合同编号：GSJCA2500357EGN00

金昌市电子政务外网有线网络服务

政府采购服务项目合同

金昌市财政局政府采购
合同备案专用章
合同备案号:2025JCSCGHTBA000275

GSJCA2500357EGN00

甲方：金昌市大数据中心

乙方：中国电信股份有限公司金昌分公司

GSJCA2500357EGN00

金昌市电子政务外网有线网络服务政府采购服务项目合同

甲方：金昌市大数据中心

乙方：中国电信股份有限公司金昌分公司

根据《中华人民共和国政府采购法》《中华人民共和国民法典》等法律法规的规定，甲乙双方本着公平、自愿的原则，按照《金昌市电子政务外网有线网络服务政府采购服务项目招标文件》（招标文件编号：2025JCSCGJHBA204）《金昌市电子政务外网有线网络服务政府采购服务项目响应文件》以及中标（成交）通知书（中标编号：D03-126203000735957384-20250429-000002-6）签订本合同。

第一条　项目服务内容及要求

1.1 网络专线接入服务

1.1.1 网络专线服务

市城域网核心节点到市级各部门、单位专线服：提供市城域网核心节点到市级各部门、单位专线链路，提供使用双芯双向点对点专线接入，链路必须符合接入带宽：市级各部门、单位接入带宽≥500M。

互联网出口专线接入：提供互联网出口链路专线接入，链路上联端口必须具备≥3G带宽服务能力，采用光口方式直接接入市行政中心机房。

市城域网核心节点到金昌市紫金云大数据中心和城市云专线服务：提供市行政中心到金昌市紫金云数字政府运营指挥中心12芯光纤，后期根据单位机构调整和场地搬迁随时调整。

1.1.2 网络规划服务

目前金昌市电子政务外网有线网络服务虽然完成了网络的规划及IP地址的划分，但随着网络规模的不断扩大，应用系统的不断扩容，原有的规划已经不能满足目前网络结构优化及扩充的需求，需要对网络的整体及安全重新进行规划部署。此次规划在原有的基础上，需从以下4个方面对网络规划与标准规范进行完善。

网络整体规划：对电子政务外网进行分层设计，包括组网、接入、网管中心、安全、网站、数据运行和管理中心和网络服务等方面内容的整体规划；按照统一的网络安全策略和安全等级，制定政务外网与其他政务专网的互联互通以及政府各部门网络的互联规划，提出规划分步实施的方案。需重新针对原有县区或镇级的链路规划，并按照行政区域来进行接入。

域名规划：参照国办政府部门域名命名的规则，针对政务外网的特点，按行政区划和政府部门进行规划与设计。

路由规划：规划骨干路由、接入路由、VPN路由、多协议标签交换虚拟专网（MPLSVPN）路由的规划原则和实施方案。

标准规范体系建设：遵循国家统一的标准，提出金昌市电子政务外网急需的网络、安全、数据、管理等方面的标准与规范。

LAN设计：VLAN是将LAN内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个LAN内隔离广播域的技术。当网络规模越来越庞大时，局部网络出现的故障会影响到整个网络，VLAN的出现可以将网络故障限制在VLAN范围内，增强了网络的健壮性。

划分方式，先分业务VLAN、管理VLAN和互联VLAN；按照业务区域划分不同的VLAN；同一业务区域按照具体的业务类型（如：Web、APP、DB）划分不同的VLAN；VLAN需连续分配，以保证VLAN资源合理利用；预留一定数目VLAN方便后续扩展。

VLAN规划，按照业务功能划分VLAN范围，如：

政府场所：VLAN10～119；

各部门接入：VLAN120～199；

事业单位接入：VLAN200～299；

相关网络接入：VLAN1000～1199。

按照逻辑区域划分VLAN范围，如：

广域骨干核心网络：10～110；

城域网：1100～1199，1201～129……2400～2499，14个地市各划分一段；

核心服务器：200～290，预留300～999。

IP地址规划：统一规划金昌市电子政务外网的IP地址，网络的骨干和边界原则上使用正式IP地址，保留各部门专网已经使用的地址，各部门已建专网和依托政务外网平台运行的业务系统通过地址翻译（NAT）或其他方法实现互联互通和信息共享。

为了便于IP地址统一运维管理，统一规划和统一分配IP地址，保留和优化市级政务外网IP地址，采用私网IP地址规化，通过Nat技术访问internet，节约公网地址。同时考虑未来IPv6改造过渡，所选设备应支持IPv4和IPv6双栈。

IP地址是动态IP或静态IP的选取原则如下：

原则上服务器，特殊终端设备（打卡机，打印服务器，IP视频监控设备等）和生产设备建议采用静态IP。

办公用设备建议使用DHCP动态获取或采用静态IP，如办公用PC、IP电话等。

IP地址规划原则。唯一性：一个IP网络中不能有两个主机采用相同的IP地址。即使使用了支持地址重叠的MPLS/VPN技术，也尽量不要规划为相同的地址。连续性：连续地址在层次结构网络中易于进行路

径叠合，大大缩减路由表，提高路由算法的效率。扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。实意性："望址生意"，好的IP地址规划使每个地址具有实际含义，看到一个地址就可以大致判断出该地址所属的设备。

IP地址基本分类：Loopback地址，为了方便管理，为每一台路由/交换设备创建一个Loopback接口，并在该接口上单独指定一个IP地址作为管理地址。

Loopback地址务必使用32位掩码的地址。最后一位是奇数的表示路由器，是偶数的表示交换机，越是核心的设备，Loopback地址越小。

互联地址：互联地址是指两台网络设备相互连接的接口所需要的地址，互联地址务必使用30位掩码的地址。核心设备使用较小的一个地址，互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。依照电子政务外网规模对整网预留三个C类地址池作为互联地址使用。

业务地址：业务地址是连接在以太网上的各种服务器、主机所使用的地址以及网关的地址，业务地址规划时所有的网关地址统一使用相同的末位数字，如："．254"表示网关。

市、县、区汇聚交换机下接入的网段可能有很多，在规划的时候需要考虑路由聚合，可以B类地址或/18～/20地址进行汇聚，这样可以减少核心网络的路由数目。

1.1.3 市广域骨干网服务

根据电子政务外网相关标准规范，金昌市电子政务外网广域网纵向贯通省、市、县区的全省统一网络基础平台，市、县区需各提供2台广域网核心路由器，负责开通电子政务外网业务。广域网核心路由器节点采用双核心设备，县区级需通过双链路、1000M带宽上联至市

广域网核心路由器骨干节点，市级需通过双链路、万兆带宽上联至省广域网核心路由器骨干节点，充分保障广域网骨干网络的可靠稳定性。

广域网由上联省广域骨干网，下联市级骨干网。组建广域网应满足适应大容量与突发性通信的要求、适应综合业务服务的要求、开放的设备接口与规范化的协议、完善的通信服务与网络管理。为了更好的提高整体网络的高可靠性，部署双链路组网。由市级广域路由器下联至市城域路由器及县区接入路由器。路由器具有判断网络地址和选择IP路径的功能，它能在多网络互联环境中，建立灵活的连接。路由器是整体网络的主要结点设备。路由器通过路由决定数据的转发。通过部署路由器，使数据传输能力更快、更好。

优化金昌市电子政务外网的核心、汇聚、接入层，与市级统一互联网出口：

优化政务外网市级统一互联网出口及完善互联网出口安全涉及的网络设备，满足等保相关要求。

新增网络设备支持IPv4/IPv6双栈部署，并支持MPLS、SRv6和EVPN技术。互联网出口区设备均支持IPv4/IPv6双栈，并需要在互联网出口防火墙和骨干环路由器部署NAT64功能进行IPv4和IPv6地址的转换，从而使互联网用户和部门、单位用户可以通过IPv6地址访问这些服务器。

汇聚层：部署汇聚设备，用于各部门、单位业务的统一接入汇聚。

本次金昌市电子政务外网项目有线网络服务，需要确保网络切换过程中尽量不影响各单位政务业务的正常开展。

1.1.4 市城域网服务

为保障金昌市电子政务外网城域网网络支撑及服务能力，市电子

政务外网城域网总体网络架构需采用具备高扩展性的双星型架构，实现核心层全冗余和高速连接，确保核心层稳定可靠高效地运行。城域网区是整个电子政务外网的核心区域，连接市、县/区各级网络、各单位接入、互联网接入、政务云平台、安全运维管理区等。核心区域部署边界防火墙，做边界隔离，连接各区域，旁挂探针等系统，保证网络对威胁的实时了解性。

市级城域网与省级广域网互联，以及内部安全域边界应部署防火墙，实现网络边界保护和访问控制。防火墙应仅开放必需的服务端口，对网络数据进行访问控制，采取有效的边界访问控制策略。为提高网络可靠性，防火墙应双机部署，并支持IPv4、IPv6会话信息记录、可溯源。

金昌市电子政务外网城域网是在市级管理区域内连接广域网、互联网、云以及市级单位的城域网络。根据网络功能划分为核心路由交换区域、互联网出口区域、政务云互联区域、市级单位接入区域、安全接入区域、运维管理区域等6个功能区域。

1.1.4.1 核心路由交换区域

核心路由交换区域提供2台城域网核心路由器和2台高性能核心交换机，负责城域网内互联以及数据路由转发。

城域网核心路由器采用40G链路上联广域网核心路由器。2台核心交换机之间分别通过40G链路聚合互联，实现核心层全冗余和高速连接，确保核心层稳定可靠高效地运行。核心交换机采用40G链路上联城域网核心路由器。核心设备全部配置冗余引擎和冗余电源系统，以满足系统高可靠的要求。每台设备配置多个40G和10G端口，与电子政务外网出口、政务云、运营商设备等互联。

1.1.4.2 互联网出口区域

互联网出口区域是金昌市本级电子政务外网各个单位用户访问互

联网的统一出口，县区在进行县本级城域网优化时也应分别统一互联网出口。

本次采用双链路上联至运营商互联网，通过链路负载均衡设备和集中NAT技术方式进行互联网访问。互联网出口方向部署2台链路负载均衡设备采用双活模式部署。

两台链路负载均衡各用1个万兆网络接口与多运营商互联采用双链路冗余方式，部署基于目的地址的策略路由，完成不同运营商目标主机互联网业务访问。

根据等级保护基本要求，电子政务外网互联网出口设备必须采用高性能防火墙作为出口的安全隔离设备，隔离互联网和电子政务外网的内部网络，保证跨安全域的访问都能通过防火墙进行控制管理，并能在网络出口处实现入侵防范功能。同时还应该在互联网出口处进行优化控制，保证用户访问选择最优的链路。因此，本期在互联网出口区域部署2台互联网出口防火墙、2台抗Ddos攻击防护设备、1台入侵防御和2台防病毒网关。

此外，在互联网出口处进行流量控制，保证网络发生拥堵的时候优先保护重要的主机。根据公安部等级保护基本要求，所有用户访问互联网需要部署上网行为管理系统，并保存3个月的日志。因此，互联网出口区域还需部署上网行为管理设备实现对内部用户访问互联网的上网行为进行监控、日志进行记录。

本次电子政务外网规划的互联网出口承载的主要为各办公节点访问互联网的流量，政务云单独规划有互联网出口承载公众通过互联网访问政务系统的流量。根据调研情况，金昌市各市级单位现有互联网终端数量超过6000台。本期电子政务外网互联网出口初期带宽按照3G专线出口考虑，未来再随着各部门接入电子政务外网后出口带宽的使用情况，再适时对租赁的出口带宽进行调整。

1.1.4.3 政务云互联区域

根据金昌市电子政务外网有线网络服务整体规划，金昌市大部分政务系统都需承载于政务云上。政务事项的办理和审批都要依托于电子政务外网与政务云进行数据交互。电子政务外网与政务云的互联需要可靠稳定的大容量带宽，以保证政务系统的正常运行。

1.1.4.4 市级单位接入区域

市电子政务外网服务纵向实现与国家、省、区（县）的互联互通，横向上实现市本级党政机关部门的全覆盖。构建完善的网络，承载未来数字政府多种业务场景应用。

市城域网核心节点到市级各部门、单位专线链路服务，需提供使用双芯双向点对点专线接入，链路必须符合接入带宽，市级各部门、单位接入带宽≥500M，要求所有线路独享专线带宽，不得与其它接入用户共享线路及带宽资源，后期根据各单位机构调整和场地搬迁随时调整。

为保证各市级单位接入电子政务外网的便捷性，同时考虑未来网络的灵活扩展性，本期在每个市级单位及有需求的二级单位分别各配置1台接入网关，城域网中新建2台各部门、单位接入汇聚交换机，用于各部门、单位的接入。

对于市行政中心的各部门、单位，通过市行政中心的汇聚交换机汇聚后上联单位接入交换机。同时新增楼层接入交换机，对市行政中心内的接入网络进行优化。对于已启用IPv6地址段的部门、单位，本次专门配置59段单位接入交换机。各市级单位的接入由市里统筹考虑，通过租赁运营商双芯双向点对点专线实现。

1.1.4.5 安全接入区域

本次电子政务外网优化除了有线城域网优化，还包括无线城域网接入的安全服务。本次设立安全接入区，部署防火墙、入侵检测、沙

箱、VPN网关等，实现无线城域网接入的安全保护

1.1.4.6 运维管理区域

考虑到新建网络的运维管理，本次单独设置运维管理域运维管理区部署2台运维管理域交换机，采用万兆链路上联核心交换机，运维管理的相关系统设备全部接入运维管理交换机下。

1.1.4.7 市行政中心网络优化服务

市行政中心网络工程优化服务，连接骨干传输网，优化各楼层交换机及内部综合布线。

市行政中心旧网段优化：早期存在部分旧网段为一个网段，包含众多接入使用单位，且同处一个广播域中，需重新优化设计，以提高网络整体运作效率和安全性能。

1.2 网络安全服务

1.2.1 统一安全防护体系优化服务

按照分级优化、分级管理的原则，构建全市统一的电子政务外网平台安全等级保护体系。通过提供市级政务网络平台安全防护体系服务，各级各部门负责建立本级、本部门政务外网安全防护体系，制定网络安全防护责任制度，确保政务外网基础设施、重要信息资源、重点业务系统的安全。

金昌市电子政务外网安全体系总体要依据国家《电子政务外网安全建设规范》的思路并符合等级保护的基本要求，金昌市电子政务外网至少达到等级保护相关要求。在此基础上结合当前电子政务外网的安全现状，从安全技术、安全运营管理、安全运维三个方面开展安全服务，打造运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、安全可闭环的电子政务外网安全体系。

1.2.1.1 市级城域网边界安全

市级城域网与省级广域网互联，以及内部安全域边界应部署防火

墙，实现网络边界保护和访问控制。防火墙应仅开放必需的服务端口，对网络数据进行访问控制，采取有效的边界访问控制策略。为提高网络可靠性，防火墙应双机部署，并支持IPv4、IPv6会话信息记录、可溯源。

1.2.1.2 互联网出口安全

互联网出口需遵循国家电子政务外网安全规范要求，满足高可用的链路双向负载均衡服务，提供精细化的安全防护和带宽管理服务，应部署防拒绝服务攻击设备、防火墙、负载均衡设备、入侵防御系统、VPN网关，日志审计系统等安全设备。

1.2.1.3 安全运营管理要求

打造统一安全防护体系，完善安全基础设施服务、提升高级威胁检测能力、提升安全体系联动闭环的能力。管理体系需要升级；运维的技术手段相对传统，运维工作量较大的问题。安全运营管理系统包括电子政务外网安全态势感知系统、安全日志系统、漏洞扫描系统和安全控制管理系统，实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力。

安全接入区服务：需提供路由器、防火墙、入侵检测、沙箱、VPN网关、探针等服务内容，实现网络接入的安全保护。

安全运维管理区服务：需提供边界防火墙、接入交换机、网络安全态势感知系统、日志审计系统、安全准入平台、网络管理平台、安全管理中心、漏洞扫描系统、僵木蠕检测系统、杀毒软件系统、堡垒机等服务，实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力。

等保三级服务：按照等级保护三级要求统筹规划优化电子政务外网安全体系，提升安全基础防御能力的水平，金昌市电子政务外网有线网络需达到等级保护三级要求，并通过专业机构评测。本次安全体

系应完善政务技术、管理、运维三大体系建设、提升新型威胁检测能力、打造联动闭环的技术体系。

1.2.1.4 电子政务外网安全态势感知系统

电子政务外网安全态势感知系统用以对网络安全进行监测与预警，实现网络安全的系统，因此系统通过采集资产、网络通信、计算环境、业务应用、脆弱性、安全事件、运行状况、审计日志和威胁情报等数据，然后进行数据融合，利用融合后的数据分析网络行为以及用户行为等因素所构成的整个网络当前状态和变化趋势，获取、理解、回溯、显示能够引起网络态势变化的安全要素，预测网络安全态势发展趋势。系统组成包括网络安全态势感知要素采集，数据预处理、网络安全态势特征提取、态势评估、态势预测和态势展示等，提供全市政务新媒体安全监测服务。

安全日志系统：安全日志系统作为信息系统的综合性管理平台，通过对客户网络设备、安全设备、主机和应用系统日志进行全面的标准化处理，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营安全；同时提供集中化的统一管理平台，将所有的日志信息收集到平台中，实现信息资产的统一管理、监控资产的运行状况，协助管理员全面审计信息系统整体安全状况。

漏洞扫描系统：漏洞扫描系统需要支持扫描操作系统漏洞、数据库漏洞、网络设备漏洞、防火墙漏洞、Web系统漏洞、登录弱口令、系统配置核查等功能，并且能为系统管理员提供漏洞的详细报告和解决方案。漏洞扫描系统需要支持资产自动发现功能，支持远程自动升级以及本地升级最新漏洞库。

安全管理控制系统：安全管理控制系统主要提供安全业务编排和策略统一管理。通过安全管理控制系统联动态势感知分析平台实现威

胁检测结果自动转化为安全策略，并将安全策略下发到安全设备，实现安全设备的闭环联动处置。

1.2.2 市级统一互联网出口优化服务

加强市本级各部门的局域网服务，完善和规范电子政务外网接入方式，确保各单位电子政务外网局域网安全、正常运行。统一市本级各单位互联网出口，加强互联网网络安全管理。

互联网出口需遵循国家电子政务外网安全规范要求，满足高可用的链路双向负载均衡服务，提供精细化的安全防护和带宽管理服务，应部署防拒绝服务攻击设备、防火墙、负载均衡设备、入侵防御系统、VPN网关，日志审计系统等安全设备。

金昌市电子政务外网市级统一的互联网出口，作为政务用户提供互联网访问通道，同时承载政务部门面向企业和公众服务的互联网业务，如政府单位门户网站、公众服务系统、服务器远程访问等。市级统一互联网出口包括主备两个出口，提高互联网出口的可靠性。

市级统一互联网出口可为市级政务单位用户提供互联网服务，原则上市各部门、单位不再保留单独的互联网出口。

互联网出口区作为政府办公人员访问互联网的出口，同时也是政府出差人员通过互联网访问政务外网办公系统的入口，对安全性有着较高的要求，金昌市级政务外网出口安全按本文安全要求内容进行。

互联网区是各级政务部门安全接入互联网的网络区域，满足各级政务部门使用互联网的需要。在互联网区，要求采取综合的安全防护措施，平滑升级负载均衡、防病毒网关、上网行为管理等安全设备，增加互联网链路负载均衡、抗Ddos设备、出口防火墙、入侵防御系统、防病毒网关等设备，对互联网接入提供安全防护。为了防止一台设备出现意外故障而导致网络业务中断，互联网出口区采用两台防火墙形成双机备份，以防火墙作为边界隔离，均采用万兆链路连接至互

联网出口区，满足各接入单位互联网使用需求。既能保证网络单点故障，又能有效保证网络带宽需求。按照国家统一的安全策略，分级接入互联网，提供互联网业务服务。县、区外网需独立部署统一互联网出口，满足县、区各单位及学校对互联网的需求，采取NAT技术，通过静态路由连接本地互联网。

本次互联网出口链路专线接入服务，链路上联端口必须具备≥3G带宽服务能力，采用光口接入方式直接接入市行政中心机房。互联网出口上联至运营商网络，必须独享上下对等的光纤专线，不能包含运营商的局域网内带宽,线路质量稳定可靠，并能很好解决各运营商之间互联互通问题。

1.2.2.1 路由部署

互联网出口路由器配置静态默认路由，或通过BGP从运营商路由器学习互联网路由；城域核心通过IGP或IBGP从出口路由器学习默认路由。

1.2.2.2 NAT及负载均衡

出口防火墙，配置公网地址池，进行IPv4公私网地址转换。使用多运营商出口的网络启用负载均衡功能，将对外访问流量按照运营商IP地址归属或自定义策略进行路径优化和带宽优化。

1.2.2.3 安全设备部署

部署IPS入侵防御设备，实现对应用层网络僵尸木马等类型的攻击的防护；部署防火墙实现安全区域隔离和访问控制，部署沙箱实现对APT威胁防御，部署抗Ddos设备实现Ddos攻击防御；出口路由器配置StrictuRPF，用于防止基于源地址欺骗的网络攻击行为。按照中华人民共和国电子政务外网部令第82号要求，应加强和规范互联网安全技术防范，保障互联网网络安全和信息安全，提升电子政务外网网络安全审计能力。日志审计的功能直接由防火墙对接日志审计设备来实

现，日志审计设备部署在运营管理区。

1.2.2.4 安全接入平台

为满足各部门、单位人员移动政务应用（如移动办公）的需求，在互联网出口区部署安全接入平台，支持IPSec和SSLVPN，确保各部门、单位人员通过互联网安全接入到政务外网，使用移动政务系统。

1.2.3 统一管控平台优化服务

目前电子政务外网运维模式仍是采用传统网络的运维管理方式。当设备故障时出现告警后运维人员需要进行网络故障情况判定并处理，运维手段比较传统落后。全网设备虽然互联连接在一起，但没有实现统一管理和安全联动，只能依靠技术人员逐台设备管理。涉及到具体设备配置时，需要telnet到具体设备的界面通过指令进行查看或运维，在运维层面缺乏智能化和平台化的管理手段。通过优化智能网络统一管控平台，实现电子政务外网业务可视化，直观显示接入终端类型、设备运行状态、链路质量、链路流量、故障告警等。

网络管理从以下几个方面进行设计，一方面是对设备的管理，另一方面是针对业务的管理，因为数据承载网是运营级的网络，对VPN等业务的管理能力是更为关注的特性，同时考虑分级分权管理，优化运维管理层次。

a.拓扑集中监视;

b.精确故障管理;

c.设备配置文件管理;

d.管理数据可靠;

e.业务网管功能;

f.智能运维。

1.3 运营维护服务

1.3.1 市行政中心机房环境优化服务

优化市行政中心1至6号机房和1号机房监控室基础设施环境，提供完善的维修服务和售后服务，对机房空调系统、UPS供配电系统、监控系统等，作为重点运行维护内容，同时对机房内的其他指标项进行检测，如机房内温度、湿度、消防系统、机房环境等，为电子政务外网运行提供安全稳定的机房环境，主要有以下内容:

机房监控设备维护管理：供配电监测系统、空调环境检测系统、门禁设备系统、漏水检测。

UPS不间断电源系统维护：负责所有机房UPS的维护、故障诊断检修和器件更换等工作。负责UPS系统、蓄电池的维护保养、一般性故障处理维护、电池充放电管理维护；负责蓄电池配套的电池开关盒、汇流盒、电池架开关盒及连接电缆等的维护、保养、更换。

电气配电系统维护：负责所有机房配电柜的器件和柜体维护。器件包括所有柜内切换机构模块、空气开关、脱扣控制器、输入输出排、电气监控传感器、电量仪以及配电系统的末端工业连接器、连接线缆、PDU等。

机房消防设备维护管理：负责灭火剂的控制装置等的维护以及灭火器药剂的更换。

环境监控系统维护：负责所有机房环境监控系统的所有部件、监控平台软件的保养、维护。

机房电气系统维护：负责所有机房电器（照明、应急照明、开关、插座）保养、维护。

机房环境：机房环境：清理机房的杂物，将机房物品定置；清洁机房门窗、地面。定期清洁电池室的地面；检查机房所有与外界的空洞是否已严密封堵，严密防鼠；检查机房玻璃、地板、天花板、通气口，墙体表面是否正常，外观是否完好，有否出现老化现象；检查机房是否有漏水现象；检查机房墙壁是否有渗水现象；填写巡检记录，

有问题及时报告。

空调系统维护：负责所有机房精密空调系统室内外机组的所有部件、空调管线及单独布设的温湿度传感器的保养、维护，并负责两台华为精密空调的保养、维护、维修、更换等。

机房供水及排水水路、电路及照明线路的维护管理：水、电路管线及接口的检查。

机房基础维护管理：机柜线路的整理、标签检查更换、机房除尘清洁及有关配套的维护管理。

机房主机设备维护管理：负责网络设备（路由及交换设备等）的维护、管理、维修、更换等。

机房运行维护管理体系建设：完善机房运行维护规范，优化机房运行维护体系。

防雷接地维护：定期检查接地系统，防止接地系统腐蚀，确保接地系统连接可靠性，规范接地系统布线，定期测量接地电阻，防止雷击危害。

提供全市电子政务外网有线网络各设备设施的日常运行、维护、网络安全保障、应急处置等工作，制定各项运行维护规章制度和应急预案，定期开展电子政务外网网络安全风险评估和应急演练，做好日常值班值守、机房和线路巡检、应急处置、故障处理、安全防护及日志记录，建立协同联动的网络安全监测与通报机制，及时处置安全事件，提升电子政务外网网络安全防护和应急处置能力。

将分散在各个机房的动环监测设备统一接入电信云网监控调度中心，设备包括但不限于温湿度传感器、烟雾探测器、门禁系统、UPS电源等，实现全天候24小时的专业化监控，通过集中化、智能化的监测手段，确保机房动力环境系统的稳定运行，提高故障响应速度和处置效率，从而保障整个IT基础设施的可用性和安全性。

提供所有机房视频监控维护服务，确保监控系统稳定运行，实时保障行政中心安全，服务涵盖视频监控设备的日常巡检、故障排查、维修更换等，同时提供统一汇聚解决方案，实现监控数据的集中管理和高效分析。

提供机房门禁出入记录服务，可实时记录人员出入情况，为机房安全管理提供有力数据支撑，大幅增强机房安全防护能力。

备注：1号机房是指行政中心1#楼1楼101，2号机房是指1#楼负1楼A05，3号机房是指4#楼4楼421，4号机房是指4#楼4楼417，5号机房是指6#楼4楼401，6号机房是指6#楼1楼123，1号机房监控室是指行政中心1#楼1楼103。

1.3.2 电子政务外网完善的售后服务

金昌市电子政务外网广域网纵向贯通省、市、县的全省统一网络基础平台，提供市、县/区各提供2台广域网核心路由器服务，负责开通电子政务外网业务。广域网核心路由器节点采用双核心设备，区/县级通过双链路、1000M带宽上联至市广域网核心路由器骨干节点，市级通过双链路、万兆带宽上联至省广域网核心路由器骨干节点，充分保障广域网骨干网络的可靠稳定性。

金昌市电子政务外网城域网总体网络架构采用具备高扩展性的双星型架构，核心路由交换区提供2台城域网核心路由器和2台高性能核心交换机服务，负责城域网内互联以及数据路由转发。同时为保证各市级单位接入电子政务外网的便捷性，考虑未来网络的灵活扩展性，在每个市级单位及有需求的二级单位提供接入网关服务，用于各部门、单位的接入。

安全接入区服务，提供防火墙、入侵检测、沙箱、VPN网关等，实现无线城域网接入的安全保护服务。

互联网接入区服务，采用双链路上联至运营商，通过链路负载均

衡设备和集中NAT技术方式进行互联网访问。根据等级保护基本要求，电子政务外网互联网出口设备需采用高性能防火墙作为出口的安全隔离设备，隔离互联网和电子政务外网的内部网络，保证跨安全域的访问都能通过防火墙进行控制管理，并能在网络出口处实现入侵防范功能。同时还应该在互联网出口处进行优化控制，保证用户访问选择最优的链路。此外，在互联网出口处进行流量控制，保证网络发生拥堵的时候优先保护重要的主机。根据公安部等级保护基本要求，所有用户访问互联网需要部署上网行为管理系统，并保存3个月的日志。因此，互联网出口区域还需部署上网行为管理设备实现对内部用户访问互联网的上网行为进行监控、日志进行记录。

提供电子政务外网市广域网核心节点到省广域网核心节点10G出口链路专线的运维服务、市广域网核心节点到县广域网核心节点专线运维服务及市广域网核心节点到区广域网核心节点主干链路运维服务，并确保线路线路质量稳定可靠。

提供7*24小时提供电话或网络报障服务，能够提供包括重大故障及事件预警。如由于线路检修、设备搬迁、工程割接、网络及软件升级等可预见的原因，影响或可能影响市级部门、单位使用该光纤电路接入服务的，应至少提前48小时告知采购人并提供相关预案。在接到市级各部门、单位网络故障申报后，需在1-4小时内解决，并给予处理报告。

支撑金昌市电子政务外网有线网络服务项目设备及设施，必须满足附件二相关参数要求。

1.3.3 驻场服务

提供三人以上专属驻场服务团队驻场式服务，并提供7*24小时全市电子政务外网运维服务，保证全市电子政务外网正常运行，驻场人员必须能够熟练操作所有设施设备，能及时有效处理各类故障，需为

驻场人员购买意外伤害保险等人身保险及社会保险。

1.4 本项目服务清单如下:

金昌市电子政务外网有线网络服务政府采购服务项目服务清单

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
一、网络专线接入服务						
1	市城域网核心节点到市级各部门、单位专线服务	1.要求提供市城域网核心节点到市级各部门、单位专线链路及提供使用双芯双向点对点专线接入，链路必须符合接入带宽：市级各部门、单位接入带宽≥500M。 2.要求所有线路独享专线带宽，不得与其它接入用户共享线路及带宽资源。 3.线路质量稳定可靠，电路可用率≥99.9%；网络平均丢包率≤0.01%，吞吐率100%；传输时延≤20ms，最大延迟≤64ms。 4.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求，后期根据各单位机构调整和场地搬迁随时调整。	项	1	1500000	1500000
2	互联网出口专线接入	1.要求提供互联网出口链路专线接入，链路上联端口必须具备≥3G带宽服务能力，具备光口方式直接接入市行政中心机房。 2.互联网出口上联至运营商网络，必须独享上下对等的光纤专线，不能包含供应商的局域网网内带宽，线路质量稳定可靠，并能很好解决各运营商之间互联互通问题。 3.互联网接入链路必须独享、不再复用，不得通过接入商缓存、cache等类似设备，且为双向全线速专线，电路可用率≥99.9%；端到端电路丢包率≤0.01%，吞吐率100%；端到端的电路传输时延≤10ms。 4.供应商无故障运行时间≥99.9%。 5.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求。	项	1	1000000	1000000

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
3	市城域网核心节点到金昌市紫金云大数据中心和城市云专线服务	1.要求提供市城域网核心节点到金昌市紫金云数字政府运营指挥中心12芯光纤接入，链路必须符合接入带宽，链路带宽≥1G，后期根据单位机构调整和场地搬迁随时调整； 2.要求提供市城域网核心节点到金昌市城市云服务平台双芯双向专线接入，链路必须符合接入带宽，链路带宽≥10G，后期根据单位机构调整和场地搬迁随时调整； 3.要求所有线路独享专线带宽，不得与其它接入用户共享线路及带宽资源； 4.线路质量稳定可靠，电路可用率≥99.9%；网络平均丢包率≤0.01%，吞吐率100%；传输时延≤20ms，最大延迟≤64ms； 5.专线接入服务质量必须保证采购人现有应用的互通性和兼容性要求。	项	1	312000	312000
二、网络安全服务						
1	市级城域网边界安全服务	市级城域网与省级广域网互联，以及内部安全域边界提供防火墙服务，实现网络边界保护和访问控制，防火墙开放必需的服务端口，对网络数据进行访问控制，采取有效的边界访问控制策略，提高网络可靠性，提供防火墙双机部署服务，并支持IPv4、IPv6会话信息记录、可溯源。	项	1	650000	650000
2	安全接入区服务	要求本次提供安全接入区服务，提供路由器、防火墙、入侵检测、沙箱、VPN网关、探针等服务内容，实现无线网络接入的安全保护。	项	1	740000	740000
3	互联网接入区安全服务	互联网出口需遵循国家电子政务外网安全规范要求并满足高可用的链路双向负载均衡服务，提供精细化的安全防护和带宽管理服务，提供防火墙、负载均衡设备、链路负载均衡、抗Ddos、探针、汇聚交换机、防病毒网关、入侵防御系统、上网行为管理、网络流量分析系统等安全服务。	项	1	900000	900000

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
4	安全运维管理区服务	根据金昌市电子政务外网的安全现状，从安全技术、安全管理、安全运维方面开展建设，打造运营平台化、管理一体化、态势可感知、事件可预警、事故可追溯、技术大融合、安全可闭环的网络安全体系。按照等级保护三级要求统筹规划电子政务外网安全体系，提升安全基础防御能力的水平，金昌市电子政务外网有线网络达到等级保护三级要求，并通过专业机构评测。本次安全体系建设应完善政务技术、管理、运维三大体系建设、提升新型威胁检测能力、打造联动闭环的技术体系。全面解决架构缺乏整体设计、安全架构缺乏协同、技术手段孤岛。完善安全基础设施服务，提升高级威胁检测能力、提升安全体系联动闭环的能力，提供边界防火墙、接入交换机、网络安全态势感知系统、日志审计系统、安全准入平台、网络管理平台、安全管理中心、漏洞扫描系统、僵木蠕检测系统、杀毒软件系统、堡垒机等服务实现电子政务外网的全网威胁可视化、通报预警和统一安全运营能力，并对全市政务新媒体进行安全监测。	项	1	1386000	1386000
5	等保三级服务	按照等级保护三级要求统筹规划建设电子政务外网安全体系，提升安全基础防御能力的水平，金昌市电子政务外网有线网络达到等级保护三级要求，并通过专业机构评测。	项	1	100000	100000
三、运营维护服务						
1	市行政中心机房环境优化服务	优化市行政中心1至6号机房和1号机房监控室基础设施环境，提供完善的维修服务和售后服务，对机房空调系统、UPS供配电系统、监控系统等，作为重点运行维护内容，同时对机房内的其他指标项进行检测，如机房内温度、湿度、消防系统、机房环境、防雷接地等，为电子政务外网运行提供安全稳定的机房环境，主要有以下内容： 1.机房监控设备维护管理：供配电监测系统、空调环境检测系统、门禁设备系统、漏水检测。 2.UPS不间断电源系统维护：负责所有机房UPS的维护、故障诊断检修和器件更换等工作。负责UPS系统、蓄电池的维护保养、一般性故障处理维护、电池充放电管理维护；负责蓄电池配套的电	项	1	500000	500000

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
		池开关盒、汇流盒、电池架开关盒及连接电缆等的维护、保养、更换。 3.电气配电系统维护：负责所有机房配电柜的器件和柜体维护。器件包括所有柜内切换机构模块、空气开关、脱扣控制器、输入输出排、电气监控传感器、电量仪以及配电系统的末端工业连接器、连接线缆、PDU等。 4.机房消防设备维护管理：负责灭火剂的控制装置等的维护以及灭火器药剂的更换。 5.环境监控系统维护：负责所有机房环境监控系统的所有部件、监控平台软件的保养、维护。 6.机房电气系统维护：负责所有机房电器（照明、应急照明、开关、插座）保养、维护。 7.机房环境：清理机房的杂物，将机房物品定置；清洁机房门窗、地面。定期清洁电池室的地面；检查机房所有与外界的空洞是否已严密封堵，严密防鼠；检查机房玻璃、地板、天花板、通气口，墙体表面是否正常，外观是否完好，有否出现老化现象；检查机房是否有漏水现象；检查机房墙壁是否有渗水现象；填写巡检记录，有问题及时报告。 8.空调系统维护：负责所有机房精密空调系统室内外机组的所有部件、空调管线及单独布设的温湿度传感器的保养、维护，并负责两台华为精密空调的保养、维护、维修、更换等。 9.机房供水及排水水路、电路及照明线路的维护管理：水、电路管线及接口的检查。 10.机房基础维护管理：机柜线路的整理、标签检查更换、机房除尘清洁及有关配套的维护管理。 11.机房主机设备维护管理：负责网络设备（路由及交换设备等）的维护、管理、维修、更换等。 12.机房运行维护管理体系建设：完善机房运行维护规范，优化机房运行维护体系。 13.防雷接地维护：定期检查接地系统，防止接地系统腐蚀，确保接地系统连接可靠性，规范接地系统布线，定期测量接地电阻，防止雷击危害。 14.提供全市电子政务外网有线网络各				

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
		设备设施的日常运行、维护、网络安全保障、应急处置等工作，制定各项运行维护规章制度和应急预案，定期开展电子政务外网网络安全风险评估和应急演练，做好日常值班值守、机房和线路巡检、应急处置、故障处理、安全防护及日志记录，建立协同联动的网络安全监测与通报机制，及时处置安全事件，提升电子政务外网网络安全防护和应急处置能力。 15.将分散在各个机房的动环监测设备统一接入监控调度中心，设备包括但不限于温湿度传感器、烟雾探测器、门禁系统、UPS电源等，实现全天候24小时的专业化监控，通过集中化、智能化的监测手段，确保机房动力环境系统的稳定运行，提高故障响应速度和处置效率，从而保障整个IT基础设施的可用性和安全性。 16.提供所有机房视频监控维护服务，确保监控系统稳定运行，实时保障行政中心安全，服务涵盖视频监控设备的日常巡检、故障排查、维修更换等，同时提供统一汇聚解决方案，实现监控数据的集中管理和高效分析。 17.提供机房门禁出入记录服务，可实时记录人员出入情况，为机房安全管理提供有力数据支撑，大幅增强机房安全防护能力。 备注：1号机房是指行政中心1#楼1楼101，2号机房是指1#楼负1楼A05，3号机房是指4#楼4楼421，4号机房是指4#楼4楼417，5号机房是指6#楼4楼401，6号机房是指6#楼1楼123，1号机房监控室是指行政中心1#楼1楼103。				
2	电子政务外网完善的售后服务	1.金昌市电子政务外网广域网纵向贯通省市、县的全省统一网络基础平台，提供市、县/区各提供≥2台广域网核心路由器服务，负责开通电子政务外网业务。广域网核心路由器节点具备双核心设备，区/县级通过双链路、≥1000M带宽上联至市广域网核心路由器骨干节点，市级通过双链路、万兆带宽上联至省广域网核心路由器骨干节点，充分保障广域网骨干网络的可靠稳定性。 2.金昌市电子政务外网城域网总体网络架构具备高扩展性的双星型架构，核心路由交换区提供≥2台城域网核心路由	项	1	100000	100000

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
		器和2台高性能核心交换机服务，负责城域网内互联以及数据路由转发。同时为保证各市级单位接入电子政务外网的便捷性，考虑未来网络灵活扩展性，在每个市级单位及有需求的二级单位提供接入网关服务，用于各部门、单位的接入。 3.安全接入区服务，提供防火墙、入侵检测、沙箱、VPN网关等，实现无线城域网接入的安全保护服务。 4.互联网接入区服务，具备双链路上联至运营商，通过链路负载均衡设备和集中NAT技术方式进行互联网访问。根据等级保护基本要求，电子政务外网互联网出口设备需具备高性能防火墙作为出口的安全隔离设备，隔离互联网和电子政务外网的内部网络，保证跨安全域的访问都能通过防火墙进行控制管理，并能在网络出口处实现入侵防范功能。同时还应该在互联网出口处进行优化控制，保证用户访问选择最优的链路。此外，在互联网出口处进行流量控制，保证网络发生拥堵的时候优先保护重要的主机。根据公安部等级保护基本要求，所有用户访问互联网需要部署上网行为管理系统，并保存≥3个月的日志。因此，互联网出口区域还需部署上网行为管理设备实现对内部用户访问互联网的上网行为进行监控、日志进行记录。 5.提供电子政务外网市广域网核心节点到省广域网核心节点≥10G出口链路专线运维服务、市广域网核心节点到县广域网核心节点专线运维服务及市广域网核心节点到区广域网核心节点主干链路运维服务，并确保线路线路质量稳定可靠。 6.提供7*24小时提供电话或网络报障服务，能够提供包括重大故障及事件预警。如由于线路检修、设备搬迁、工程割接、网络及软件升级等可预见的原因，影响或可能影响市级部门、单位使用该光纤电路接入服务的，应至少提前48小时告知采购人并提供相关预案。在接到市级各部门、单位网络故障申报后，需在4小时内解决，并给予处理报告。 7.支撑金昌市电子政务外网有线网络服务项目设备及设施必须满足附件二相关参数要求。				

序号	服务名称	服务要求	单位	数量	单价（元/年）	合计（元/年）
3	驻场服务	提供三人以上专属驻场服务团队驻场式服务，并提供7*24小时全市电子政务外网运维服务，保证全市电子政务外网正常运行，驻场人员必须能够熟练操作所有设施设备，能及时有效处理各类故障，需为驻场人员购买意外伤害保险等人身保险及社会保险。	项	1	360000	360000
	总计					7548000

1.5 支撑金昌市电子政务外网有线网络服务政府采购服务项目软硬件清单见附件一。

1.6 中标供应商承诺函见附件二。

第二条　合同总价款及付款方式

2.1 合同总金额¥7548000元整（大写：柒佰伍拾肆万捌仟元整）经甲乙双方确认签订合同后，甲方向乙方支付合同总金额的 60% 即人民币¥4528800元整（大写：肆佰伍拾贰万捌仟捌佰元整），甲乙双方验收合格后，支付合同总金额的 30% 即人民币¥2264400元整（大写：贰佰贰拾陆万肆仟肆佰元整）。剩余合同总金额的 10% 即人民币¥754800元整（大写：柒拾伍万肆仟捌佰元整）留做绩效评价款项。评价等次为优秀，甲方向乙方支付 100% 绩效评价款项；评价等次为良好，甲方向乙方支付 80% 绩效评价款项；评价等次为合格，甲方向乙方支付 60% 绩效评价款项；评价等次为不合格，甲方扣除所有绩效评价款项，甲方根据考核结果确定是否授予下年度合同。

金昌市电子政务外网有线网络服务政府采购服务项目服务质量绩效评分表见附件三。

2.2 乙方应开具真实有效的服务费增值税电子普通发票，税率为6%，甲方根据乙方出具的发票向乙方采用转账方式支付与发票金额等值服务费。

乙方账户信息如下:

开户行: 金昌工行镍都支行

开户行地址: 甘肃省金昌市金川区盘旋路

户名: 中国电信股份有限公司金昌分公司

账号: 27050452090221011 86

联行号: 102823000033

纳税人识别号: 91620300767726771R

地址: 甘肃省金昌市建设路117号

第三条　组成本合同的有关文件

下列有关本次招标采购的招标响应文件或与本次采购活动相适应的文件及有关附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于:

（1）政府采购招标文件;

（2）乙方提供的响应文件;

（3）开标一览表;

（4）投标承诺;

（5）服务承诺;

（6）中标通知书;

（7）甲乙双方商定的其他文件。

第四条　权利保证

乙方应保证甲方在使用服务时不受第三方提出侵犯其专利权、版权、商标权或其他权利的起诉。一旦出现侵权，乙方应承担全部责任。

第五条　双方权利和义务

5.1 甲方权利和义务

5.1.1 甲方享受乙方提供的服务清单内容。

5.1.2 在开通和使用电子政务外网有线网络服务业务过程中出现的所有问题，均由乙方处理。

5.1.3 甲方协调乙方网络建设，系统调测等工作。

5.1.4 甲方有权根据自身业务需求变化，放弃租用乙方提供的电子政务外网有线网络服务内容，但应在退出前一个月提出需求，乙方应全力配合，提供技术及方案支持，并保证甲方所有数据安全。

5.1.5 甲方有权对乙方进行验收并进行评价，确定乙方服务等次进行评价的标准由甲方确定。

5.2 乙方权利和义务

5.2.1 乙方确保提供的全市电子政务外网有线网络服务7×24小时不间断安全稳定运行。

5.2.2 乙方建设的电子政务外网有线网络必须符合国家电子政务外网建设规范和标准。

5.2.3 乙方必须采取有效措施阻止任何破坏或试图破坏网络安全的行为（包括但不限于钓鱼，黑客，网络诈骗，网站或空间中含有或涉嫌散播病毒、木马、恶意代码，及通过云服务器等对其他网站、服务器进行涉嫌攻击的行为，如扫描、嗅探、ARP欺骗、DDOS等），电子政务外网在运行期间发生网络安全事件、网络及设备故障等影响电子政务外网安全可靠稳定运行的情况，网络安全防护责任及由此造成的损失由乙方承担。

5.2.4 金昌市电子政务外网有线网络发生网络故障时，乙方应及时向甲方报告，按照应急预案提出具体处置措施，并进行有效稳妥处置。

5.2.5 在服务期内全市电子政务外网有线网络发生故障，乙方维修或更换设备所产生的费用均由乙方承担。

5.2.6 各部门、单位接入金昌市电子政务外网时，乙方未经甲方同意不得擅自接入。

5.2.7 乙方应向甲方提供金昌市电子政务外网有线网络专属驻场服务团队人员名单及联系方式，并在上述信息发生变化时及时通知甲方。

5.2.8 乙方不得利用金昌市电子政务外网有线网络上传、下载、存储、制作、复制、发布、传播含有下列内容的信息：违反国家规定的政治宣传和新闻信息；涉及国家秘密和安全的信息；违反国家民族和宗教政策的信息；妨碍互联网运行安全的信息；侵害他人合法权益的信息和其他有损于社会秩序、社会治安、公共道德的信息或内容；封建迷信、淫秽、色情、下流的信息或教唆犯罪的信息；其他违反法律法规、部门规章或国家政策的内容，如有上述情形发生，乙方应承担由此造成的所有损失。

第六条　售后服务及培训

6.1 乙方应按照国家有关法律法规和“三包”规定在服务期内提供7×24小时保障服务。

6.2 乙方必须遵守甲方的有关管理制度、操作规程。对于乙方违规操作造成甲方损失的，由乙方承担赔偿责任。

6.3 发生网络故障乙方应及时进行处置，一级网络故障4小时内处置完毕，二级故障2小时内处置完毕，三级故障1小时内处置完毕。

6.4 乙方提供7×24小时的服务支持和运维巡检保障，确保提供的服务安全可靠运行。巡检时发现服务项目出现问题时，应第一时间通知甲方，并对责任范围内的故障进行及时修复。

6.5 人员培训：对甲方操作人员进行系统操作与维护培训确保他们能够熟练掌握系统的使用方法和维护技巧。

6.6 其他售后服务及培训内容同第一条项目服务内容及要求中的相关条款。

第七条　产权归属

7.1 乙方为项目服务采购的所有设备设施产权归乙方所有。甲方以购买服务模式向乙方每年支付服务费。

7.2 金昌市电子政务外网有线网络所有相关资料、软件、数据、资源等的知识产权均归甲方所有。

7.3 甲方提供给乙方的数据、资料等资源，以及电子政务外网运行过程中收集、产生、存储的数据和文档等的知识产权均归甲方所有，乙方应保证甲方对这些资源的访问、利用、支配等权利。

7.4 针对本项目提供的软硬件产品（包括载体和文档）和相关系统接口，由甲乙双方共同确定使用范围和对象，未经甲方书面许可乙方不得擅自对外转让或允许第三方使用。

第八条　违约责任

8.1 甲方违约行为及赔偿责任

8.1.1 甲方无正当理由拒绝验收，因此造成的损失由甲方自行承担。

8.1.2 甲方未按合同规定的期限向乙方支付服务费的，需向乙方说明逾期支付理由，如为无理由拒付的，所造成的损失由甲方承担。

8.2 乙方违约行为及赔偿责任

8.2.1 乙方未按本合同规定提供售后服务及培训的，乙方须赔偿甲方因此遭受的所有损失。

第九条　保密条款

9.1 乙方应严格遵守保密义务，保证遵守《中华人民共和国保守国家秘密法》等有关规定，严守国家秘密，自觉维护国家安全和利益。金昌市电子政务外网有线网络服务政府采购服务项目所有相关资料、

软件、数据等的知识产权均归甲方所有，与乙方无关，乙方无权复制、传播、转让这些资源，也无权允许或提供他人使用这些资源。

9.2 乙方应当负责金昌市电子政务外网有线网络相关软硬件的口令、数据信息，并为其保密性负责。因维护不当或保密不当致使以上信息丢失或泄漏所引起的一切损失和后果均由乙方承担。

9.3 乙方未经甲方授权，不得访问、修改、披露、利用、销毁金昌市电子政务外网数据；在服务合同终止时，应将数据、文档等归还给甲方，并按要求彻底清除数据。

9.4 乙方应采取有效的管理和技术措施确保金昌市电子政务外网数据的保密性、完整性和可用性。

9.5 因金昌市电子政务外网有线网络设备损坏、升级或其他原因而更换新设备时，如原设备存储有电子政务外网数据的，甲方应积极配合乙方将原设备上的数据迁移至新设备，乙方负责对原设备上的数据进行完全清除，保证数据不被泄露。

9.6 保密责任不因本合同的无效、提前终止、解除或不具操作性而失效。

第十条　验收

10.1 项目具备验收条件后，乙方向甲方书面提交《项目验收申请》，进行项目验收。

10.2 乙方应根据投标文件，列出项目服务清单，出具《金昌市政府采购验收清单（服务类）》作为甲方验收的条件依据。

10.3 验收时，甲乙双方必须同时在场，乙方所提供的服务不符合合同内容规定的，甲方有权拒绝验收。乙方应及时按本合同内容规定和甲方要求进行整改，直至验收合格，方视为乙方按本合同规定提供相关服务内容。

第十一条　不可抗力

11.1 本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况，包括但不限于：自然灾害、地震、洪水、雷击、火灾、战争或准战争状态、恐怖活动、戒严等公认的不可抗力事件。

11.2 合同生效后，合同各方的任何一方由于不可抗力事故而影响到本合同履行时，则延长履行合同的期限，这一期限应相当于事故所影响的时间，并可根据情况部分或全部免予承担违约责任，但一方延误履约后发生不可抗拒力的，不能免除责任。

11.3 如果不可抗力事件的影响持续达30日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。

第十二条　合同的变更和终止

本合同一经签订，甲乙双方不得擅自变更、中止或终止合同。

第十三条　合同的转让

本合同必须由乙方单独全面履行。乙方不得擅自将本合同部分或全部转给第三方。乙方擅自转让部分或全部合同的行为无效。

第十四条　法律适用和争议解决

14.1 本合同适用中华人民共和国法律。

14.2 所有因本合同引起的或与本合同有关的任何争议将通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可采取下述两种争议解决方式：

（1）将该争议提交本地仲裁委员会，按照申请仲裁时的仲裁规则进行仲裁。仲裁在本地进行（金川区）。仲裁语言为中文。仲裁裁决是终局的，对双方均有约束力。仲裁费用由败诉方承担。

（2）向甲方所在地的人民法院起诉（金川区）。

14.3 仲裁或诉讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其它部分。

第十五条　合同生效及其他

15.1 本合同自签订之日起生效，有效期为【壹】年。

15.2 服务期：自签订合同之日起3年，合同采取“1+1+1”模式逐年考核签订，采购人根据服务情况进行年度考核，根据考核结果确定是否授予下年度合同。

15.3 本合同须由甲乙双方法定代表人（或负责人）或授权代表签字并加盖公章。

15.4 本合同一式陆份，甲乙双方各执叁份。

15.5 对本合同条款的任何修改、变更或增减，须经双方授权代表签署书面文件并加盖公章或者合同章，成为本合同的补充文件，具有同等法律效力。

15.6 未尽事宜由双方另行协商决定，并以附件形式予以说明，本合同附件为合同不可分割的一部分，与合同具有相同的法律效应。

附件:

附件一：　支撑金昌市电子政务外网有线网络服务政府采购服务项目软硬件清单

附件二：　中标供应商承诺函

附件三：　金昌市电子政务外网有线网络服务政府采购服务项目服务质量绩效评分表

（以下无正文）

GSJCA2500357EGN00

签章页

甲方（盖章）：金昌市大数据中心

法定代表人(委托代理人)：[redacted]

经办人：[redacted]

签订日期：2025 年 5 月 29 日

乙方（盖章）：中国电信股份有限公司金昌分公司

法定代表人(委托代理人)：[redacted]

2025年05月28日

经办人：[redacted]

签订日期：2025 年 5 月 29 日

GSJC2503357EG00

附件一：

支撑金昌市电子政务外网有线网络服务项目

设备及实施清单

序号	设备名称	技术要求	单位	数量	备注
一、网络专线接入服务					
（一）市广域网内容					
1	市广域网核心路由器	提供高性能市广域网核心路由器，需满足：1.设备支持100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS等接口类型；2.支持bras双机热备场景，设备升级其中一台，另一台需能正常工作，用户不下线；3.IPv4、Ipv6路由及转发表容量要求：支持IPv4路由表容量≥25M，IPv6路由表容量≥10M，支持IPv4转发表容量≥4M，IPv6转发表容量≥2M；4.支持独立NAT板卡；支持10G端口支持网络硬切片（FlexE）；5.支持随业务流的检测技术，实现基于IP五元组筛选追踪业务流，进行实时检测，精准定位到故障点，丢包、误码类故障，确保业务性能；6.关键芯片(包括但不限于CPU、NP、TM、TCAM、FIC及交换芯片)具备自研国产化芯片；7.冗余主控，冗余交流电源，≥20个万兆/千兆光接口，交换容量≥130Tbps，转发性能≥25000Mpps；8.支持根据不同的网络服务要求如时延、带宽、安全性和可靠性等来划分切片网络，应对不同的网络应用场景。	台	2	
2	县区广域网核心路由器	提供区县广域网核心路由器，永昌县、金川区各部署≥2台，需满足冗余主控，冗余交流电源，≥20个万兆/千兆光接口；交换容量≥130Tbps；转发性能≥25000Mpps；支持独立NAT板卡；支持10G端口支持网络硬切片（FlexE）。	台	4	
3	广域网万兆单模光模块	提供广域网万兆单模光模块，满足光模块-SFP+-10G-单模模块(1310nm,10km,LC)要求。	个	12	
4	广域网万兆多模光模块	提供广域网万兆多模光模块，满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	36	
5	广域网千兆单模光模块	提供广域网千兆单模光模块，满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	40	
（二）市级城域网内容					
1	城域网边界防	提供城域网边界防火墙服务做边界隔离连接各区域，需满足≥48个万兆光口，≥6个40G光口，冗余引擎，	台	2	

	火墙	冗余交流电源；吞吐量≥80Gbps，最大并发连接数2400万，每秒新建连接数≥80万，并提供服务期内免费IPS、AV、URL等特征库升级服务。			
2	城域网核心路由器	提供城域网核心路由器实现核心层全冗余和高速连接，确保核心层稳定可靠高效地运行，城域网核心路由器需满足冗余主控，冗余交流电源，冗余主控，冗余交流电源，≥20个万兆/千兆光接口，≥6个40/100G光口；交换容量≥130Tbps；转发性能≥25000Mpps；支持独立NAT板卡；支持≥10G端口支持网络硬切片（FlexE）。	台	2	
3	城域网核心交换机	提供城域网核心交换机上联城域网核心路由器，需满足：1.冗余主控、冗余交换网板、冗余交流电源，≥96个万兆/千兆光口，≥12个不少于40G光口，≥4根不少于3米高速堆叠电缆；交换容量≥500Tbps，包转发率≥96000Mpps；3.支持独立的硬件监控模块，控制平面和监控平面物理槽位分离，支持1+1备份，能集中监控风扇、电源等模块，能调节能耗；4.支持整机MAC地址≥1M，支持ARP表项≥384K；5.支持IPv4路由转发表FIB规格≥3M，支持Ipv6路由转发表FIB规格≥1M；6.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性；7.支持真实业务流的实时检测技术，实现对IP网络的精确丢包监控和快速故障定界能力。	台	2	
4	市级城域网探针	提供市级城域网探针旁挂城域网边界防火墙，需满足6G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	
5	市级各部门、单位接入防火墙	提供市级各部门、单位接入防火墙，需满足：1.≥12个千兆电口+8个千兆光口+4个万兆光口，冗余交流电源，≥240G固态硬盘，吞吐量≥20Gbps，并发连接数≥800万，每秒新建连接数≥20万，并提供服务期内免费威胁防护（IPS、URL、AV，云沙箱检测功能）功能授权；2.支持每IP，每用户的最大连接数限制，防护服务器；3.支持DNS过滤，提高WEB网页过滤的性能；4.支持恶意域名过滤，实现对C&C进行阻断；5.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测；6.支持Portal页面定制及调查问卷。	台	2	
6	市级各部门、单位接入汇聚交换机	提供市级各部门、单位接入汇聚交换机，需满足：1.≥48个万兆/千兆光口+240个千兆光口，冗余交流电源，4根高速堆叠电缆，交换容量≥85Tbps，包转发率≥57600Mpps；2.支持真实业务流的实时检测技术，秒级快速故障定位；3.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性。	台	2	
7	市级各部门、单位接入探针	提供市级各部门、单位接入探针旁挂市级各部门、单位接入防火墙，需满足6G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	
8	59段市级各部门、单位接入交换机	为市级各部门、单位提供59段接入交换机，需满足1.≥48个千兆光口，≥4个万兆光口（非复用接口），交流供电，≥48个千兆单模光模块，≥4个万兆多模光模块；2.交换容量≥2.72Tbps，包转发率≥780Mpps；3.支持MAC地址规格≥32K；4.支持Ipv4路由FIB表≥8K，Ipv6路由FIB表≥4K。	台	1	

9	市级各部门、单位接入网关	提供市级各部门、单位接入网关，需满足≥5个千兆电口+4个千兆光口，交流供电，整机交换容量≥20Gbps，转发性能≥9Mpps。	台	200	
10	市行政中心楼层接入交换机	提供市行政中心楼层接入交换机，需满足1.≥48个千兆电口+4个千兆光口（非复用接口），交流供电；2.交换容量≥400Gbps，包转发率≥80Mpps；3.支持MAC地址≥32K，支持ARP表项≥4K。	台	30	
11	市级城域网40G单模光模块	提供市级城域网40G单模光模块，需满足40GBase-ER4光模块-QSFP+-40G-单模模块(1310nm,40km,LC)要求。	个	12	
12	市级城域网40G多模光模块	提供市级城域网40G多模光模块20个，需满足40GBase-eSR4光模块-QSFP+-40G-多模模块(850nm,0.3km,MPO)(可对接4个SFP+)要求。	个	20	
13	市级城域网万兆单模光模块	提供市级城域网万兆单模光模块，需满足光模块-SFP+-10G-单模模块(1310nm,10km,LC)要求。	个	24	
14	市级城域网万兆多模光模块	提供市级城域网万兆多模光模块，需满足光模块-SFP+-10G-多模模块(850nm,0.3km,LC)要求。	个	60	
15	市级城域网千兆单模光模块	提供市级城域网千兆单模光模块，需满足光模块-eSFP-GE-单模模块(1310nm,10km,LC)要求。	个	500	
16	市级城域网千兆多模光模块	提供市级城域网千兆多模光模块，需满足光模块-eSFP-GE-多模模块(850nm,0.55km,LC)要求。	个	80	
二、网络安全服务					
（一）安全接入区内容					
1	安全接入区路由器	提供安全接入区路由器，需满足1.双主控，双交流电源，≥10个万兆/千兆光接口+10个千兆光接口；2.支持交换容量≥110Tbps，支持包转发率≥14000Mpps；3.设备支持100GE、50GE、40GE、25GE、10GE、GE、FE、E1、POS、CPOS等接口类型；4.支持MACSec加密技术；5.10G端口支持网络硬切片（FlexE）。	台	2	
2	安全接入区防火墙	提供安全接入区防火墙，需满足≥12个千兆电口+8个千兆光口+4个万兆光口，冗余交流电源；≥240G固态硬盘，吞吐量≥20Gbps，并发连接数≥800万，每秒新建连接数≥20万，并提供服务期内免费威胁防护（IPS、URL、AV，云沙箱检测功能）功能授权。	台	2	
3	安全接入区VPN	提供安全接入区VPN设备，需满足≥12个千兆电口+12个万兆光口+2个40G光口，冗余交流电源，≥240G固	台	2	

	设备	态硬盘，提供服务期内免费特征库升级服务，并发SSLVPN≥2000用户，吞吐量≥30Gbps，并发连接数≥1200万，每秒新建连接数≥40万。			
4	安全接入区探针	提供安全接入区探针，需满足3G检测能力，≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，并提供服务期内免费威胁防护服务。	台	1	
5	安全接入区入侵防御	提供安全接入区入侵防御，需满足≥8个千兆COMBO+4个千兆电口+10个万兆光口，冗余交流电源，IPS检测吞吐量≥18Gbps，每秒新建连接数≥50万，并发连接数≥2000，并提供服务期内免费特征库升级服务License。	台	1	
6	安全接入区沙箱	提供安全接入区沙箱，含配套服务器，冗余电源，≥8个千兆电（1个千兆管理接口、3个千兆备用接口、4个千兆监听接口）+2*10GE光口；高性能APT威胁检测系统，可以精确识别未知恶意文件渗透和C&C恶意外联。通过直接还原网络流量并提取文件或依靠下一代防火墙提取的文件，在虚拟的环境内进行分析，实现对未知恶意文件的检测。	台	1	
7	安全接入区万兆多模光模块	提供安全接入区万兆多模光模块，需满足光模块-SFP+-10G-多模模块(850nm, 0.3km, LC)要求。	个	30	
8	安全接入区千兆单模光模块	提供安全接入区千兆单模光模块，需满足光模块-eSFP-GE-单模模块(1310nm, 10km, LC)要求。	个	6	
（二）互联网接入区内容					
1	互联网接入区链路负载均衡	1.提供互联网接入区链路负载均衡，需满足：1.≥14个千兆电口，≥8个千兆光口，≥8个万兆光口，≥480G固态硬盘，冗余交流电源，L4吞吐量≥40Gbps，4层新建≥60W，7层新建≥65W，并发会话数≥2000万；2.支持基于管理员自定义的时间计划来配置出站访问的链路调度策略；3.支持基于应用协议的智能选路，能识别主流互联网应用如P2P、微信、网银，进行调度；4.通过ICMP、TCP、DNS等方式，检验SNAT地址池中的地址有效性，避免出口SNAT池中地址被意外封杀后仍然被使用造成网络访问中断；5.支持IPv6基础特性及IPv6的负载均衡，满足今后IPv6网络的升级，可以通过负载均衡设备进行网站发布的NAT64转换，以及IPv6站点的负载；6.支持基于TCP、HTTP的被动健康检查，通过监控链路中的重置、重传、错误应答码等信息判断服务器的健康状态；7.支持Vlan、QinQ、STP、MSTP等二层协议，满足二层的区域隔离以及链路冗余；8.支持中文界面管理，支持具备命令行，而非Linux命令，对设备进行功能配置。	台	2	
2	互联网接入区抗Ddos设备	提供互联网接入区抗Ddos设备，需满足≥8个千兆combo口+6个万兆光口，冗余电源，≥20G流量清洗能力，含配套服务器；实时防御流量型攻击和应用层攻击。	台	2	

3	互联网出口防火墙	提供互联网出口防火墙，需满足≥12个千兆电口+12个万兆光口+2个40GE光口，冗余交流电源，≥240G固态硬盘，吞吐量≥40Gbps，并发连接数≥1200万，每秒新建连接数≥40万，并提供服务期内免费IPS、AV、URL、云沙箱等特征库升级服务。	台	2	
4	互联网接入区汇聚交换机	提供互联网接入区汇聚交换机，需满足≥24个万兆光口+24个千兆光口，冗余主控，冗余交流电源，1根万兆堆叠线缆；交换容量≥18Tbps，包转发率≥26000Mpps。	台	2	
5	互联网接入区探针	提供互联网接入区探针，需满足≥6G检测能力；≥16个千兆电口，≥6个千兆光口，≥6个万兆光口，交流供电，≥1T硬盘，≥4个万兆多模光模块，提供服务期内免费威胁防护服务。	台	1	
6	互联网接入区防病毒网关	1.提供互联网接入区防病毒网关服务，含显示屏，冗余电源，≥4个万兆光口，≥4个千兆光口，≥6个千兆电口（含光模块），网络层吞吐≥20G，防病毒吞吐≥12G，最大并发会话数≥400万，每秒新增会话数≥20万，对利用HTTP、SMTP、POP3、FTP、IM等多种协议进行传播的病毒进行扫描，完成对木马病毒、蠕虫病毒、宏病毒、脚本病毒等的查杀，同时支持多线程并发控制、深层次压缩文件杀毒、病毒白名单等功能，提供服务期内免费特征库升级；2.策略匹配时有极高的匹配效率，并经过相关机构的检测证明，基本信息只需统一匹配一次，不用每个上层策略都匹配一次，提高网络数据流的转发、规则匹配的性能；3.支持对1600+种应用平台及2500+种的应用进行识别和控制，至少支持5大类，比如：商业系统、协作应用、一般网络应用、媒体等及≥28子类，比如：认证服务、数据库、ERP-CRM、软件更新、电子邮件、VOIP视频、游戏等。	台	2	
7	互联网接入区入侵防御系统	提供互联网接入区入侵防御系统服务，需满足≥8个千兆COMBO+4个千兆电口+10个万兆光，冗余交流电源，IPS检测吞吐量≥18Gbps，每秒新建连接数≥50万，并发连接数≥2000，提供服务期内免费特征库升级服务License。	台	1	
8	互联网接入区上网行为管理	提供互联网接入区上网行为管理，需满足≥12个千兆电口+12个千兆光口，含1对Bypass，≥4个万兆光口，≥1T硬盘，包含管理软件；冗余交流电源；网络吞吐量≥40Gbps，应用性能≥5Gbps，最大并发连接数≥1000万，最大用户数≥20000。提供服务期内免费特征库升级许可。	台	1	
9	互联网接入区网络流量分析系统	提供互联网接入区网络流量分析系统，需满足1.冗余电源，机架式设备，含液晶屏，接口≥4千兆电口+4千兆光口+2万兆光口，吞吐量≥5G，并发≥300万，异常流量的检测、流量统计分析等，提供服务期内免费版本与特征库升级许可；2.支持威胁情报查询，在设备界面查询攻击源IP的地理位置、开放端口、关联域名、ASN及安全信息等；3.配置空路由牵引时，每个BGP支持配置≥5个community名称，用于多出口场景下实现空路由。支持配置路由邻居，支持配置RemoteAS、NeighborIP，并支持NTA与FlowspecBGP邻居路由器之间加密码认证；4.攻击事件支持对Top源IP、Top端口、Top接口、Top协议、Top源AS、Top源	套	1	

		子网以及TOPtcpflag进行监控数据呈现。			
10	互联网接入区万兆多模光模块	提供互联网接入区万兆多模光模块，满足光模块-SFP+-10G-多模模块(850nm, 0.3km, LC)要求。	个	40	
11	互联网接入区千兆单模光模块	提供互联网接入区千兆单模光模块，满足光模块-eSFP-GE-单模模块(1310nm, 10km, LC)要求。	个	8	
12	互联网接入区千兆多模光模块	提供互联网接入区千兆多模光模块，满足光模块-eSFP-GE-多模模块(850nm, 0.55km, LC)要求。	个	10	
（三）安全运维管理区内容					
1	安全运维管理区边界防火墙	提供安全运维管理区边界防火墙，需满足≥12个千兆电口+12个万兆/千兆光口+2个40GE光口，冗余交流电源；≥240G固态硬盘；吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万，提供服务期内免费IPS、AV、URL、云沙箱等特征库升级服务。	台	2	
2	安全运维管理区接入交换机	提供安全运维管理区接入交换机，需满足≥96个万兆光口，冗余主控，冗余交流电源，4根高速堆叠电缆；交换容量≥85Tbps，包转发率≥26000Mpps。	台	2	
3	安全运维管理区网络安全态势感知系统	提供安全运维管理区网络安全态势感知系统服务，含服务器，冗余电源，≥10Gbps流量处理能力；具备最新大数据分析和智能学习技术，从海量数据中提取关键信息，通过多维度风险评估，具备大数据分析方法关联单点异常行为，从而还原出APT攻击链，准确识别和防御APT攻击，能够对攻击链进行可视化呈现、展示全网安全态势、提供威胁报表等，展示资源侦查、外部渗透、命令与控制、内部扩散、数据外发等APT攻击过程，感知全网威胁态势、攻击路径、高危资产等信息，帮助快速掌控全网威胁，感知全网威胁态势，避免核心信息资产损失。提供全市政务新媒体安全监测服务。	套	1	
4	安全运维管理区日志审计系统	提供安全运维管理区日志审计系统，需满足：1.含服务器，冗余电源，≥6个千兆电口，≥4个千兆光口，≥1个console口，≥3*4T硬盘；≥200日志源，提供服务期内免费维保服务与特征库升级license；2.系统应支持规则自适应日志接入，应支持将新接收的日志信息与系统内置规则、自定义规则进行匹配，完成自动接入；3.系统应能够对主机日志展开深度分析，分析场景包括但不限于登录情况、用户核心文件/文件夹监控、敏感操作及异常外联；4.系统应提供日志转发功能，应支持日志转发多个目标地址，可实现原始日志、范式化日志的转发，且不丢失原始日志源IP	套	1	

		信息.			
5	安全运维管理区安全准入平台	提供安全运维管理区安全准入平台，含配套服务器，≥3000个接入终端管理授权；网络管理控制系统，是集管理、控制、分析和AI智能功能于一体的网络自动化与智能化平台。	套	1	
6	安全运维管理区网络管理平台	提供安全运维管理区网络管理平台，需满足：1.配套服务器，≥700个网络设备管理，提供交换机、防火墙等多种设备的统一管理，支持多厂商设备统一视图、资源、拓扑、故障、性能以及智能配置功能；2.场景化模版建网，支持快速复制到其他站点，满足小型网络不同的行业场景；3.支持内置CA服务器，满足企业CA运维管理，如个人证书颁布、挂失和过期处理，该个人证书可以作为网络准入认证身份源；4.支持用户业务随行，将用户和IP解耦，帐号即用户，根据用户登录条件（5W1H）授权安全组，基于UCL的策略矩阵，实现用户权限互访限制，满足随时随地接入网络业务权限一致。	套	1	
7	安全运维管理区安全管理中心	提供安全运维管理区安全管理中心，含机架式硬件设备，冗余交流电源，≥4千兆光口+4千兆电口，≥3*2T硬盘，可管理设备≥500台，日志处理性能≥12000条/秒；链接短信告警平台，实现日志统计告警结果短信通知，进行设备状态监控、设备管理、设备升级、策略下发、日志查询、报表统计、虚拟化设备集中授权等功能。	套	1	
8	安全运维管理区漏洞扫描系统	提供安全运维管理区漏洞扫描系统，需满足1.≥6个千兆电口+4个千兆光口，内存≥8G，硬盘≥1T，并发扫描数≥150个IP地址，最大扫描速度≥2000ip/h，最大并发任务数≥50，支持多路扫描，满足在复杂环境中部署的要求，支持不同网段同时检测的需求；2.支持授权IP数无限；3.发现信息系统存在的安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。支持分布式部署，提供服务期内免费特征库升级服务；4.为了漏洞扫描检测漏洞的全面性，支持检测的漏洞数大于250000条，兼容CVE、CNCVE、CNNVD、CNVD、Bugtraq标准。	套	1	
9	僵木蠕检测系统	提供僵木蠕检测系统，检测通过网页、电子邮件或文件共享方式试图进入企业网络的病毒、蠕虫、木马，以及高级恶意软件、APT威胁和勒索软件，冗余电源，≥4个万兆光口+4个千兆光口+4个千兆电口（含光模块），网络吞吐量≥5Gbps，最大并发连接数≥500W，文件处理数≥12万/天，硬盘≥1TBSATA，通过行为特征库检测引擎、流式病毒检测引擎、静态文件分析引擎、动态沙箱检测引擎、威胁情报等多种技术手段，实现了对恶意样本文件的还原、检测、保存、上报以及特征分发等全部能力；提供服务期内免费特征库升级服务。	套	1	
10	安全运维管理区杀毒	提供安全运维管理区杀毒软件系统，含配套服务器，杀毒软件客户端授权2000个终端授权，提供服务期内免费特征库升级。	套	1	

	软件系统				
11	安全运维管理区堡垒机	提供安全运维管理区堡垒机，需满足：1.具备液晶屏，≥4个千兆电口，≥2TSATA硬盘，1个网络接口扩展槽，字符并发会话数≥300，图形并发会话数≥700，可管理设备数≥200台，系统对运维人员维护过程进行全面跟踪、控制、记录、回放，支持细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告，实现运维过程的事前预防、事中控制、事后审计的严格管控；2.具有用户角色权限自定义功能，可对用户进行细粒度权限划分，可细分用户录入管理员，设备录入管理员，设备账号管理员，运维权限管理员，运维审批管理员，运维审计管理员，普通运维人员和审计员（提供配置界面截图证明并加盖公章）；3.支持划分多级组织架构（至少10个层级），不同层级有独立的用户管理，用户角色管理，资产管理，密码管理，策略管理、审计管理的权限角色，支持不同角色相互组合（提供配置界面截图证明并加盖公章）；4.用户登录堡垒机支持多种认证方式，包括本地静态密码认证、LDAP认证、RADIUS认证、USBKEY认证、PIN+软件OTP、短信认证、企微认证、钉钉认证、OAuth2.0等身份认证方式；支持可知因素和不可知因素的双因素认证；5.支持可通过参数配置开启或关闭字符、图形、文件等协议运维行为审计，但不影响对应协议的会话审计，防范涉密运维行为泄露。	台	1	
12	安全运维管理区运维笔记本电脑	提供安全运维管理区运维笔记本电脑，需满足≥14.2英寸显示屏，正版≥Windows10专业版、≥16G内存，≥512G固态硬盘，CPU≥i5-12500H四核处理器（含鼠标、键盘）。	台	1	
13	安全运维管理区二合一电脑	提供安全运维管理区运维笔记本平板二合一电脑，需满足≥13英寸显示屏，正版≥Windows10专业版，≥16G内存，≥256G固态硬盘，CPU≥i5-1135G7四核处理器（含鼠标、键盘、触控笔）。	台	2	
14	安全运维管理区运维终端	提供安全运维管理区运维终端，需满足i5-9400F及以上处理器，内存≥8G，硬盘≥256GSSD+1TSATA硬盘，≥2G独显，≥23英寸显示器。	台	3	
15	安全运维管理区运维平板电脑	提供安全运维管理区运维平板电脑，需满足≥10.8英寸显示屏，≥8G内存，≥256G存储容量。	台	3	
16	安全运维管理区会议平板电脑	提供安全运维管理区运维平板电脑，需满足≥11英寸显示屏，≥12G内存，≥256G存储容量。	台	1	

17	安全运维管理区KVM	提供安全运维管理区KVM，需满足屏幕规格≥19英寸，接口数≥16口；网卡≥1个RJ-45；连接线VGA线。	台	2	
18	安全运维管理区万兆多模光模块	提供安全运维管理区万兆多模光模块，需满足光模块-SFP+-10G-多模模块(850nm, 0.3km, LC)要求。	个	50	
三、运营维护服务-市行政中心机房环境优化内容					
1	UPS主机	模块化在线式双变换式主机，配置≥3个不少于50KVA功率模块（2+1），支持热插拔，冗余控制模块，具备集中旁路方式，旁路模块支持热插拔。	台	1	
2	锂电池机柜（主柜）	电池模组具备模块化设计，支持可插拔，且支持靠墙、背靠背安装；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；整机满足抗震≥8级烈度；锂电柜配备≥7寸的LCD屏幕，且锂电柜可监控并显示单体电芯温度、电压、SOH/SOC等数据、电池模块数据、电池柜数据、系统数据。	个	1	
3	锂电池机柜（辅柜）	电池模组具备模块化设计，支持可插拔，且支持靠墙、背靠背安装；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；整机满足抗震≥8级烈度。	个	3	
4	电池储能模块	≥64V，≥40Ah；电池柜内单个电池模块故障，剩下电池模块支持串联后继续运行，不影响业务；电芯具备过放电、过充电、外部短路、挤压、重物冲击、机械冲击、加热、跌落等可靠性测试；电芯具备针刺测试。	个	56	
5	市电输入柜	主路输入（不低于以下配置）：630A，带自动切换开关，400A维修旁路。主路输出1路400A/3P，2路250A/3P，2路160A/3P，4路40A/3P，4路16A/1P。	个	1	
6	UPS输出柜	主路输入（不低于以下配置）：2*400A，≥400A维修旁路。主路输出2路250A/3P，2路160A/3P。	个	1	
7	配电柜	支持两路市电输入；具有防雷开关或防雷器故障指示的微动开关，以便远程监控防雷状态。≥2个63A/3Pups输出空开，≥14个40A/3P机柜电源空开，≥2个40A/3P空调电源空开。	个	1	6号楼汇聚机房
8	UPS主机	UPS主机容量≥20kVA，高频在线双变换式UPS，具备≥IGBT整流，功率变换器和系统元件均由DSP控制。输出功率因数≥0.9。输入额定电压，满载运行时，UPS设备输入功率因数应≥0.99。整机最高效率≥95%。逆变过载能力≥5分钟（125%额度电流），1分钟（150%额定电流）。具有声光告警功能，具备LCD屏幕显示，便于操作，界面显示输出，市电模式，负载容量，电池模式，电池容量，市电，逆变，旁路，故障状态。支持风扇故障预警、电容器故障预警、电池故障预警。支持电池组共用，电池节数32-40节可调。防雷能力：交流输入端满足5kA防雷和6kV防浪涌。	台	1	6号楼汇聚机房
9	蓄电池	阀控式密封免维护铅酸蓄电池，≥12V，≥100AH。	只	32	6号楼汇聚机房

10	电池柜	配套电池柜。	个	1	6号楼汇聚机房
11	精密空调	风冷级精密空调，上送风，总冷量≥13KW，风冷量≥11KW，风量≥3000m^3/h，具备R410A制冷剂；具备低功耗加湿系统，加湿量2kg/h；室内机具备高效工业用直流变频涡旋压缩机；EC风机；蒸发器具备“V”型；室外机风机驱动具备变频调速器；精密空调具备电子膨胀阀。	台	2	
12	动力环境管理系统	机架式服务器：CPU主频≥2.0GHz，核数≥16Core；DDR4内存≥32GB；硬盘≥2*1200GBSAS2.5“HDD；Raid卡；双网卡、每块网卡≥4*GE电口；冗余交流电源软件平台：统一动力环境管理平台，实现对配电、UPS、精密空调、视频监控、温湿度、烟雾、水浸等设备和环境进行集中监控和管理；基于Web的远程管理功能，通过短信、Email告警方式，实现机房安全无人职守；要求系统软件具备B/S架构，服务器具备Linux操作系统；客户端软件基于IE浏览器；数据中心管理系统具备高安全设计，着重对操作系统、数据库、管理软件进行加固，可有效防御窃听、伪造、篡改、越权访问、病毒、网络入侵等危害动作，避免管理系统服务器成为用户网络中的安全短板，并提供3种以上主流杀毒软件的扫描报告。系统应提供南向集成接口，可支持接入各个监控子系统，支持的接口类型必须包括但不限于：SNMP、Modbus-TCP、电信C接口、BACnet、跨平台的API接口。系统须具有开放性，要求支持的接口协议包括但不限于：Webservice、API、SNMP、Modbus、BACnet、电信C接口。短信猫，网络制式：支持4G、5G，无线GPRS-48Kbp，USB供电，移动APP运维。	套	1	
13	动力环境采集器	用于非标信号的采集处理，转化为SNMP协议上传到服务器处理，采集器支持Web访问。	台	5	
14	交换机	≥24个10/100/1000Base-T太网端口，4≥个复用的千兆ComboSFP，≥4个万兆SFP+，PoE+，冗余交流电源。	台	5	

附件二：中标供应商承诺函

十一、承诺函

1、对服务内容及技术要求完全响应承诺函。

2、清单内容响应性承诺函。

格式自拟

承诺函一：

在合同履行过程中，若我方未能达到本项目服务内容及技术要求，采购人有权采取以下措施：

（1）要求我方限期整改，整改期间服务期限相应顺延；

（2）按合同约定扣除相应款项；

（3）单方解除合同，并要求我方承担由此产生的全部法律责任及经济损失。

4.法律效力

我方承诺，如因我方原因导致项目未能达到约定要求，愿依法承担违约责任，包括但不限于赔偿损失、支付违约金等。

附：服务内容及技术要求偏离表/规格偏离表

供应商名称（单位盖章）：中国电信股份有限公司金昌分公司

法定代表人（单位负责人）或其委托代理人：[redacted]

日期：2025 年 5 月 20 日

承诺函二：

清单内容投标响应承诺函

致：金昌市大数据中心

中国电信股份有限公司金昌分公司（以下简称“我方”）就参与金昌市电子政务外网有线网络服务政府采购服务项目（项目编号：2025JCSCGJHBA204）的投标及合同履行事宜，针对清单内容响应性要求，郑重作出如下承诺：

1.清单内容完全响应承诺

我方承诺严格按照招标文件及采购人提供的技术清单要求，提供全部约定的软件、硬件及数据服务（具体清单详见附件），确保其型号、规格、性能、数量及服务标准完全符合本项目技术要求，无任何缺项、漏项或降配情况。

2.服务质量与技术保障

我方保证所提供的软、硬件及数据服务满足以下要求：

（1）功能完整性：实现招标文件及合同约定的全部功能；

（2）技术合规性：符合国家及行业相关标准，并通过安全检测认证；

（3）数据服务稳定性：保障数据传输、存储及处理的稳定性、安全性和时效性.

3.合同附件效力

本承诺函为项目合同的附件组成部分，与合同具有同等法律效力。若我方中标，将严格按照承诺内容履行合同义务，确保清

事所列内容逐项落实。

4. 违约责任承诺

在合同履行过程中，若出现以下情形：

（1）未按清单提供约定的软、硬件或数据服务；

（2）提供的服务未达到技术要求或存在质量缺陷；

采购人有权采取以下措施：

（1）要求我方限期整改，整改期间服务期限相应顺延；

（2）按合同约定扣除相应款项；

（3）单方解除合同，并依法追究我方违约责任及经济损失赔偿责任。

5. 法律效力

我方承诺因自身原因导致清单内容未达标或服务缺陷的，愿承担全部法律责任，包括但不限于赔偿损失、支付违约金及承担诉讼费用等。

附：支撑金昌市电子政务外网有线网络服务项目设备清单

供应商名称（单位盖章）：中国电信股份有限公司金昌分公司

法定代表人（单位负责人）或其委托代理人：[redacted]

日期：2025 年 5 月 20 日

附件三：

金昌市电子政务外网有线网络服务政府采购服务项目服务质量绩效评分表

一级分类	二级分类	权重	考核内容	评分标准	得分
服务可靠性	网络完好率	10	电子政务外网整体运行情况，包括电路可用率、丢包率等	电路可用率≥99.9%；网络平均丢包率≤0.01%，吞吐率100%；传输时延≤20ms，最大延迟≤64ms，每一项不符合扣2分	
	网络可靠性	5	除各单位接入线路外，电子政务外网内部网络设备均提供双路由备份，且每半年开展一次链路倒换测试，并提供倒换测试报告	双路由备份未生效且未按时提供倒换测试报告扣5分	
	网络连通性	5	电子政务外网、互联网等其他网络畅通可用。	因运营商原因造成电子政务外网、互联网网络故障，SLA作为依据每次扣1分	
	备份管理	5	维护人员按月对核心网络设备配置数据进行采集备份，按季度对安全设备配置数据进行采集备份。	未按要求备份一项考核1分	
服务安全性	安全管理	10	构建全市统一的电子政务外网平台安全等级保护体系。通过提供市级政务网络平台安全防护体系服务，制定网络安全防护责任制度确保政务外网基础设施、重要信息资源、重点业务的系统安全。	因运营商原因造成政务外网发生网络安全事件每次扣2分，影响恶劣被省大数据中心或者公安机关、网信部门通报的每次扣5分	

	安全监测	5	维护人员按周监测并通报漏扫、态势感知、僵木蠕等高危漏洞和高威胁事件，按月提供安全服务报告。	数据未按要求监测并通报或未按时提供安全服务报告，每次扣1分	
	安全风险研判	5	运维人员每季度进行网络安全风险研判并出具风险研判报告	未按要求进行风险研判或未按时出具风险研判报告每次扣2分	
运维可靠性	机房巡检	10	驻场维护人员每日对设备、机房环境、动环等运行情况进行巡检	未主动巡检每次扣0.5分，因环境导致重大故障每次扣5分	
	资料完整	5	驻场运维人员应建立运维台账，台账应完整并及时更新	台账不完整或未及时更新每次扣1分	
	标签准确	5	机房所有设备及线缆按要求应及时准确粘贴标签	未及时准确粘贴标签或粘贴标签不准确每次扣1分	

	故障响应	5	电子政务外网发生网络故障时，一级网络故障4小时内处置完毕，二级故障2小时内处置完毕，三级故障1小时内处置完毕。	未按时限完成故障处置每次扣1分	
	环境卫生	5	所有机房应保持干净整洁，工器具应摆放整齐，每周进行一次卫生清洁	未按时完成卫生清洁或未整齐摆放工器具，每次扣0.5分	
	运维团队	5	按要求提供人员驻场服务且能够熟练操作设备，及时有效处理故障	未按要求提供驻场人员或未及时有效处理故障扣5分	
	服务质量	5	运维人员到各单位提供服务时应具备良好的服务态度与专业的服务技能	因处理不及时或服务态度不好，反应至大数据中心，每次考核0.5分	

	UPS系统可靠性	5	每日进行一次UPS系统的状态巡检，每半年进行一次电池放电测试，每年进行一次倒换演练	未按时进行UPS系统状态巡检每次扣0.5分，未按时进行电池放电测试和倒换演练，每次扣1分	
应急安全管理	应急预案	5	应具备符合实际、可操作性的应急预案	未建立应急预案扣5分，不符合实际、可操作性不强扣0.5分	
	应急演练	5	每年进行一次网络安全应急演练	未按要求完成应急演练，缺一次扣5分	

注：项目绩效评价得分大于90分为优秀；大于80分为良好；大于70分为合格；等于或小于70分为不合格。

GSJC125[illegible]