、不得向任何第三方披露、转让或协助使用上述秘密信息；
- 3、如发现上述秘密被泄露或者自己过失泄露，应当采取有效措施防止泄密进一步扩大，并及时向对方报告；

4、凡未经对方书面同意，一方以直接、间接、书面、口头等形式为第三方提供第一条保密内容的行为均属违反保密义务的行为。但以下情况不属于违反保密义务：

- 4.1 获取或披露一方已公开发表，或已为公众所知的信息；
- 4.2 获取或披露一方已书面授权公开的信息；
- 4.3 获取的信息属于一方通过合法手段从第三方在未受到任何限制的情况下获得的；
- 4.4 根据法律、法规，司法或行政命令的要求向有关国家机关提供他方的秘密信息，提供前必须经过双方的书面认可。

#### **五、保密期限**

甲、乙双方确认，双方的保密义务从本协议签署之日起生效。自本合同生效之日起算，保密期限为无限期。

#### **六、违约责任**

1、如果一方不履行本协议第四条所规定的保密义务，应当承担给对方造成的直接损失的赔偿责任，并承担合同金额20%的违约金。

2、因一方的违约行为侵犯了另一方的合法权益，对方可以选择根据本协议要求其承担违约责任，或者根据国家有关法律、法规要求

其承担侵权责任。

3、任何一方及其工作人员未按照本协议约定使用保密信息或者泄露保密信息而触犯有关法律，一方都可以有权按照本条的规定取得赔偿，还将依法追究另一方的行政及刑事责任。

### 七、争议的解决

甲乙双方友好协商解决本协议中的争议。协商不成的，任何一方都有权向甲方所在地人民法院即西安市未央区人民法院提起诉讼。

### 八、法律适用、协议文本及效力和变更

1、本协议适用中华人民共和国的法律。

2、本协议的任何修改必须经过双方协商一致，并以书面方式确认方为有效。

3、本协议经双方负责人/法定代表人或授权代表签字并加盖单位公章之日起生效。

(以下无正文，为双方签章处)

甲方：陕西省高速公路收费中心  
(盖章)

负责人(授权代表): 路红

日期: 2025 年 6 月 25 日

乙方：中电信数智科技有限公司  
(盖章)

法定代表人(授权代表):

日期: 2025 年 6 月 25 日