2024-2027年广西电子政务外网广域网数字专线线路项目采购方案

一、基本情况

**（一）项目名称**

项目名称：2024-2027年广西电子政务外网广域网数字专线线路项目

**（二）项目建设依据**

《广西壮族自治区大数据发展局关于印发广西电子政务外网横向接入方案的通知》（桂数发〔2021〕11号）；

《自治区党委办公厅 自治区人民政府办公厅关于印发〈广西政务数据资源管理与应用改革实施方案〉的通知》（厅发〔2019〕141号）；

《广西壮族自治区人民政府办公厅关于印发广西政务信息化项目建设管理办法（试行）的通知》（桂政办发〔2021〕21号）；

《广西壮族自治区大数据发展局关于印发广西电子政务外网管理办法》（桂数发〔2020〕9号）等有关文件。

**（三）项目现状**

广西电子政务外网广域网数字专线线路服务是广西电子政务外网的重要组成部分，支撑连接全区电子政务外网广域骨于网区、市、县三级的传输线路，保障网络和应用的安全。目前的广域网线路服务将于2024年6月30日到期，安全资源池服务将于2024年9月30日到期，态势感知服务将于2024年11月30日到期。到期后如不继续采购，一是广域网缺少传输线路，网络无法组建，全区电子政务外网的连通性将受到影响；二是政务外网网络及所承载的应用缺少安全防护，将存在安全风险。

**（四）项目目标、规模、周期、内容**

**1.项目目标**。不断完善电子政务外网基础网络，切实强化电子政务外网的运行维护管理，规范政务外网建设管理，不断提升电子政务外网的支撑能力和服务水平，为各单位提供更稳定更可靠的网络支撑，为全区政务数据“聚通用”工作的深入推进夯实基础。

**2.项目规模**。广西电子政务外网广域网数字专线线路26条622M二级网数字专线电路和218条155M三级网数字专线电路，电子政务外网安全资源池服务和态势感知服务。

**3.项目内容**。提供广西电子政务外网广域网数字专线线路服务，包括但不限于以下内容：两个不同运营商的各13条622M二级网数字专线电路和109条155M，总共26条622M二级网SDH数字专线电路，218条155M三级网MSTP数字专线电路，以及安全资源池服务和态势感知服务等。

**4.项目周期。**本项目服务周期为3年，其中线路服务使用从2024年7月1日起，安全资源池从2024年10月1日起，态势感知服务从2024年12月1日起。

二、采购需求

**（一）广域网线路需求**

提供26条（不同运营商各13条）622M二级网SDH数字专线线路和218条（不同运营商各109条）155M三级网MSTP数字专线线路，具体参数要求和服务要求如下：

|  |  |  |
| --- | --- | --- |
| 广域网线路服务 | 技术参数要求 | 1.单条端到端线路可用率≥99.90%。  2.单条端到端线路误码率，SDH线路≤10E-7。  3.单条端到端线路故障率≤1次/4个月、所有端到端线路累计障率≤4次/1个月。  4.26条622M二级网SDH数字专线线路，218条155M三级网MSTP数字专线线路，要求点对点提供独享带宽，全程不进行IP层转发，不得利用VPN组网，线路质量应符合国家相关标准和规定。  5. 双物理路由要求。对自治区和13个市，109个县（区）要求网络传输服务提供商提供的SDH线路和MSTP线路必须是双物理路由接入，即从两个不同通讯局的两根不同光缆线路（必须是不同物理路由）接入互联点用户节点。同缆不同芯的方式实现环路不算不同的物理路由。  6. 用户传输端设备具备双电源供电。 |
| 服务要求 | 1.以所有互联点的用户端路由器和交换机端口为界面，网络传输服务提供商负责将SDH数字线路和MSTP线路接至路由器和交换机的端口，路由器和交换机之前所涉及的设备、线缆及材料（包括光端机、各类协议转换器、连接或转换数据线缆、光衰减器、连接用户端设备使用的六类网线、光纤等）全部由网络传输服务提供商提供，并负责接入设备的安装、调试及接入线路的联调。  2.所有用户故障申告由网络传输服务提供商的自治区级公司统一受理，由自治区级公司负责协调相关互联点所在地分公司和相关技术人员，全程跟踪故障的响应、处理和解决，并在故障申告后3个工作日内以书面形式反馈故障申告用户。网络传输服务提供商应向业主提供一份自治区级公司和所有互联点所在分公司业务人员、技术人员（如有相应的技术资格证书，请提供）和联系人员名单，该名单人员原则上在服务期内保持不变，如因特殊原因确需要变动，应在人员调整后15天内以书面形式告知业主。  3.网络传输服务提供商提供7\*24小时电话服务热线和传真服务热线，并确定专人联系。  4.对自治区至各市的端到端线路：在故障发生时，用户提出申告后30分钟内响应，1小时到现场，2小时内恢复。  5.对各市到县（市、区）的端到端线路：在故障发生时，用户提出申告后1小时内响应，2小时到现场，3小时内恢复。  6.如果网络传输服务提供商因自身业务扩容或维修线路需对其城域物理光缆进行割接，网络传输服务提供商应该评估这个行为是否可能会导致自治区网络中心所租用的任一端到端线路发生中断，无论中断时间长短，网络传输服务提供商应该将该行为所产生的风险降至最低，并至少提前一天以传真或书面的方式通知自治区网络中心将要发生的行为。  7.网络传输服务提供商应每月向业主提交运行分析报告（包括所有端到端线路的可用情况、线路流量报告、当月故障清单、故障详细原因、故障发生时间和结束时间等）。每条端到端线路流量报告记录自治区网络中心和13个市节点端口，以一小时为单位按IN、OUT分类记录，每天记录24次，每天一张以图表方式提供，并给出每天和本月的最大值、最小值、平均值。  8.网络传输服务提供商应每半年到所有互联点对提供的所有端到端线路、设备、线缆等经行巡检，并将巡检结果以书面形式递交给业主。  9.线路中断及质量问题的赔偿承诺。除不可抗力的因素外（不可抗力的因素定义：（1）自然灾害、如台风、洪水、冰雹、地震；（2）政府行为，如征收、征用；（3）社会异常事件，如罢工、骚乱。），网络传输服务提供商在接到用户申告后，应在承诺时间内使线路恢复正常。如超过承诺恢复时间则每超过1小时减免该条端到端线路当月租费的10%直至该条线路恢复为止。  10.网络传输服务提供商应详细描述每条线路端到端链接情况，包括线路端到端链接所涉及的通讯局、传输设备（SDH、PDH等）、转换设备、ODF、DDF等，并要求线路端到端链接的中间节点越少越好。 |

**（二）安全资源池服务需求**

提供安全资源池平台管理软件、安全组件、基础硬件系统、定制开发和运营保障服务等，具体服务需求如下：

|  |  |  |
| --- | --- | --- |
| 服务名称 | 数量 | 服务内容 |
| 安全资源池服务 | 3年 | 为电子政务外网数据中心提供三年期安全资源池服务，包括平台管理软件、安全组件、基础硬件系统、定制开发和运营保障服务5部分内容：  1.提供2套异构的安全资源池软件平台，分别部署于电子政务外网互联网业务区和公用业务区；实现物理服务器虚拟化管理并提供安全组件运行所需要的虚拟环境，实现对安全组件的管理、安全状态监测及预警、租户管理等，通过API接口兼容第三方厂家安全产品或安全组件，支持引入第三方安全产品运行。  2.提供不少于满足210个安全资源池租户账户和1000个应用系统安全防护需求的安全组件，至少具备访问控制、入侵防御、网页防篡改、安全审计等安全防护功能；提供不少于450个安全组件授权，至少包含132个云防火墙组件（108个500M /24个1G），84个Web应用防火墙组件，72个网页防篡改组件，159个安全审计组件，3个日志审计组件（每年可根据需求变更不超过总数的组件数量）；每种安全组件提供不少于2个可选品牌；每年可以根据使用情况进行一次组件更换。  3.提供满足安全资源池正常运行管理所需的基础硬件系统，配置物理服务器和交换机，为资源池运行提供计算、存储和网络资源，配置不少于16台服务器，其中不少于10台4路高性能服务器；配置不少于8台交换机，其中不少于4台高性能交换机。  4.提供基于安全资源池服务需求的定制开发服务，可基于各租户个性化流程需求定制相关功能；完善开放和标准化接口，支持第三方的安全资源组件接入；提供开放接口。  5.提供运营服务，保障安全资源池的正常运行、业务开展和安全事件及时处置；提供不少于1个固定驻场工程师进行驻场运营服务，提供全年5×8小时的现场运营服务，每年不少于20天的重要安全保障活动期间进行7×24小时的现场运营值守服务，完成日常的现场监测、系统巡检、缺陷管理、故障处理、上线服务、系统优化升级、应急保障、数据运营分析服务、运营报告编写、培训与技术支撑以及安全管理等工作。 |

**（三）态势感知服务需求**

提供提供态势感知软件平台服务、基础硬件系统服务、基于态势感知服务需求的定制开发服务、驻场运营及应急保障服务等。具体服务需求如下：

|  |  |  |
| --- | --- | --- |
| 服务名称 | 数量 | 服务内容 |
| 态势感知服务 | 3年 | 为电子政务外网提供三年期态势感知服务，态势感知平台监测采集范围覆盖自治区电子政务外网和云计算中心的网络流量和所有设备日志，态势感知平台支持≥5000台设备的日志采集，日志数据存储≥180天，支持对存储的日志数据进行实时查询分析与统计，支持≥44Gbps网络流量采集，网络流量元数据索引存储≥14天，网络流量元数据存储≥30天，存储的网络流量元数据可根据需要快速恢复进行在线查询；平台算力能够顺畅支撑监测大数据分析和各种态势展示需求。态势感知服务主要包括软件平台、基础硬件设备、定制开发和运维保障服务4部分内容：   1. 提供态势感知软件平台服务，包括态势感知大数据平台使用服务、态势感知基础业务服务、日志采集服务、资产管理服务、安全事件关联分析服务、威胁检测服务、风险评估服务、资产风险态势大屏展示服务、外部威胁态势大屏展示服务、安全运营态势大屏展示服务、漏洞管理服务、安全态势报表管理服务、安全数据展示服务、流量日志检索分析服务、大数据存储分析服务、调查分析服务、攻击链分析服务、场景分析服务、网络结构管理服务、威胁情报服务、漏洞知识库服务、外部威胁平台查询服务、安全事件监控分析服务、安全通报服务、设备运行安全监测服务、安全策略优化服务、配置及备份更新服务、应急响应处置服务、应用渗透测试服务、基础性安全评估服务、资产发现分析服务、应用失陷检测服务、流量深度风险分析服务、租户安全态势感知服务、全网网络流量与网络行为分析与可视化服务、租户级别安全态势分析展示服务、态势感知平台威胁情报升级、可视化定制服务。（对完成**态势感知系统的升级维保服务，提供本服务期内的威胁情报升级服务，包含了域名、URL、IP、MD5等多种格式。**） 2. 提供满足态势感知平台正常运行管理所需的基础硬件系统。配置≥13台的万兆网络流量采集分析硬件探针（流量探针1）；配置≥5台万兆网络流量采集分析器硬件探针（流量探针2），与流量探针1为不同厂商，形成流量探针异构；≥1台文件威胁鉴定探针、≥6台TAP分光分流设备、≥30台物理服务器（包含所需软件平台授权）、≥**2台配置接入交换机、**≥**2台配置管理交换机**（提供本服务期内软硬件设备维保服务，所有探针本服务期内的全功能特征库升级服务）。 3. 提供基于态势感知服务需求的定制开发服务。提供平台与网信办平台对接定制服务、与地市平台对接服务。 4. 提供驻场运营及应急保障服务，保障态势感知平台的正常运行、分析和安全事件及时处置；提供不少于2个固定驻场工程师进行驻场运营服务，提供全年5×8小时的现场值守服务，每年不少于20天的重要安全保障活动期间进行7×24小时的现场值守服务。重要时期安全检查服务、网络安全攻防演习服务、安全合规检查及指导服务。提供对客户每年不低于2次的原厂专项认证类网络安全专业技术培训；开展技术研究，输出研究报告或者论文。 5. 根据国家安全法规对政务外网态势感知完成服务期内每一年度的三级等保测评工作，并提供测评报告。 |