

# 政府采购项目 采 购 需 求

项目名称： 电子政务外网优化升级

采购单位： 莱阳市人民政府办公室

编制单位： 莱阳市人民政府办公室

编制时间： 2024 年 10 月

# 编制说明

一、采购单位可以自行组织编制采购需求，也可以委托采购代理机构或者其他第三方机构编制。

二、编制的采购需求应当符合《财政部关于印发政府采购需求管理办法的通知》（财库〔2021〕22号）要求及政府采购的相关规定。

三、斜体字部分属于提醒内容，编制时应删除。

四、对不适用的内容应删除，并调整相应序号。

## 一、需求调查情况

### （一）是否开展需求调查

按照《财政部关于印发政府采购需求管理办法的通知》（财库〔2021〕22号）的相关规定，本项目无须开展需求调查。

## 一、需求清单

### （一）项目概况

本项目为莱阳市人民政府办公室的电子政务外网优化升级，共为1个包。

### （二）采购项目预（概）算

总 预 算：人民币陆拾叁万柒仟贰佰元整/年  
(¥637200.00/年)。

### （三）采购标的汇总表

包号	序号	标的名称	品目 分类编码	计量 单位	数量	是否 进口
A	1	电子政务外网优化升级	C17010100	项	1	否

### （四）技术商务要求

#### 技术要求

## 一、项目说明

本项目为莱阳市人民政府办公室的电子政务外网优化升级，共划分为1个包；供应商需完成电子政务外网优化升级相关工作，供应商须对所报内容进行全部响应，若有遗漏，视为对采购人免费提供。

## 二、采购标的具体情况

### 1、项目总体概述

根据《山东省人民政府办公厅关于印发山东省政务信息系统整合共享实施方案的通知》（鲁政办发〔2017〕75号）和《山东省人民政府

办公厅关于印发 2018 年政务信息系统整合共享工作要点的通知》(鲁政办字[2018]50 号) 要求:“进一步优化外网网络结构, 实现全市乡镇(街道) 全覆盖, 基本具备跨层级、跨地域、跨部门、跨业务的支撑服务能力。完成市、县政府部门互联网出口整合。” 根据要求, 莱阳市电子政务外网公共服务域优化升级项目由供应商使用独立、专用的线路、设备, 并负责后续电子政务外网的运行维护。

## 2、项目总体要求

山东省电子政务外网是我省电子政务领域重要的信息化基础设施, 是满足各级政务部门经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。政务外网纵向覆盖省、市、县(区)、乡, 横向连接各级党委、人大、政府、政协、法院和检察院等政务部门。

烟台市电子政务外网是山东省电子政务外网在烟台的延伸和拓展, 烟台市电子政务外网公共服务域(原外网) 是全市各级各部门的政务专用网络平台、资源共享的公用网络平台和互联网接入平台。在电子政务外网公共服务域上全网使用 IPv4/IPv6 双协议栈的方式, 采用 MPLS (多协议标签交换) 技术, 提供 VPN (虚拟专用网) 服务满足各政府部门的业务承载需求。允许市级各单位通过市级统一出口访问互联网, 允许全市各级政府及部门授权用户的互联网安全接入。采取适当的方式, 通过与烟台市政务外网公共服务域市级平台的上下互联, 以及与网络管理系统、审计系统等互联, 实现系统化部署与监测管理, 达到无缝对接。

莱阳电子政务外网公共服务域作为烟台市电子政务外网公共服务域的延伸，是莱阳市各级各部门的政务专用网络平台、资源共享的公用网络平台，凡不涉及涉密政务信息的业务系统均需通过区级政务外网承载。

### 3、烟台市广域网与莱阳城域网网络结构

烟台市广域网由市广域网核心、市广域网边界和长途链路组成。莱阳城域网，采用两台核心作为城域网核心设备，上联广域网边界，下联莱阳市各级各部门。莱阳市级城域网可以采用“核心-汇聚-接入”三层架构。城域网设备设计、选型时应综合考虑 MPLS VPN 的承载能力和业务开通方式，保障各类业务畅通。

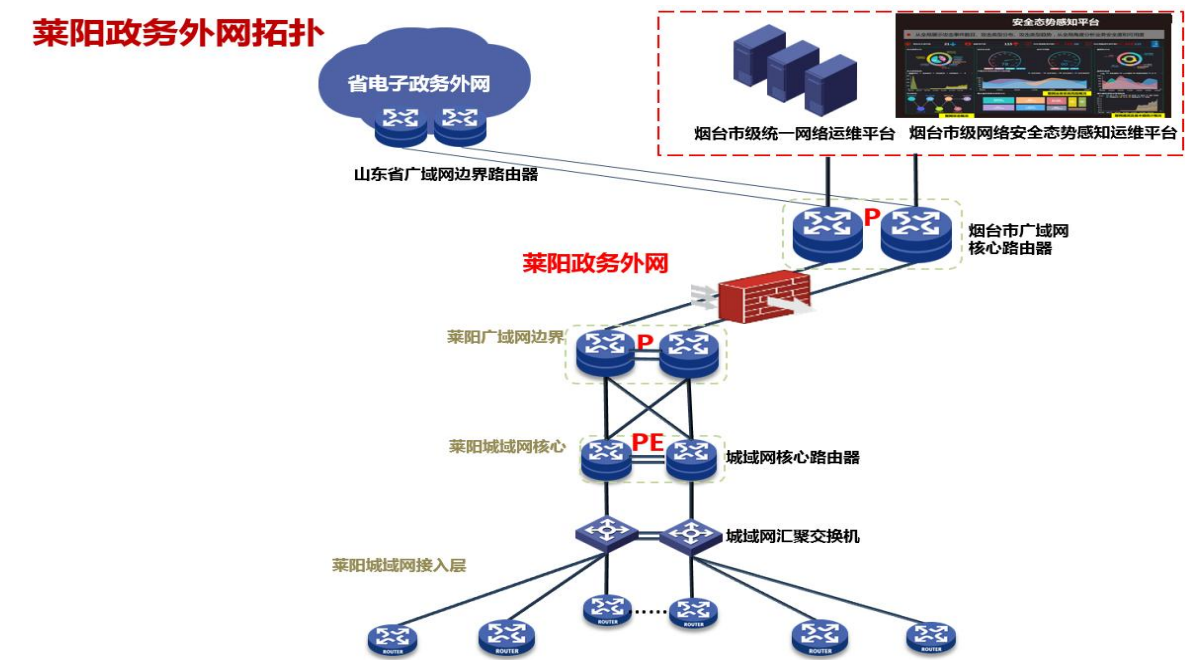


图 1 莱阳电子政务外网公共服务域网络拓扑

### 4、逻辑业务网络模型

根据政务外网公共服务域所承载的业务和系统服务类型的不同，在逻辑上，将整个政务外网公共服务域划分为公用网络区、专用网络区和互联网接入区三个功能区，分别提供政务外网公共服务域整合共

享的公共业务、部门专用业务和互联网业务。政务外网公共服务域采用 MPLS VPN 技术将一张物理网络逻辑上划分为“2+N”个业务网络，其中，“2”是公用网络区和互联网接入区，“N”是根据政务部门专用业务需求开设的多个虚拟业务专网。互联网接入区和专用网络区使用 MPLS VPN，公用网络区不使用 MPLS VPN。

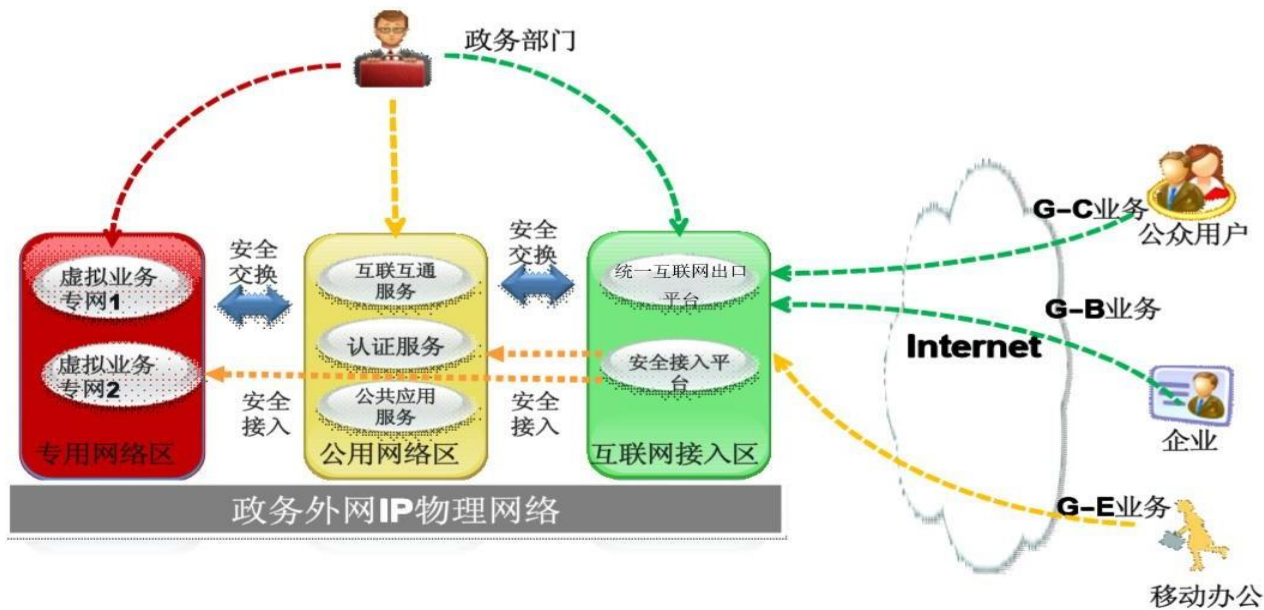


图 2 政务外网公共服务域业务承载模型示意图

公用网络区是实现各级政务部门之间互联互通的逻辑业务网络。公用网络区承载跨地区、跨部门的业务，提供认证、目录交换、公共应用等共性支撑服务。

互联网接入区是实现政务外网公共服务域连接互联网的网络区域。互联网接入区通过部署区级统一互联网出口，提供政务各部门访问互联网资源的网络通道。政务外网广域网原则上不承载互联网的流量。

专用网络区是由多个逻辑业务网组成。每个逻辑业务网是一个独立的 VPN 网络，逻辑业务网内有独立的 IP 地址规划和独立的路由表、路由协议选择。

公用网络区不使用 MPLS VPN，各专用网络区和互联网接入区分别承载在不同的 MPLS VPN 内。每个 MPLS VPN 各自独立的路由表，网

络上路由不可达。

## 5、电子政务外网公共服务域区级城域网优化升级建设和服务建设

### 5.1 电子政务外网公共服务域接入线路 90 条。

序号	网络类型	技术要求	数量
1	电子政务外网公共服务域接入线路	要求线路使用 PTN、OTN 或裸光纤方式，带宽要求 200M，并提供实际带宽可用率大于 95%，端到端传输时延不高于 100ms，年可用性大于 99.99%。同时对未来 5 年内各个 MPLS VPN 专网业务增多做到提前规划、充分考虑，供应商需提供带宽 100M、200M、500M 及 1G 带宽资费报价以供扩容及增加点位选择，新增点位与之前线路享受同等服务。	90

### 5.2 莱阳电子政务外网公共服务域区级城域网优化升级服务要求

莱阳城域网，采用两台核心作为城域网核心设备，上联广域网边界，下联莱阳市各级各部门。莱阳市级城域网可以采用“核心-汇聚-接入”三层架构。

区级城域网采用双核心，双链路接入市广域网边界路由器。如两者不在同一机房，供应商应将双链路光缆使用不同物理路由的管道敷设，并采用 MSTP、SDH、OTN、PTN 等带有自愈能力的链路承载。带宽 1Gbps，实际带宽可用率大于 95%，端到端传输时延不高于 10ms，年可用性大于 99.99%。

建设莱阳市级城域网接入层，供应商应提供到各部门的接入线路和接入路由器，并负责线路和设备的运行和维护。要求线路使用 PTN、OTN 或裸光纤方式，带宽要求 200M，并提供实际带宽可用率大于 95%，端到端传输时延不高于 100ms，年可用性大于 99.99%。同时对未来 5

年内各个 MPLS VPN 专网业务增多做到提前规划、充分考虑，供应商需提供带宽 100M、200M、500M 及 1G 带宽资费报价以供扩容及增加点位选择，新增点位与之前线路享受同等服务。

接入设备放置在各政务部门内，实现终端接入及业务隔离等功能；供应商应提供接入设备下联端口（包含公用网络区、互联网区和各业务专用网络区端口）至各部门汇聚上行端口单条线路的建设。接入设备由供应商负责管理维护，接入设备下联端口以下的线路、设备由各政务部门和单位自主建设管理、维护。

## 6、莱阳市电子政务外网公共服务域市级城域网优化升级服务要求

供应商须按照采购人要求提供莱阳市电子政务外网公共服务域市级城域网优化升级服务所需的全部设备。服务设备如下：

序号	项目名称	技术要求	数量	单位
1	核心系统	1. 交换容量 780Tbps，整机包转发性能 120000Mpps； 2. 采用 CLOS 硬件架构，主控和交换网板物理分离； 3. 业务槽位数 12 个； 4. 可支持热插拔、主控板 1+1 冗余备份、风扇模块 1+1 冗余备份、电源 1+1 冗余备份； 5. IPV4 路由协议：支持静态路由；支持 RIP v1/v2、OSPF v1/v2、BGP、ISIS；支持策略路由、等价路由； 6. IPV6 路由协议：支持静态路由；支持 RIPng、OSPFv3、BGP4+、ISISV6；支持策略路由；支持手工隧道，自动隧道，GRE 隧道，6to4，TELNET V6； 7. 支持手工隧道，自动隧道，GRE 隧道，6to4，TELNET V6； 8. 支持 IGMPv1/v2/v3、PIM-SM、PIM-DM、MSDP、MBGP、组播静态路由； 9. 支持 MPLS ,MPLS L2VPN,MPLS L3VPN,VPLS；	2	套



		<p>10. 内置硬件加密，支持 IPSEC；SSL VPN 加密；最大可创建 VPN 数量<math>\geq 250</math>；具备 L2TP、GRE 功能；支持预共享密钥（PSK）认证；</p> <p>11. 支持 PQ/FIFO/CQ/CBWFQ 等队列调度机制；支持 CAR、WRED、RED；</p> <p>12. 支持 console 口登录，支持 telnet（VTY）登录，支持 SSH 登录，支持 FTP 登录；</p>		
2	流量分析系统	<p>1. 1U, 内存<math>\geq 32G</math> 硬盘<math>\geq 4TB</math>, 千兆电口<math>\geq 8</math> 个, 千兆光口<math>\geq 4</math> 个, 插槽<math>\geq 1</math> 个 CONSOLE 口, 冗余电源, 扩展槽位<math>\geq 2</math> 个, 最大并发连接数<math>\geq 50W</math>, 综合威胁检测能力<math>\geq 1Gbps</math></p> <p>2. WEB 防护；支持 WEB 攻击检测，包含 SQL 注入攻击、跨站攻击、URL 跳转攻击、WEB 远程代码执行攻击、WEB 缓冲区溢出攻击、WEB 漏洞攻击、WEBSHELL 上传攻击、WEB 越权攻击、WEB 扫描攻击、目录遍历攻击、WEB 口令暴力破解攻击等多种 WEB 攻击类型。</p> <p>3. 支持通过智慧引擎检测未知威胁，通过威胁情报、僵尸主机检测已知 APT 攻击行为和已知 APT 组织。</p> <p>4. 支持针对不同类别告警信息进行配置，包括：安全（攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、异常流量、DDoS 检测、URL 过滤、黑名单）、管理、系统、硬件、容错、测试等，并可进行告警测试。（提供产品功能截图证明）</p> <p>5. 支持威胁视角和运维视角分析，威胁视角按照受害者、攻击者、威胁事件、恶意文件、攻击类型、攻击主机、受害主机、应用类型、恶意程序类型等维度进行综合分析，支持数据下钻查看威胁详情。运维视角分析能够帮助运维人员了解设备运行状态。</p>	1	套

		<p>6. 支持威胁分析功能，威胁分析展示包括：威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息。（提供产品功能截图证明）</p> <p>7. 支持恶意加密流量检测，采用恶意 TLS 流量智慧引擎、异常握手、非法证书和内网流量检测恶意加密流量。（提供产品功能截图证明）</p> <p>8. 资产管理：支持资产识别功能，识别资产信息包括：资产名称、IP 地址、MAC、操作系统、所属分组、发现时间、更新时间、服务/应用（角色、名称、版本、协议、端口、应用协议、厂商、更新时间）。支持资产导入导出。（提供产品功能截图证明）</p> <p>9. 流量审计；持对传统协议审计，包括：TCP/UDP、ICMP、HTTP、SMTP、POP3、IMAP、WEBMAIL、FTP、SMB、NFS、文件、MYSQL、SQLServer、ORACLE、POSTGRESQL、DB2、REDIS、MONGODB、达梦、南大通用、人大金仓、SSL、RDP、DNS、SNMP、TFTP、IKEV2、LDAP、SIP、SSDP、SOCKS4、SOCKS5、AFP、VNC、SSH、TELNET、DHCP、RADIUS、NTP、认证、SPICE、FEIQ、WAP、OSPF、KRB5 等 40 余种协议。（提供产品功能截图证明）</p> <p>10. 溯源取证；支持取证功能，取证类型包括：PCAP 取证、样本取证两种形式，PCAP 取证文件支持在线预览。（提供产品功能截图证明）</p>		
3	网络准入系统	<p>1. 硬件<math>\geq</math>2U, 千兆电口<math>\geq</math>8 个, 千兆光口<math>\geq</math>4 个, 冗余电源, 扩展槽位<math>\geq</math>2 个, 最大支持终端同时在线数<math>\geq</math>2000</p> <p>2. 支持 802.1X、Portal、透明网关、策略路由等多种准入模式选择，单设备情况下可进行混合准入模式应用；</p>	1	套

	<p>3. 支持同账户多在线管理，可设置同一用户名同时在线数量，并对用户名超过在线数进行处理。（提供产品功能截图证明）</p> <p>4. 支持入网终端健康检查，对检查项可进行权重、修复向导自定义设置，检查项包括：系统时间检查、系统运行时长检查、Guest 用户检查、AD 域域名检查、Windows 文件共享检查、Windows 防火墙检查等。</p> <p>5. 支持终端非法外联监控，可判断通过 http、telnet、ping 三种方式检测主机违规外联行为，给予违规处理方式（不处理、重启、断网、提示），并信息提示。（提供产品功能截图证明）</p> <p>6. 支持终端接口外设监控，可对终端所有接口外设实施启用停用控制，对 USB 设备添加 USB 硬件 ID 和设备信息，可设置例外项。</p> <p>7. 支持准入设备黑/白名单管理，可根据所应用的不同准入模式，设置黑/白名单终端 IP、MAC、协议、端口、VLAN 号等信息，以便针对该名单中设备进行入网控制。（提供产品功能截图证明）</p> <p>8. 提供客户端认证及手机短信认证方式，客户端认证可与第三方 AD 域、LDAP 服务器进行用户信息同步；手机短信认证可与短信服务器联动，在终端入网认证时下发验证码。（提供产品功能截图证明）</p> <p>9. 支持资产管理功能，可管理不同类型入网资产；提供交换机网络设备管理功能，可查看交换机设备接口状态、主机连接等详细信息。对入网资产可发现、可审批入网。（提供产品功能截图证明）</p> <p>10. 提供终端解绑、资产登录、报警、系统、终端认证、</p>	
--	--	--

		健康检查等详细日志信息，可采取图形化方式统计分析，并自定义模板进行报表定时输出。（提供产品功能截图证明）		
4	光汇聚交换系统	1. 交换容量 $\geq 600\text{Gbps}/6\text{Tbps}$ ； 2. 包转发率 $\geq 170\text{Mpps}/300\text{Mpps}$ ； 3. 千兆光口 $\geq 24$ 个，万兆 SFP+光口 $\geq 4$ 个，Console 口 $\geq 1$ 个、Manage 口 $\geq 1$ 个； 4. 所投交换机需具备工信部颁发的电信设备入网许可证书； 5. 支持 MAC 地址 $\geq 16\text{K}$ ，支持 4K 个 VLAN； 6. 支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现）； 7. 支持静态路由、支持 DHCP Server。	1	套
5	电汇聚交换系统	1. 交换容量 $\geq 600\text{Gbps}$ ，包转发率 $\geq 171\text{Mpps}$ ，若存在双参数以小参数为准； 2. 千兆电口 $\geq 24$ 个，万兆 SFP+光口 $\geq 4$ 个，Console 口 $\geq 1$ 个； 3. 支持静态路由、支持 DHCP Server； 4. 支持 IEEE 802.3az 标准的 EEE 节能技术：当 EEE 使能时，从而大幅度的减小端口在该阶段的功耗，达到了节能的目的； 5. 支持终端 IP-MAC 绑定，当 IP+MAC 不对应时，可以将终端加入黑名单实现断开终端流量； 7. 所投交换机需具备工信部颁发的电信设备入网许可证书； 8. 支持 MAC 地址 $\geq 16\text{K}$ 、支持 4K 个 VLAN。	6	套

## 7. 服务要求

### 7.1 迁移服务要求

项目运行期，根据上级要求和其他特殊情况，如政府新建政务外网城域网中心机房等，需要将电子政务外网公共服务域等相关设备或平台等做迁移，供应商需要根据双方协商结果按时提供迁移和安装等服务，保证不影响采购人的需求。

## 7.2 技术文档

提供完整的建设方案及安装、调试、使用技术文档。

## 8. 技术支持服务

供应商须提供 7\*24\*365 的故障应急反应机制。采购人系统一旦出现重大故障，则马上启动故障应急反应程序，提供远程技术支持，并承诺采用最快的交通工具赶到现场，提供现场的技术支持和技术保障，以协助生产和运行的顺利进行。到达现场后，供应商将协助客户进行故障诊断和排除。如故障发生的原因是由供应商提供的产品或服务引起的，则供应商会调集技术人员以尽早修复，并提出书面故障分析报告；如确认故障发生的原因是由第三方提供的产品或服务引起的，则供应商向客户提供书面故障诊断分析报告，在提供书面故障诊断分析报告之前，供应商将口头报告故障原因，并协助客户与该第三方交涉，配合第三方排除故障。在跟踪维护期内，供应商为采购人提供采购人工作时间的远程技术电话支持。供应商在接到采购人通过电话或电子邮件方式提出的服务请求后，应在 0.5 小时内给予响应。如有软件故障不能通过电话解决，供应商应在 1 小时内提供现场技术支持，2 小时内解决问题。服务完成后，供应商应将完整的、与所提供技术有关的技术资料，包括但不限于：系统维护纪录、系统变更记录、完整的源程序代码等装订成册提交给采购人系统管理部门；供应商应提供必要的技术指导和封闭式技术业务培训，保证采购人能正确、安全、有效地使用及维护系统。根据采购人要求对修正系统差错、改进系统性能、增加系统功能；供应商保证派出人员遵守采购人有关制度、工作纪律和安全规定，供应商服务人员应在采购人规定的工作场地范

围内工作。

## **9. 技术咨询与支撑**

技术咨询与支撑指在业务使用过程中由专业技术专家向采购人提供技术咨询和支撑，及时解决业务使用过程中遇到的疑难技术问题。

## **10. 业务培训服务**

定期对项目人员及采购方管理人员开展正确应对和处理突发应急通信工程的技能培训，培训内容包括应急预案流程、应急通信设备原理等相关内容。

## **11. 重要保障期值班服务**

根据网络安全重要保障期值班制度，在网络安全重要保障期，仍保留必要的技术人员候命，以应对网络安全保障任务的需求。

## **12. 保密要求**

供应商应严格履行保密义务，未经采购人书面正式批准，不得未经授权擅自查阅、复制、散布或使用电子政务外网的相关数据、日志等各类信息，确保采购人数据安全，违者承担相关法律责任。

## **★13. 其他服务要求（供应商须提供承诺函，格式详见附件；未提供的按无效响应处理。）**

(1) 供应商承诺与采购人同意的其它供应商（含运营商）紧密配合，不对其它供应商（含运营商）采取歧视性措施。若采购人后期有广域网、城域网地址迁移、系统建设或带宽升级等需求，供应商应承诺在迁移或升级过程中与其他供应商全力配合。因配合不力给采购人造成不良影响和损失的，承担全部后果。

(2) 供应商遵守省、市、区政务外网主管单位制定的运维服务指标体系和评估评价标准，承诺配合采购人对电子政务外网公共服务域运行情况进行年度评价和绩效考核；服从采购人委派监理并全力做好配合工作。

(3) 供应商承诺在本项目建设和后期的运行维护中,接受采购人的监督和管理,与采购人建立沟通对接机制,根据采购人要求,安排一名专人进行对接,为采购人提供各类运行数据。供应商需协助采购人制定详细的电子政务外网公共服务域运维工作细则,在服务过程中须详细记录服务内容,包括日常巡检、故障处理等。

(4) 供应商承诺具备应急通信的能力,并制定完善的紧急故障处理流程及应急预案。如遇不可抗力因素(如地震、洪水等)造成的线路中断,应在短期内采用应急手段恢复通信。

(5) 供应商承诺在本项目建设和后期的运行维护中,若出现上级政策、技术规范、标准等方面变化,根据情况进行适应性改造或升级。

(6) 供应商承诺选用安全可控的国产软、硬件设备组网,设备须全新未拆封,支持 IPv4/IPv6 双栈协议、MPLS VPN 等技术。

(7) 供应商应负责免费培训采购人指定的技术人员和管理人员,制定培训计划表,列出每种培训的地点和时间,培训内容应包括所提供设备的原理和技术性能、操作维护方法、安装调试、排除故障等各个方面。

(8) 为保证提供优良的设备售后服务,签订合同前,所有设备需提供原厂质保函和授权书;所有设备在服务期内需提供原厂质保服务。

注:

1. ★标要求为实质性要求,供应商须按要求提供承诺函,未提供的按无效响应处理;非★标参数为一般要求。以上要求仅供参考,供应商提供的服务应相当于或优于以上要求,并填写偏离表,针对本项目供应商可提供除以上服务内容外的增值服务项目或内容。

2. 成交供应商须保障采购人在使用成果资料的过程中不受到第三方关于侵犯专利权的指控。如果任何第三方提出侵权指控,成交供应商须与第三方交涉,并承担由此而产生的索赔、损失、损害、支出

等一切费用（含律师费）。如采购人因此而遭致损失的，成交供应商应赔偿该损失。

### 商务要求

1. 付款方式：采购人于政府采购合同签订生效、具备实施条件且财政资金到位后5个工作日内支付首年合同总额的90%作为本项目预付款，项目投入使用之日起一年后无服务质量问题支付上一年度剩余服务费用，每年度服务费用支付方式以此类推，全部服务期结束后支付剩余全部款项。

2. 服务质量要求：符合国家、山东省、烟台市现行有关规定及合同约定。

3. 项目准备期：接到采购人通知后5个日历日内完成全部线路接入，并开始提供政务外网接入服务。

4. 服务期限：自合同签订之日起1年，合同期满后乙方服务质量良好且经双方协商无异议后可续签合同，续签合同一年一签，连续续签合同累计不超过5年。

5. 服务地点：采购人指定地点。

6. 售后服务响应时间：提供全年7×24小时响应服务，对用户反应的任何问题须0.5小时内响应，1小时内到达现场，2小时内解决问题。