CMGS-JC-202500309

金昌市电子政务外网无线网络服务

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:2025JCSCGHTBA000276

中国移动
China Mobile

甲方：金昌市大数据中心

乙方：中国移动通信集团甘肃有限公司金昌分公司

中国移动
China Mobile

金昌市电子政务外网无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：中国移动通信集团甘肃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无线网络服务政府采购服务项目招标文件》（招标文件编号：2025JCSCGJHBA205）《金昌市电子政务外网无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：D03-12620300073595738 4-20250429-000003-3）签订本合同。

第一条 项目服务内容及要求

1.1 网络接入服务

1.1.1 市级城域网服务

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采用具备高扩展性网络架构，可实现核心层冗余和高速连接，确保核心层稳定可靠高效地运行。

市级城域网与市级广域核心路由器互联，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。防火墙应支持IPv4、IPv6会话信息记录、可溯源。

1.1.2 互联网出口区服务

互联网出口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、采取综合安全防护措施，部署包括抗DDOS、上网行为管理、堡垒机、下一代防火墙、VPN、全流量监测等设备，对互联网接入提供安全防护。互联网边界处部署防火墙，实现安全隔离及策略的准入控制，通过防火墙集成的入侵防御功能和防病毒功能，实现对应用层网络僵尸木马等类型的攻击的防护；部署上网行为管理系统规范用户上网行为，保障带宽合理使用；堡垒机设备为网络设备、安全设备提供安全的运维通道，提供运维审计、身份认证、多因素校验、权限审批等功能。以防火墙作为边界隔离，采用千兆链路连接至互联网出口区，满足各部门单位互联网使用需求。金昌市电子政务外网无线网络服务项目部署统一互联网出口，采取NAT技术，通过静态路由连接本地互联网。

互联网出口带宽按照1G专线出口提供，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，适时对出口带宽进行调整。

1.1.3 无线网络服务

1.1.3.1 政务外网盲点区域延伸覆盖

为了使接入电子政务外网单位安全稳定使用政务外网，杜绝各办公室私自建立电子政务外网无线网络环境，造成网络安全事故，故本项目用无线网方式进行政务外网盲点区域补点，提升政务外网安全性，具体接入方案如下：

本项目无线网络的架构使用现在主流的无线控制器AC+瘦AP的无线网络架构进行盲点区域无线网络覆盖，该架构下的无线网络由1台无线控制器和5台无线AP组成，所有的无线AP皆由该控制器进行统一的配置和管理，并提供1条千兆互联网专线。无线AP可以通过PoE交换机进行远程的PoE供电或者选择本地供电，如果采用远程的PoE供电，则可以在无线控制器上按照时间进行无线AP的开关定时，按照设定好的策略自动定时开关AP，满足一定的节能需求。通过AC+无线AP方式完成盲点区域补点。

a.采用最新一代支持802.11acWave2协议，单个AP同时具备二个射频，一个射频支持2.4GHz频段，一个射频支持5GHz频段；

b.不低于2个10/100/1000Mbps，整机协商速率不低于1000Mbps，一台AP覆盖范围30米，满足应用需求；

c.每射频最大接入用户数：512（整机最大接入用户数1024）；

d.提供1个AC，5个AP。

1.1.3.2 无线网卡服务

提供8张5G无线网卡，用于远程无线管理和办公使用。

1.1.3.3 VPN服务应用

VPN主要用户无线网络服务，建立相对安全的无线网络通道提供特定网络服务的应用，VPN服务应用具备以下能力：

a.吞吐量≥20Gbps，最大并发链接数≥800万，每秒新建连接数链接≥20万；

b.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议；

c.支持NAT66，NAT64，6RD隧道；

d.支持每IP，每用户的最大连接数限制，防护服务器；

e.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维；

f.支持识别国标SIP协议及主流安防厂家的私有协议；

g.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等；

h.支持对HTTPS、POP3S、SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护；

i.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护；

j.支持流探针功能，采集网络流量的网络层、传输层和应用层信息，并将采集到的信息发送到网络安全智能分析系统，通过网络安全智能分析系统评估网络中的威胁和APT攻击；

k.支持Portal页面定制及调查问卷，进行营销推广；

l.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。

1.2 网络安全服务

1.2.1 安全运维管理区服务

安全运维管理区提供统一管控平台、数据立体安全管控系统等服务，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。

安全运维管理区边界一台高性能防火墙作为边界隔离手段，采用万兆链路连接至市城域网核心交换机。下接一台接入交换机，通过万兆链路进行互联，保障链路的带宽需求。

为更安全、更快捷的管理电子政务外网设备，及时发现并解决电子政务外网故障，需提供电子政务外网统一管控平台服务，统一通过智能网络统一管控平台管理、监控电子政务外网二平面设备网络运行情况，实现电子政务外网业务可视化，设备运行状态、链路质量、链路流量、故障告警等。统一管控平台满足以下功能：一是实现网络拓扑的可视化监视，二是能够快速精确故障管理，三是实现业务网管功能，通过管控平台快速登录相关网络设备完成配置操作，无需维护人员现场登录设备，响应快速。

数据立体安全管控系统实现对政务云平台服务器集群安全管控，并完成运维等高危终端数据防泄密安全管控，涉及政务数据整个生命周期。达到以下效果：一是业务应用服务器数据安全防护；二是数据库服务器审计安全防护；三是系统运维终端数据安全防护。

1.2.2 等保三级服务

根据《关于加快推进国家电子政务外网安全等级保护工作的通知》（政务外网〔2011〕15号）、《信息系统安全等级保护定级指南》（GB/T22240-2008）有关要求，结合项目实际情况，确定金昌市电子政务外网无线网络服务项目需满足三级等保要求，并通过专业机构评测。

1.2.3 售后服务

1.2.3.1 提供互联网出口链路专线接入，链路上联端口必须具备≥1G带宽服务能力，采用光口接入方式直接接入甲方机房。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，不能包含中标方的局域网网内带宽，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。

1.2.3.2 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。

1.2.3.3 专线接入服务质量必须保证现有应用的互通性和兼容性要求。

1.2.3.4 提供完善的售后服务，提供7*24小时电话或网络报障服务，能够提供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，影响或可能影响甲方及全市各单位使用该光纤电路接入服务的，应至少提前48小时告知甲方并提供相关预案。在接到甲方及全市各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。

1.2.3.5 支撑金昌市电子政务外网无线网络服务项目的软硬件设施，必须满足附件2相关参数要求。

1.2.3.6 提供金昌市电子政务外网无线网络服务项目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，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。

1.2.3.7 提供1人驻场服务，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。

1.3 本项目服务清单如下：

金昌市电子政务外网无线网络服务政府采购服务项目服务清单

序号	服务名称	服务内容	单位	数量	单价（元/年）	合计（元/年）
一、网络接入服务						
1	市级城域网服务	提供市城域网核心交换服务，实现市级城域网与市级广域网互联；提供城域网边界防火墙服务和接入防火墙服务，满足网络边界保护和访问控制要求。	项	1	164400	164400
2	互联网出口区服务	1.提供互联网出口链路专线接入，链路上联端口必须具备≥1G带宽服务能力，采用光口接入方式直接接入甲方机房。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，不能包含中标方的局域网网内带宽，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。 2.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。 3.互联网出口区采用单链路上联至运营商，通过链路负载均衡设备和集中NAT技术方式提供互联网访问服务。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	项	1	505900	505900

序号	服务名称	服务内容	单位	数量	单价（元/年）	合计（元/年）
		个月的日志。				
3	无线网络服务	1.政务外网盲点区域延伸覆盖 使用现在主流的无线控制器AC+瘦AP的无线网络架构进行盲点区域无线网络覆盖，该架构下的无线网络由1台无线控制器和5台无线AP组成，所有的无线AP皆由该控制器进行统一的配置和管理，并提供1条千兆互联网专线。无线AP可以通过PoE交换机进行远程的PoE供电或者选择本地供电，如果采用远程的PoE供电，则可以在无线控制器上按照时间进行无线AP的开关定时，按照设定好的策略自动定时开关AP，满足一定的节能需求。通过AC_无线AP方式完成盲点区域补点。 2.VPN接入服务 VPN主要用户无线网络服务，建立相对安全的无线网络通道提供特定网络服务的应用，VPN接入服务具备以下能力： ①吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； ②支持静态路由、策略路由、RIP、OSPE、BGP、ISIS等路由协议； ③支持NAT66，NAT64，6RD隧道； ④支持每IP,每用户的最大连接数限制，防护服务器； ⑤支持策略的模糊查询，策略组、策略规则标签，方便策略的管理及运维； ⑥支持识别国标SIP协议及主流安防厂家的私有协议； ⑦支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等；	项	1	30000	30000

序号	服务名称	服务内容	单位	数量	单价（元/年）	合计（元/年）
		⑧支持对 HTTPS、POP3S、SMTPS, IMAPS 加密流量代理解密后、并进行内容过滤，审计、安全防护； ⑨支持 HTTP、FTP、SMTP、POP3、IMAP、NFS 等协议的病毒防护； ⑩支持流探针功能，采集网络流量的网络层、传输层和应用层信息，并将采集到的信息发送到网络安全智能分析系统、通过网络安全智能分析系统评估网络中的威胁和 APT 攻击； ⑪支持 Portal 页面定制及调查问卷、进行营销推广； ⑫可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。 3. 无线网卡服务 提供8张5G 无线网卡，用于远程无线管理和办公使用。				
二、网络安全服务						
1	安全运维管理区服务	提供运维管理区边界防火墙服务、安全管控平台服务、高危服务端口安全管控服务、安全风险智能学习服务、系统管理服务、服务器数据非法访问防护服务、系统引导区保护服务、服务器安全自我保护服务、运维终端安全防护服务、数据库审计安全防护服务，实现运营平台化、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运维管理。	项	1	329700	329700
2	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需达到等级保护三级要求，并通过专业机构评测。	项	1	100000	100000

序号	服务名称	服务内容	单位	数量	单价（元/年）	合计（元/年）
3	售后服务	提供1人驻场服务、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。提供全市电子政务外网无线网络各设备设施的日常运行、维护、网络安全保障、应急处置等售后服务工作。乙方负责提供金昌市电子政务外网无线网络服务项目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，乙方应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。	人	1	118000	118000
	总计					1248000

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

1.5 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¥1248000元整（大写：壹佰贰拾肆万捌仟元整），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¥748800元整（大写：柒拾肆万捌仟捌佰元整），甲乙双方验收合格后，甲方向乙方支付合同总金额的 30% 即人民币¥374400元整（大写：叁拾柒万肆仟肆佰元整）。剩余合同总金额的 10% 即人民币¥124800元整（大写：壹拾贰万肆仟捌佰元整）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无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增值电信服务费电子普通发票，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：招商银行北京分行营业部

开户行地址：北京市西城区复兴门内大街156号A座一层

户名：中国移动通信集团甘肃有限公司金昌分公司

账号：888801480000 4828

联行号：308100005027

纳税人识别号：91620000710391210N

地址：甘肃省金昌市金川区公园路65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系统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无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无线网络服务内容，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 乙方确保提供的电子政务外网无线网络服务 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无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无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无线网络发生故障，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无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无线网络上传、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无线网络服务政府采购服务项目所有相关资料、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，以及金昌市电子政务外网无线网络政府采购服务系统使用过程中收集、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费用的，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无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无线网络服务政府采购服务项目相关的口令、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无线网络服务政府采购服务项目。

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无线网络设备损坏、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力。

附件：

附件一： 支撑金昌市电子政务外网无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无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）

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）：中国移动通信集团甘肃有限公司金昌分公司

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

附件一：

支撑金昌市电子政务外网无线网络服务政府采购服务项目
软硬件清单

序号	软硬件名称	技术参数要求	单位	数量
一、网络接入服务				
（一）市级城域网服务				
1	金昌市城域网核心交换机	1.交换容量≥500Tbps，包转发≥96000Mpps，主控引擎与交换网板物理分离；主控引擎≥2；独立交换网板≥4；整机业务板槽位数≥8； 2.设备支持支持以太网千兆电口、千兆光口、万兆光口、万兆电口、25G端口、40G端口、100G端口； 3.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自动化部署； 4.支持横向虚拟化技术，将多台设备虚拟为一台，支持长距离集群； 5.支持整机MAC地址≥1M，ARP表项≥256K； 6.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6； 7.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2； 8.单台配置双主控、双交换网板、双交流电源、万兆光口≥96个、40GE光口≥24个、万兆多模光模块≥10个、万兆单模光模块≥10个、千兆单模光模块≥10个、40G单模光模块（40Km传输距离）≥2个。	台	2
2	防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66，NAT64，6RD隧道； 5.支持每IP，每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护；	台	2

		11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广； 13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。		
（二）互联网出口区服务				
1	抗DDOS设备	1.实配：千兆光电复用口≥8个、千兆电口≥4个、千兆光口≥4个、万兆光口≥6个、双交流电源、20G清洗能力； 2.支持风扇冗余和可插拔更换，当风扇模块出现故障时，可以在设备不断电的情况下，对风扇模块进行更换； 3.直路部署模式，攻击响应延迟<1秒； 4.支持检测设备、清洗设备旁路部署，逐包检测动态引流，支持BGP动态引流，支持PBR回注(策略路由)、二层回注； 5.支持基于源SYN报文比例异常检测防御真实源SYN攻击； 6.支持HTTP应用层Flood/HTTPCC识别及防御，支持HTTPS应用层Flood/HTTPSCC识别及防御，支持DNSQueryFlood识别及防御； 7.支持基于会话检测防御FIN/RSTFlood； 8.系统支持综合报表查询，报表内容包含攻击趋势、流量对比、攻击类型分布、攻击事件TOPN、流量TOPN等，支持报表导出； 9.支持IPv4/IPv6共栈防御。	台	1
2	互联网出口区边界防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66、NAT64、6RD隧道； 5.支持每IP、每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询、策略组、策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广； 13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。	台	1

3	互联网出口区接入交换机	1.双主控，双电源，万兆光口≥48个； 2.主控引擎≥2；整机业务板槽位数≥6； 3.交换容量≥70Tbps，包转发率≥57000Mpps； 4.为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数≥2；支持颗粒化电源，整机电源槽位数≥4个； 5.为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计； 6.支持独立的硬件监控板卡，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； 7.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自动化部署； 8.支持整机MAC地址≥512K；支持整机ARP表项≥256K； 9.支持业务板集成AC功能，实现对AP的接入控制和管理，实现对无线无线用户的统一认证管理，用户数据报文的隧道集中转发； 10.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例； 11.支持真实业务流的实时检测技术，秒级快速故障定位； 12.支持PQ、WRR、DRR、PQ+WRR、PQ+DRR等调度方式； 13.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理。	台	1
4	上网行为管理	1.实配：千兆电口≥12个，千兆光口≥12个，万兆光口≥4个，硬盘≥2T，交流冗余电源，含集中管理软件，3年特征库升级许可； 2.网络层UDP吞吐量≥39Gbps，应用层HTTP吞吐量≥16Gbps，并发连接数≥500万； 3.支持双机热备，支持主主模式，主备模式，支持同步配置、会话、运行状态、VPN状态、特征库，支持配置抢占模式和抢占延时，支持配置HA监控接口； 4.支持路由和透明模式配置源地址转换、目的地址转换、双向地址转换等； 5.支持4GUSB插卡，支持在4G接口上运行IPSecVPN； 6.支持静态路由、策略路由、动态路由、ISP路由； 7.支持IPv6/v4双栈，支持IPv6安全策略； 8.支持基于全局或链路进行DNS透明代理，支持指定DNS或继承链路DNS配置，针对多链路支持基于优先级、权重、流量算法进行DNS负载； 9.支持基于接口和目的地址进行健康检查，可自定义检查间隔、重试次数等； 10.支持在设备旁路部署时针对违规上网行为进行阻断过	台	1

		滤； 11.支持自定义应用，包括但不限于数据包方向、协议、端口、IP地址、目标域名、关键字识别等维度，数据包方向包括任意、请求数据、响应数据，关键字匹配模式支持文本或正则表达式； 12.支持智能和快速识别模式配置； 13.针对私接网络行为，惩罚方式包括但不限于无操作、阻断和限速，阻断和限速支持自定义惩罚时长；支持使用设备内置公告页面或引用第三方公告页面，支持自定义提醒频率，支持定时发布公告； 14.支持IPsecVPN冷备份技术，指定VPN主备链路，当主链路存活时，备链路不接受不发送报文，避免主备链路同时收发包来回路径不一致导致业务中断的情况； 15.支持单用户全天行为分析报表，一个界面同时展示用户名、用户组、在线时长、虚拟身份（如QQ号码、微博账号等）、日志关联情况、全天流量使用分布、网站访问类别分布、全天关键网络行为轴等信息。		
5	堡垒机	1.设备高度：1U，交流单电源，4GCF卡，2TSATA硬盘，8G内存，4*GE电口，2*USB接口，1*RJ45串口，1*GE管理口，1个接口扩展槽，缺省授权管理200台设备； 2.为了运维人员登录安全，支持自动登录、手工登录、半自动登录、密钥登录方式； 3.为了运维人员运维方便，支持自动填写特权密码，从普通管理模式进入到特权模式，提供对部分配置操作进行向导式配置界面； 4.除用户身份认证外，对特定目标设备访问还需要高级管理员授权才能访问，授权审批方式支持web和手机APP审批两种方式，手机APP上进行登录授权审批、仓库授权审批，工单审批三种审批模式，方便随时随地进行审批工作，支持手机APP上进行运维监控，包括设备信息推送，系统告警监控两种数据； 5.要求支持孤儿账号功能，能够提供对各从账号的运维使用率的分析功能，当发现使用率异常的从账号，对相关管理员采取告警、记录及通知操作； 6.支持第三方客户端实现SSH、RDP、VNC、X11、Telnet、SFTP、FTP协议自动、手动登录运维设备，并实现审计功能。	台	1
6	全流量安全监测	1.可管理路由器数量20台，含12万flows/s授权许可，引擎模块，2U，含交流冗余电源模块，8GCF卡，2T硬盘，32G内存，2*USB接口，1*RJ45串口，2*GE管理口，4个100/1000M以太网电口，3个网络接口卡扩展插槽，2个万兆SFPP插槽（不含光纤接口模块），支持万兆多模光纤接口模块，万兆单模光纤接口模块； 2.设备支持IPv4/IPv6环境下的异常流量检测功能；	台	1

		3.支持的数据分析格式至少包括sflowv4/v5、netflowv5/v9、netstreamv5、flexiblenetflow、ipfix; 4.支持自定义攻击特征进行检测和告警; 5.支持从外网到内网异常流量检测，支持从内网到外网异常流量检测; 6.支持检测阈值自动学习，支持学习时间、学习对象预先指定，同时支持学习阈值自动配置与手动配置功能; 7.针对不同防护对象，支持设置不同的异常流量检测参数和牵引策略; 8.支持对自定义的IP域范围检测入域流量超常和出域流量超常; 9.支持对指定时间范围的告警阈值进行抬升/降低，避免因业务流量正常波动带来误报和漏报; 10.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; 11.支持自定义或根据告警详情定义BGPFlowspec规则并发送给路由器进行流量过滤; 12.管理界面友好、易用性强，支持集中管理、本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息; 13.配置空路由牵引时，每个BGP至少支持配置5个community名称，用于多出口场景下实现空路由; 14.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; 15.提供完善的日志管理功能，包括日查询、删除、备份、生成报表等操作，而且要支持自定义报表、自动生成报表等功能。		
7	链路负载均衡	1.40Gbps吞吐、1U机型，14*10/100/1000M电口，8*千兆SFP插槽、8*万兆SFPP插槽，4*可选扩展插槽，5*风扇，480GB硬盘模块*2，双电源; 2.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，支持RIP、OSPF、BGP等路由协议以及各自的IPv6版本; 3.支持多种链路检测方法，能够通过ICMP、UDP、TCP、FTP、DNS、HTTP、RADIUS、SSL、HTTPS、TCPhalf-open、SNMP-DCA、RADIUS-ACCOUNT等方式监控链路的连通性; 4.支持轮询、加权轮询、最小连接、加权最小连接、随机、源地址HASH、目的地址HASH、源地址端口HASH，静态就近性、动态就近性、带宽算法、最大带宽算法、本地优先级、基于ISP选路等链路调度算法; 5.支持基于ToS、五元组条件（源IP地址，源端口、目的IP地址、目的端口、传输层协议号）来配置出站访问的链路调度策略;	台	1

		6.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； 7.支持基于域名的流量调度，针对特定网站选择指定的链路转发； 8.ISP地址库支持自动升级功能，使设备的ISP地址库保持在最新状态，保证流量调度的准确性； 9.支持主备部署，支持两台设备统一管理，配置只配置一端，配置自动同步，设备间会话实时同步； 10.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。		
（三）无线网络服务				
1	VPN	1.吞吐量≥20Gbps，最大并发连接数≥800万，每秒新建连接数≥20万； 2.支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议； 3.支持NAT66，NAT64，6RD隧道； 4.支持每IP，每用户的最大连接数限制，防护服务器； 5.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 6.支持识别国标SIP协议及主流安防厂家的私有协议； 7.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 8.支持对HTTPS、POP3S、SMTPS、IMAPS加密流量代理解密后，并进行内容过滤、审计、安全防护； 9.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 10.支持流探针功能，采集网络流量的网络层、传输层和应用层信息，并将采集到的信息发送到网络安全智能分析系统，通过网络安全智能分析系统评估网络中的威胁和APT攻击； 11.支持Portal页面定制及调查问卷，进行营销推广； 12.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。	台	1
2	AC	提供主流的无线控制器AC+瘦AP的无线网络架构进行盲点区域无线网络覆盖，该架构下的无线网络由无线控制器和多台无线AP组成，所有的无线AP皆由该控制器进行统一的配置和管理。	台	1

3	AP	1.采用最新一代支持802.11acWave2协议，单个AP同时具备二个射频，一个射频支持2.4GHz频段，一个射频支持5GHz频段； 2.不低于2个10/100/1000Mbps，整机协商速率不低于1000Mbps，一台AP覆盖范围30米，满足应用需求； 3.每射频最大接入用户数：512（整机最大接入用户数1024）。	台	5
4	无线上网卡	提供5G无线网卡，用于远程无线管理和办公使用。	张	8
三、网络安全服务				
（一）安全运维管理区服务				
1	安全运维管理区边界防火墙	1.标准机架式1U设备；实配：千兆电口≥12，万兆光口≥12；双交流电源，固态硬盘≥240G；三年IPS、AV、URL、云沙箱特征库升级服务； 2.防火墙吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万； 3.支持静态路由，策略路由、RIP、OSPF、BGP、ISIS等路由协议； 4.支持NAT66、NAT64、6RD隧道； 5.支持每IP，每用户的最大连接数限制，防护服务器； 6.支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； 7.支持DNS过滤，提高WEB网页过滤的性能； 8.支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； 9.支持恶意域名过滤，实现对C&C进行阻断； 10.支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； 11.要求防火墙具备AI引擎，AI引擎用于恶意C&C流量检测； 12.支持Portal页面定制及调查问卷，进行营销推广； 13.可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式。	台	1
2	安全运维管理区接入交换机	1.双主控，双电源，万兆光口≥48个； 2.主控引擎≥2；整机业务板槽位数≥6； 3.交换容量≥70Tbps，包转发率≥57000Mpps； 4.为保证设备散热效果和可靠性，要求设备支持模块化风扇框，可热插拔，独立风扇框数≥2；支持颗粒化电源，整机电源槽位数≥4个； 5.为适应机柜并排部署，设备机箱（包括业务板卡区）采用后出风风道设计； 6.支持独立的硬件监控板卡，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； 7.支持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自	台	1

		动化部署； 8.支持整机MAC地址≥512K；支持整机ARP表项≥256K； 9.支持业务板集成AC功能，实现对AP的接入控制和管理，实现对无线无线用户的统一认证管理、用户数据报文的隧道集中转发； 10.支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；支持路由协议多实例； 11.支持真实业务流的实时检测技术，秒级快速故障定位； 12.支持PQ、WRR、DRR、PQ+WRR、PQ+DRR等调度方式； 13.支持硬件BFD/OAM，3.3ms稳定均匀发包检测，提高设备的可靠性； 14.支持SNMPV1/V2/V3、Telnet、RMON、SSHV2，支持通过命令行、中文图形化配置软件等方式进行配置和管理。		
3	应用服务器	1.国产品牌设备，2U机架式服务器，非OEM产品，具有自主知识产权； 2.配置2颗英特尔至强处理器（主频2.4GHz，核数12）； 3.配置128GDDR4内存，可支持至少24个内存插槽； 4.配置2*480GBSSD硬盘，1000GB以上的SAS硬盘，支持热插拔SAS/SATA/SSD硬盘，可支持配置8块2.5inch托架的SATA/SAS硬盘，最大支持28块2.5寸硬盘； 5.支持双MiniSSD硬盘可做RAID1，可安装操作系统，hypervisor，虚拟化软件等； 6.配置1块SR430C-MIG(LSI3108)SAS/SATARAID卡，支持RAID0.1，提供Raid状态迁移，Raid配置记忆，自诊断，WEB远程设置等功能； 7.配置2*GE+2*10GE网口以太网卡； 8.配置2块900W双冗余电源，支持电源热插拔； 9.可管理和维护性：①集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志，可通过可视化工具提供系统未来状况的可视显示；②具有图形管理界面及其他高级管理功能；③配置独立的远程管理控制端口，支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作。	台	1
4	应用服务器	1.国产品牌设备，2U机架式服务器，非OEM产品，具有自主知识产权； 2.配置2颗英特尔至强处理器（主频2.4GHz，核数12）； 3.配置64GDDR4内存，可支持至少24个内存插槽； 4.配置2*480GBSSD硬盘，2200GB以上的SAS硬盘，支持热插拔SAS/SATA/SSD硬盘，可支持配置8块2.5inch托架的SATA/SAS硬盘，最大支持28块2.5寸硬盘； 5.支持双MiniSSD硬盘可做RAID1，可安装操作系统，	台	1

		hypervisor，虚拟化软件等； 6.配置1块SR430C-M1G(LSI3108)SAS/SATARAID卡，支持RAID0,1，提供Raid状态迁移、Raid配置记忆、自诊断，WEB远程设置等功能； 7.配置2*GE+2*10GE网口以太网卡； 8.配置2块900W双冗余电源，支持电源热插拔； 9.可管理和维护性：①集成系统管理处理器支持：自动服务器重启、风扇监视和控制、电源监控、温度监控、启动/关闭、按序重启、本地固件更新、错误日志、可通过可视化工具提供系统未来状况的可视显示；②具有图形管理界面及其他高级管理功能；③配置独立的远程管理控制端口、支持远程监控图形界面，可实现与操作系统无关的远程对服务器的完全控制，包括远程的开机、关机、重启、虚拟软驱、虚拟光驱等操作。		
5	安全管控平台模块	1.数据安全防护系统的基础承载平台； 2.最大支持400个服务器安全软件授权； 3.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
6	高危服务端口安全管控模块	1.通过端口控制限制对服务器的访问； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
7	安全风险智能学习模块	1.自动学习被保护数据的操作访问行为，禁止恶意程序的启动和运行； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
8	系统管理模块	1.提供B/S方式管理界面。支持系统管理员、安全管理员和日志管理员权限三权分立，支持进行统一的策略配置和软件版本升级，支持终端安全策略管理； 2.支持VMWare、KVM、Xen等主流虚拟化技术。	套	1
9	服务器数据非法访问防护模块	1.对被保护数据进行非法操作防护； 2.支持windowsServer和LinuxServer主流内核版本。	套	140
10	系统引导区保护模块	1.对操作系统引导区进行保护，阻断勒索病毒攻击引导区导致系统引导失败，业务受损； 2.支持windowsServer和LinuxServer主流内核版本。	套	140
11	服务器安全自我保护模块	1.支持自我保护功能； 2.支持windowsServer和LinuxServer主流内核版本。	套	140
12	运维终端安全防护模块	1.对下载到本地的数据实现透明加解密，非授权环境无法使用、授权环境使用无感知； 2.支持外发数据审批电子流，并集成密码认证、权限控制、截屏录屏等多项管控技术，制作成外发文件； 3.监控终端行为，阻断采用系统原生或第三方截屏录屏工具的数据窃取行为； 4.完善的自我保护能力，抵御恶意卸载、恶意关闭、病毒加密； 5.支持windows系列操作系统。	套	140

13	数据库审计安全防护模块	1.支持国际主流数据库：Oracle、MySQL、SQLserver、DB2、Sybase、Informix、Teradata、PostgreSQL、Cache; 2.支持国产主流数据库：达梦、南大通用、人大金仓、神通、浪潮KDB、湖南上容; 3.支持大数据平台非关系型数据库：Hive、HBase、MongoDB等; 4.支持对日志进行细粒度解析，支持数据库操作(DML)、对象管理(DDL)、控制(DCL)等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端IP地址、客户端MAC、终端程序、访问账号、访问数据库名、操作表名、SQL语句、数据库响应时间以及返回结果等关键信息; 5.三层关联审计，实现用户、主机、SQL操作三层关联分析，精确定位具体操作人员; 6.支持智能定义高危动作识别，实现对数据库的高危动作的阻断; 7.支持SYSLOG、SNMPTRAP、邮件、FTP等多种事件告警和提示方式; 8.支持对SQL语句操作类型统计、事件类型统计、风险级别统计、流量统计、同时接在线用户、客户端IP、会话、模板数等支持在线信息统计，并生成多种专业报表; 9.支持SQL语句进行拼接功能，能够完整解析与审计超长SQL语句（超过1460字节），屏蔽逃逸审计通道。	套	1

附件二：中标供应商承诺函

十一、承诺函

11.1 服务内容及技术要求完全响应承诺函

致：金昌市大数据中心

我公司参加本次金昌市电子政务外网无线网络服务政府采购服务项目（采购项目编码为：2025JCSCGJHGA205）的投标，在此郑重承诺：

我公司完全理解本项目采购服务内容及技术要求，并提供完全满足招标文件采购要求的服务。

投标人名称（盖章）：中国移动通信集团甘肃有限公司金昌分公司

日期：2025年7月20日

11.2 清单内容响应性承诺函

致:金昌市大数据中心

我公司参加本次金昌市电子政务外网无线网络服务政府采购服务项目（采购项目编码为：2025JCSCGJHBA205）的投标，在此郑重承诺：

我公司完全理解本项目采购服务内容及技术要求，并提供完全满足招标文件清单中（附件一：支撑金昌市电子政务外网无线网络服务政府采购服务项目设备参数清单）的软、硬件和数据服务。

投标人名称（盖章）：中国移动通信集团甘肃有限公司金昌分公司

日期：2025 年 8 月 20 日

附件三：

金昌市电子政务外网无线网络服务政府采购服务项目
服务质量绩效评分表

指标分类	考核指标	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0.5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。	未按要求备份一项扣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、重点业务系统的安全。	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	10	运维人员每季度进行网络安全风险研判并	未按要求进行风险研判或未按时出具风险研判报告	

			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。	未主动巡检一次扣0.5分，因环境导致重大故障每次扣5分。	
	资料完整	5	驻场运维人员因建立运维台账，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及时准确粘贴标签。	未及时未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。	未按时限处置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。	
	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和专业的服务技能。	因处理不及时或服务态度不好，反映到大数据中心每次扣0.5分	
	运维团队	5	按要求提供人员驻场服务且能熟练操作设备，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。	
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。