

采购合同

合同名称：覃塘区电子政务外网线路租用、网络安全及设备运维服务合同

项目编号：GGZC2024-G3-040242-GXKY

招标单位（甲方）：贵港市覃塘区人民政府办公室

供 应 商（乙方）：中国电信股份有限公司贵港分公司

签订合同地点：贵港市覃塘区

签订合同时间：2024年 11 月 22 日

合同书

采购计划号：_____ 合同编号：_____

采购人（甲方）： 贵港市覃塘区人民政府办公室

供应商（乙方）： 中国电信股份有限公司贵港分公司

项目名称： 覃塘区电子政务外网线路租用、网络安全及设备运维服务

项目编号： GGZC2024-G3-040242-GXKY

签订地点： 贵港市覃塘区 签订时间： _____

本合同为中小企业预留合同： （否）。

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、法规规定，按照公开招标 文件规定条款和乙方响应文件及其承诺，甲乙双方签订本合同。

第一条 合同标的

1. 项目一览表

序号	名称	技术服务内容	数量	单位	单价（元）	总价（元）
----	----	--------	----	----	-------	-------

1	覃塘区电子政务外网线路租用、网络安全及设备运维服务	<p>一、数据专线接入服务（服务期36个月）</p> <p>（一）1条3Gbps互联网主出口专线带宽，接入方式为光纤接入，提供24个互联网公网IP地址，互联网光纤通信线路到达各大门户网站的实测PING值：平均时延15ms，丢包率<1/1000。</p> <p>（二）173条100Mbps点对点数据专线接入服务，上下行速率100Mbps，时延<15ms，丢包率<1%。</p> <p>（三）光纤专线线路要求具有端到端全程网管监控功能，并实行7×24小时实时监控；</p> <p>（四）接入地点：招标人指定地点，铺设路线我公司自行勘探。</p> <p>二、网络安全服务</p> <p>（一）提供2台政务外网出口防火墙、2台互联网出口防火墙服务</p> <p>1. 单台基本配置</p> <p>（1）1U机架防火墙，提供1个MGMT接口，16个千兆电口，4个千兆Combo口，4个千兆光口，6个万兆光口，2个USB接口，提供以上接口后剩余扩展槽位1个，2个硬盘扩展槽；</p> <p>（2）为了后续业务需要，设备支持扩展2×40G接口卡；</p> <p>（3）实配冗余双交流电源、6个万兆多模光模块；</p> <p>（4）提供3年应用识别库、URL分类库、病毒特征库、入侵防御特征库升级服务；</p> <p>（5）提供3年原厂硬件质保服务。</p> <p>2. 性能功能参数</p> <p>（1）网络层吞吐量18Gbps，最大并发连接数500万，每秒新建连接数15万/秒；</p> <p>（2）支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求；</p> <p>（3）支持国密SM1/2/3/4算法；</p> <p>（4）●支持9000条以上的应用识别，且提示风险类型及风险级别，便于用户根据实际情况进行上网行为管理；</p> <p>（5）支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等；</p> <p>（6）可针对HTTP/HTTPS的安全策略来专门为Web应用提供保护。对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护；</p> <p>（7）●支持对检测到的攻击行为的前后报文进行自动化抓包功能，方便用户对攻击行为进行取证；</p> <p>（8）●支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署；</p> <p>（9）当终端流量流经设备时，设备可以分</p>	1	项	5127810.00	5127810.00
---	---------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---	---	------------	------------

（印）

	<p>析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时（比如将原厂商的摄像头换为其他厂商的摄像头）向用户发送日志，提示用户；</p> <p>(10) 发现病毒发送的告警信息，支持用户编辑告警内容；</p> <p>(11) 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率；</p> <p>(12) 支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略；</p> <p>(13) 支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；虚拟防火墙规格、资源分配、独立管理功能、独立配置保存功能、会话独立管理功能、NAT功能和独立路由功能；</p> <p>(14) ●支持IPsecVPN智能选路，根据应用和隧道质量调度流量。</p> <p>(二) 提供1套终端安全管理系统服务</p> <p>1. 产品支持与现有终端安全管理系统共用同一套管理控制中心进行管控；配置500个Windows客户端授权，客户端操作系统支持：WindowsXP_SP3及以上/WindowsVista/Windows7/10、WindowsServer2008/2012/2016/2019等；</p> <p>2. ●管理控制中心支持双因子认证登录方式，支持设置登录账号/密码输入错误的锁定次数、锁定时间；</p> <p>3. 支持根据分组、计算机名称、IP地址、操作系统、在线状态等条件筛选终端进行管理，支持单点维护功能；</p> <p>4. 支持通过图形化展示终端部署统计、终端安全趋势、终端更新状态、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息；</p> <p>5. 支持定时公告功能，可配置开机显示、周期显示和立即推送；</p> <p>6. ●客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新，支持设置不同终端类型设置和每批次观察时长；</p> <p>7. 支持终端“防退出”、“防卸载”密码保护，支持设置自我保护功能，防止客户端进程被恶意终止、注入、劫持；</p> <p>8. 支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本；</p> <p>9. 支持手动添加、导入、导出黑白名单，支持通过文件数字签名添加黑白名单管理；</p> <p>10. 支持扫描所有文件和仅扫描程序及文档</p>			
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

	<p>文件设置，支持对压缩包文件设置最大扫描层数和大小；</p> <p>11. 支持扫描资源占用设置，可设置不限制、均衡型、低资源等三种模式；</p> <p>12. ●支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护；</p> <p>13. 支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录；</p> <p>14. 支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁；</p> <p>15. 支持对Windows操作系统、IE、.NETFramework、Office、Adobe、硬件驱动更新等软件进行补丁修复，支持补丁类型和级别包括： 安全更新、重要补丁、功能补丁、可选补丁等；</p> <p>16. ●支持灰度发布的漏洞修复策略，将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复；</p> <p>17. 支持开启自动修复漏洞，包括设置开机时修复、随机延迟执行、间隔修复和按时间段修复等；</p> <p>18. 支持当影响到编辑Office文档时进行提醒，可取消此次修复任务；</p> <p>19. 支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口、IP范围；</p> <p>20. 支持对终端各种外设（USB存储、硬盘、存储卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB口、串口、并口、1394、PCMCIA）设置使用权限，并支持生效时间设置；</p> <p>21. ●支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源，并支持通过设备名称、PID/VID、实例路径等多维度进行添加例外或加黑；</p> <p>22. 支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理；</p> <p>23. ●支持对终端节能管理，支持对长时间运行、定时关机、空闲节能、工作时间外开机等节能类型设定策略，支持仅提示、关机、注销、锁定、关闭显示器、锁定+关闭显示器、休眠和睡眠处理；</p> <p>24. 支持对网卡进行防护，支持阻止终端修</p>				
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

	<p>改IP地址、使用动态IP地址、热点创建等，可自定义提示内容和生效时间。</p> <p>(三) 提供1套态势感知系统平台服务</p> <ol style="list-style-type: none"> 1. 标准2U机架式设备，配置4个千兆电口，内存96GB，配置960GSSD+6×8TB SATA存储硬盘，冗余交流电源；提供现场安装和培训服务，提供三年的软硬件质保、三年威胁情报更新授权； 2. 能够接收云端提供的威胁情报，对网络中的威胁事件进行发现和告警；威胁情报可支持在线和离线升级两种方式； 3. ●支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒索软件、流氓推广、窃密木马、网络蠕虫、远控木马、其他恶意软件，并可自定义威胁情报； 4. ●支持与云端威胁情报中心联动，可对攻击IP、C&C域名和恶意样本MD5进行一键搜索，查看基本信息、相关样本、关联URL、可视化分析、域名解析、注册信息、关联域名、数字证书等； 5. 威胁支持按照威胁事件视图、受害主机视图、受害服务器视图、受害用户视图、威胁视图进行分类展示； 6. 威胁告警类别需要包括webshell上传、网页漏洞利用、网络攻击、APT事件、远控木马、窃密木马、僵尸网络、勒索软件、黑市工具、网络蠕虫、恶意样本执行、恶意样本投递； 7. 提供一键查询威胁事件详情，威胁事件详情需要包括告警来源、威胁类型、威胁名称、威胁情报IOC、已经相关的会话记录； 8. 支持与本项目的防火墙进行联动，发现威胁事件后支持对攻击IP、恶意域名和受害资产的流量进行阻断，将策略下发给防火墙，由防火墙执行阻断； 9. 支持与杀毒软件或终端安全管理系统进行联动，实现恶意文件的查杀、被感染主机的网络隔离； 10. 威胁事件的追踪溯源分析能力，可基于事件告警进行调查分析，对攻击过程进行可视化展现，可展示命中威胁情报的内部主机之间的连接行为，能输出完整的基于时间序列和攻击链的事件报告，事件报告支持word格式导出； 11. 本地分析平台产生告警中出现的C&C地址可以一键进行云端威胁情报中心进行分析追踪，查看地址的基础信息、威胁检测结果、地址解析变化、关联样本； 12. 流量日志包含DNS、HTTP、TCP、SMTP等流量行为日志，并可按照以上应用协议的各个关键字段搜索日志； 13. 流量日志记录包含以下字段：时间、IP 				
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

	<p>、IP地理位置、端口、域名、HTTP头信息、SQL语句、邮件收件人和发件人、文件名、文件MD5、应用层payload前100字节；</p> <p>14. 支持搜索文件访问行为，并展示还原流量中文件的MD5和文件名；</p> <p>15. 可自定义选择报表生成的时间、可以按照安全告警和流量日志生成报表；</p> <p>16. 告警报表中需要包括告警事件、受害主机、受害服务器、受害用户等部分，可以按照需要生成分项或是汇总报表导出；</p> <p>17. 日志报表内部需要包括网络日志、终端日志、告警日志三个部分，报表内容可以按照汇总报表和分项报表进行生成导出；</p> <p>18. ●对于重要的未知威胁告警，将告知客户攻击的相关背景信息（攻击行业，受害范围）；</p> <p>19. ●能够对未知威胁告警进行处置，可设置不同状态对告警进行跟踪；</p> <p>20. 生成的报表内容可以按照危害的等级进行升序或是降序的方式排列；</p> <p>21. 支持在线升级和离线升级两种升级方式，并支持定时自动升级；</p> <p>22. 支持新增并管理用户，可控制用户使用权限；支持用户初次登陆强制修改密码功能；</p> <p>23. 支持集群部署，可水平扩展至多台设备集群，以应对大量数据情况，可支持PB级数据检索。</p> <p>（四）提供1套态势感知系统流量探针服务</p> <p>1. 标准1U机架式设备，配置4个千兆电口，2个万兆光口，2个接口扩展插槽，硬盘存储2TB，交流电源，含威胁检测系统软件；提供现场安装和培训服务，提供三年的硬件维保服务、三年软件及检测规则升级服务；</p> <p>2. 系统应用层吞吐量1Gbps，并发会话数150万/s，新建会话数1万/s；</p> <p>3. 支持对常见扫描以及远控木马的检测；</p> <p>4. 能够通过双向流量检测的方式发现可利用的SQL注入、跨站、命令执行等web漏洞，并记录已经发生过的攻击事件和相关报文；</p> <p>5. 支持通过沙箱技术精确检测多种针对PHP语言环境的WEBSHELL攻击；</p> <p>6. ●支持对web漏洞利用检测规则、入侵检测规则等多种规则的配置，选择，可以有针对性的选择部分规则开启；</p> <p>7. ●能够对网络通信行为进行还原和记录，以供安全人员进行取证分析，还原内容包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为；</p> <p>8. 支持对流量中出现文件传输行为进行发</p>				
--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

	<p>现和还原，将文件MD5发送至分析平台；</p> <p>9. 支持对HTTP、SMTP、POP3、IMAP、FTP、MSSQL、MYSQL、ORACLE、POSTGRESQL、LDAP、DNS、SSL、TDS、TFTP等协议的分析还原；</p> <p>10. ●支持对文件传输协议进行还原和分析，可分析的协议包含如下：邮件（SMTP、POP3、IMAP、webmail）、Web（HTTP）、FTP、SMB；</p> <p>11. 支持对常见可执行文件的还原：EXE、DLL、OCX、SYS、COM、apk等；</p> <p>12. 支持对常见压缩格式的还原：RAR、ZIP、GZ、7Z等；</p> <p>13. 支持常见的文档类型的还原：word、excel、pdf、rtf、ppt等；</p> <p>14. 支持将还原后的文件传送至威胁感知系统分析平台进行检测分析；</p> <p>15. ●支持将抓取的原始流量包保存于本地以供后续分析和取证使用；</p> <p>16. 支持在线升级和离线升级两种升级方式，并支持定时自动升级；</p> <p>17. 支持实时监控设备的CPU、内存、存储空间使用情况；</p> <p>18. 支持分析统计1天或1周时间内的文件还原数量情况；</p> <p>19. 支持分析统计1天或1周时间内的各个应用流量的大小和分布情况；</p> <p>20. 支持提供威胁告警以SYSLOG格式输出给第三方设备；</p> <p>21. 支持IPv4网络和IPv6网络两种部署场景，支持两种网络流量均进行分析还原；</p> <p>22. 支持分布式部署，可以多台采集器同时部署于客户网络不同位置并将数据传输到同一套分析平台。</p> <p>（五）提供1台漏洞扫描服务</p> <p>1. 单台基本配置</p> <p>（1）硬件：1U高机架式硬件架构，1T硬盘容量，1个管理口，5个以太网千兆业务电口，支持1个接口扩展槽位，具备14个以太网千兆接口或4个万兆接口的可扩展能力；</p> <p>（2）配置3年漏洞库（含操作系统、数据库和WEB应用的漏洞规则库）升级授权函，128个IP扫描数量；</p> <p>（3）提供3年原厂硬件质保服务。</p> <p>2. 性能功能参数</p> <p>（1）单任务系统、数据库、基线扫描IP总并发120个，系统、数据库、基线扫描任务总并发6个；</p> <p>（2）支持持分布式、单机部署方式；</p> <p>（3）支持IPV4、IPV6环境的漏洞扫描；</p> <p>（4）●支持通过SSH、SMB、TELNET、RDP、POP、POP3、IMAP、FTP、WMI、RSH、REXEC</p>				
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

	<p>、WINRM、SNMP等协议对目标主机进行登录扫描；</p> <p>(5) 支持系统漏洞扫描、WEB漏洞扫描、安全基线漏洞扫描、数据库漏洞扫描功能和口令猜解功能；</p> <p>(6) 系统支持检测的系统漏洞数20万，覆盖CVE、CVSS、CNVD、CNNVD、CNCVE、Bugtraq多种漏洞标准；</p> <p>(7) 支持针对工控专用网络设备的漏洞扫描，支持多种漏洞验证方式，漏洞报表涵盖漏洞描述、漏洞参考链接和详尽的安全修补方案建议，支持邮件、短信、SNMPtrap、SYSLOG、FTP等多种告警方式；</p> <p>(8) ●系统支持批量导入认证信息，能够批量验证登录认证信息是否正确；</p> <p>(9) 系统支持国产操作系统、数据库的扫描，国产操作系统包含中标麒麟、凝思、华为欧拉、深度、红旗、中兴新支点，国产数据库包括神通、人大金仓、南大通用、达梦等；</p> <p>(10) ●系统支持不同维度的漏洞库视图，包含漏洞类别维度、操作系统维度、漏洞发现时间维度、服务维度、应用维度；</p> <p>(11) 系统支持自适应网络扫描，根据网络状况自动调整发包速率，减少对用户网络的影响；</p> <p>(12) 系统支持Web登录认证扫描，支持基于Cookie认证、Form认证、Basic认证、NTLM认证、Session认证、Digest认证的Web应用系统扫描；</p> <p>(13) ●系统支持对网络不可达的目标提供离线基线核查功能，离线核查工具支持常见操作系统、数据库、中间件、网络设备和安全设备，离线检查结束后支持将检查结果批量导入扫描器中，便于统一分析和输出报告。</p> <p>(六) 提供1套智能运维平台系统服务1. 根据自治区信息中心技术要求，实现跟自治区电子政务外网一体化运维平台对接，包含接口文档分析，资源数据、子资源数据、拓扑关系、资源性能、端口性能、资源告警、端口告警的采集及推送上报；</p> <p>2. 推送现网运维平台产生的告警，针对API提供的三种级别的告警，分别对应运维平台系统的三种级别告警，分别是：“特级”对应“紧急”，紧急对应“重要”，“一般”对应“次要”；</p> <p>3. 网络设备信息推送：发送告警的指标：设备离线、CPU利用率过高、内存利用率过高等；</p> <p>4. 网络端口信息推送：发送告警的指标：输入\输出丢包率过高、输入\输出错包率过高</p>			
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

	<p>、端口断开、端口利用率过高等；</p> <p>5. 物理机设备信息推送：发送告警的指标：设备离线、CPU利用率过高、内存利用率过高等；</p> <p>6. 包含运维软件工程师上门安装、调试技术支持服务；</p> <p>7. 为保证实施过程中运维平台稳定性以及对兼容性，运维平台提供3年原厂服务。</p> <p>8. 提供承载智能运维平台系统的服务器配套服务。</p> <p>（七）提供1套Web应用防火墙系统服务</p> <p>1. 采用B/S设计架构，1U机架式硬件架构，标配单电源，1T硬盘，提供2个以太网千兆管理接口+4个千兆电口（2组Bypass），1个接口扩展槽位；</p> <p>2. 应用层吞吐量300Mbps，HTTP并发连接数20万、HTTP每秒新建连接数6K；</p> <p>3. 支持透明流模式、透明代理模式、反向代理模式、路由牵引模式、镜像检测模式及镜像阻断模式等部署模式，支持注入攻击防护、CC攻击防护、跨站脚本攻击防护、爬虫攻击防护、恶意软件防护等多种防护能力，支持web漏洞扫描、弱密码检测、黑白名单等多种高级防护能力，内置网页防篡改客户端及管理能力，能够对实时态势进行检测以及进行网站一键断网，支持支持IPv4、IPv6双栈防护，支持生成虚拟补丁功能；</p> <p>4. 保护网站站点数量无限制，3年特征库升级授权，设备本身可做网页防篡改的管理平台，设备本身自带一套软件。</p> <p>三、利旧安全设备特征库升级服务</p> <p>1. 提供2台互联网防火墙服务授权，含3年防火墙AV防病毒安全授权、IPS特征库升级服务授权和上网行为管理特征库升级服务授权；</p> <p>2. 采购人现有的网络安全设备（6台安全防火墙及2台入侵防御安全设备）2025年合同服务期到期后，我公司针对现有的网络安全设备提供2年服务授权和设备维保服务。</p> <p>四、运维服务</p> <p>1. 提供机房2台核心交换机与2台核心路由器3年维保服务</p> <p>（1）提供核心交换机、路由器日常调试、维护服务，保障接入各单位业务正常接入电子政务外网；</p> <p>（2）设备安全巡检。按月、季度、年进行安全巡检，主要包括深入现场、检查设备、了解设备运行情况、仔细观察各个安全节点的可靠性；</p> <p>（3）提供网络架构优化、调整技术支持、故障排除；</p> <p>（4）提供网络攻防专项技术支持服务；</p>				
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

	<p>(5) 线路整理, 对接入的凌乱跳线进行整理整治, 确保各设备间连接的线缆干净整洁。</p> <p>2. 提供各租用单位接入路由器设备维保服务</p> <p>(1) 对专线租用单位接入路由器或交换机设备进行维保服务、数据添加, 配合专线租用单位解决本单位的网络故障, 协助接入电子政务外网, 保障上级部门推广的新业务系统上线。提供每个季度一次对租用单位主设备进行除尘保洁、现场巡检服务, 保障网络主设备、接入电线、接入网线整齐与干净。整改产生所需易耗易损材料费用由我公司承担, 服务期3年;</p> <p>(2) 提供路由器设备备件服务。备件支持IPv4特性:支持LLDP、802.1Q、802.1P、802.3ad、STP/RSTP/MSTP、DHCP Snooping等以太网功能;支持端口镜像;支持静态路由、RIPv1N2、OSPFv2、BGP、S-IS、策略路由、路由策略等;支持VRRP、FTP、TFTP, 支持静态/动态NAT、静态/动态NAPT、VPNNAT等支持DHCP Server/Relay、Client;支持DNS地址解析、智能DNS;支持NTP Server/Client IPv6特性:支持静态路由、RIPng、OSPFv3、BGP4+、ISISv6、等价路由、策略路由等;支持VRRPv3;支持手工隧道、自动隧道、ISATAP隧道、支持GRE隧道等组播:支持IGMPv1, v2, v3;支持PIM-DM、PIM-SM、PIM-SSM等组播路由协议;支持组播静态路由MPLS:支持MPLS转发。</p> <p>3. 提供IPv6路由规划调试服务</p> <p>(1) 服务内容涵盖覃塘区电子政务外网本级以及所有接入单位IPv6地址规划与改造;</p> <p>(2) 包含实现与自治区电子政务外网骨干网IPv6路由对接服务。</p> <p>4. 等保整改专项服务</p> <p>(1) 安全制度建设: 结合采购人的业务需要, 建立符合其单位实际情况的安全制度体系, 需包括信息安全方针、安全策略、安全管理制度、安全技术规范以及流程等(1次);</p> <p>(2) 安全运维服务: 根据等保制度要求网络安全巡检1年服务(每季度1次), 对终端、服务器系统提供漏扫服务, 确保网络安全运营处于高效良性状态;</p> <p>(3) 安全意识培训服务: 现场安全意识培训1次;</p> <p>(4) 机房服务: 对过期的消防系统按原配置标准进行换新, 对机房监控留存时长超过6个月以上。</p> <p>(5) 配合等保测评单位进行等保测评服务, 确保各软硬件达到二级等保要求并能通过</p>				
--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

		二级等保测评。				
人民币合计金额（大写）： <u>伍佰壹拾贰万柒仟捌佰壹拾元整(¥ 5127810.00)</u>						

2. 合同合计金额包括但不限于满足本次竞标全部采购需求所应提供的服务，以及伴随的货物和工程（如有）的价格；包含竞标服务、货物、工程的成本、运输（含保险）、安装（如有）、调试、检验、技术服务、培训、税费等所有费用。如公开招标文件对其另有规定的，从其规定。

第二条 质量保证

乙方所提供的服务及服务内容必须与响应文件承诺相一致，有国家强制性标准的，还必须符合国家强制性标准的规定，没有国家强制性标准但有其他强制性标准的，必须符合其他强制性标准的规定。

第三条 权利保证

1. 乙方应保证所提供服务在使用时不会侵犯任何第三方的专利权、商标权、工业设计权等知识产权及其他合法权利，且所有权、处分权等没有受到任何限制。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或者任何合同条文、规格、计划、图纸、样品或者资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。乙方的保密义务持续有效，不因本合同履行终止、解除或者无效而解除。

第四条 服务期限和验收

1. 服务完成期限： 合同签订之日起36个月 ， 服务地点： 贵港市。
2. 乙方应按响应文件的承诺向甲方提供相应的服务，并提供所服务内容的相关技术资料。
3. 乙方提供不符合响应文件和本合同规定的服务成果， 甲方有权拒绝接受。
4. 乙方完成服务后应及时书面通知甲方进行验收， 甲方应在收到通知后七个工作日内进行验收，逾期不开始验收的，乙方可视同验收合格。验收合格后由甲乙双方签署验收单并加盖采购人公章，甲乙双方各执一份。
5. 甲乙双方应按照《广西壮族自治区政府采购项目履约验收管理办法》、双方合同、响应文件验收。
6. 甲方在初步验收或者最终验收过程中如发现乙方提供的服务成果不满足响应文件及本合同规定的， 可暂缓向乙方付款，直到乙方及时完善并提交相应的服务成果且经甲方验收合格后，方可办理付款。

7. 甲方验收时以书面形式提出异议的，乙方应自收到甲方书面异议后五个工作日内及时予以解决，否则甲方有权不出具服务验收合格单。

第五条 售后服务及培训

1. 乙方应按照国家有关法律法规和本合同所附的《售后服务承诺》要求为甲方提供相应的售后服务。

2. 甲方应提供必要测试条件（如场地、电源、水源等）。

3. 乙方负责甲方有关人员的培训。培训时间、地点：贵港市。

第六条 付款方式

1. 合同金额：人民币伍佰壹拾贰万柒仟捌佰壹拾元整（¥5127810.00）

2. 付款方式：乙方完成所有设备安装调试并验收合格后，甲方在验收合格后30个工作日内付款人民币叁佰零贰万零柒佰柒拾元整（¥3,020,770.00）；剩余合同款项分两次支付，甲方于2026年6月30日前付款人民币壹佰零伍万叁仟伍佰贰拾元整（¥1,053,520.00）；于2027年6月30日前付款人民币壹佰零伍万叁仟伍佰贰拾元整（¥1,053,520.00）给乙方。

第七条 履约保证金

本项目不收取履约保证金。

第八条 税费

本合同执行中相关的一切税费均由乙方负担，合同另有约定的除外。

第九条 违约责任

1. 除不可抗力原因外，乙方没有按照合同规定的时间提供服务的，甲方可要求乙方支付违约金。每推迟一天按合同金额的 1% 支付违约金，该违约金累计不超过合同金额的 1%。

2. 乙方提供的服务如侵犯了第三方合法权益而引发的任何纠纷或者诉讼，均由乙方负责交涉并承担全部责任。

3. 甲方延期付款的，每天向乙方偿付延期款额 1% 滞纳金，但滞纳金累计不得超过延期款额 1%。

第十条 不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十一条 合同争议解决

1. 因服务质量问题发生争议的，应邀请国家认可的质量检测机构进行鉴定。服务符合标准的，鉴定费由甲方承担；服务不符合标准的，鉴定费由乙方承担。

2. 因履行本合同引起的或者与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地有管辖权的人民法院提起诉讼。

3. 诉讼期间，本合同继续履行。

第十二条 合同生效及其它

1. 合同经双方法定代表人或者授权代表签字并加盖单位公章后生效（委托代理人签字的需后附授权 委托书，格式自拟）。

2. 合同执行中涉及采购资金和采购内容修改或者补充的，须经财政部门审批，并签书面补充协议报 财政部门备案，方可作为主合同不可分割的一部分。

3. 本合同未尽事宜遵照《中华人民共和国民法典》有关条文执行。

第十三条 合同的变更、终止与转让

1. 除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或者终止。

2. 乙方不得擅自转让其应履行的合同义务。

第十四条 签订本合同依据

1. 成交通知书；

2. 竞标报价表；

3. 商务要求偏离表和技术要求偏离表；

4. 服务方案；






5. 响应文件中的其他相关文件。

6. 上述合同文件互相补充和解释。如果合同文件之间存在矛盾或者不一致之处， 以上述文件的排列顺序在先者为准。

第十五条 本合同一式四份，具有同等法律效力，财政部门（政府采购监管部门）、采购代理机构各一份，甲乙双方各一份（可根据需要另增加）。

本合同甲乙双方签字盖章后生效，自签订之日起七个工作日内，甲方应当将合同副本报同级财政部门备案。

本合同自签订之日起2个工作日内，甲方应当将采购合同在广西壮族自治区财政厅指定的媒体上公告。

<p>甲方：（章）</p>  <p>2020年 11月 22日</p>	<p>乙方：</p>  <p>2020年 11月 22日</p>
<p>单位地址：贵港市覃塘区行政中心主楼617号</p>	<p>单位地址：贵港市港北区中山北路11号</p>
<p>法定代表人：</p> 	<p>法定代表人：</p> 
<p>委托代理人：</p> 	<p>委托代理人：</p>
<p>电话：</p>	<p>电话：</p>
<p>开户银行：</p>	<p>开户银行：中国工商银行贵港支行</p>
<p>账号：</p>	<p>账号：2111710009221023007</p>
<p>邮政编码：</p>	<p>邮政编码：537100</p>

附件1:

服务承诺

一、 供应商承诺具体事项:

项目整体质保期 36 个月（整体自验收合格之日起算）；质保期内设备本身质量出现问题或由于设备本身质量原因造成的任何损伤或损坏，我公司会及时给予免费维修或免费更换，由此引起的施工费、人工费、材料费等其它一切费用由我公司负责。

二、 服务期责任:

(一) 租赁的数据专线免费提供维修服务：提供7*24小时电话支持服务，质保期内线路出现故障，按照项目服务需求表中规定的时限进行处理。规定时限内无法修复的，我公司会提供同品牌备用设备及必要的零

配件或备件进行替换，以免影响整套系统的正常运行。

(二) 采购的网络入侵防御系统、录像机硬盘等设备质保期内，提供7*24

小时电话支持服务。电子政务外网机房网络、设备发生故障时，按照项目服务需求表中规定的时限进行处理。规定时限内无法修复的，我公司会提供同品牌备用设备及必要的零配件或备件进行替换，以免影响整套系统的正常运行。

(三) 免费提供完善的操作培训或技术培训方案，免费现场培训技术员2

名以上，保证熟练掌握全部功能为止；当用户网络需要扩展或升级时，负责免费提供相应解决方案；在服务期内，如国家政策进行网络调速，项目招标人应享受同等政策和待遇，我公司会给予调速。

二、 其他具体事项:

(一) 合同期内，如果有超出招标范围的新增或扩容线路扩容将低于同等价格提供线路，新增或扩容线路扩容不超出合同价的10%。

(二) 为每个接入单位切换原有网络。

(三) 1. 投入本项目设备配置清单：设备参数达到现行《广西电子政务外网市、县级节点技术规范》、《广西市、县级电子政务外网建设和运维指南》要求。2. 我公司所采购的设备与原有的设备完全兼容。

甲方（章）



2024年 11 月 22 日

乙方（章）



2024年 11 月 22 日

注：填不下时可另加附页

附件2:

保密协议书

甲方: 贵港市覃塘区人民政府办公室

乙方: 中国电信股份有限公司贵港分公司

鉴于: 甲乙双方正在就进行的招标采购项目, 项目名称: 覃塘区电子政务外网线路租用、网络安全及设备运维服务(项目编号: GGZC2024-G3-040242-GXKY), 需要取得甲方本项目相关业务和技术资料, 为此, 甲乙双方本着互惠互利、共同发展的原则, 经友好协商签订本协议。

第一条 保密资料的定义

乙方作为潜在投标人, 甲方披露给乙方的本项目相关业务和技术资料的书面或其它形式的资料和信息(简称: 保密资料), 但不包括下述资料和信息:

(一) 已经或将公布于众的资料, 但不包括甲乙双方或其代表违反本协议规定未经授权所披露的;

(二) 在任何一方向接受方披露前已为该方知悉的非保密性资料;

第二条 双方责任

(一) 甲乙双方互为保密资料的提供方和接受方, 负有保密义务, 承担保密责任。

(二) 甲乙双方中任何一方未经对方书面同意不得向第三方(包括新闻界人士)公开和披露任何保密资料或以其他方式使用保密资料。双方也须促使各自代表不向第三方(包括新闻界人士)公开或披露任何保密资料或以其它方式使用保密资料。除非披露

、公开或利用保密资料是双方从事或开展合作项目工作在通常 情况下应承担的义务(包括双方今后依法律或合同应承担的义务)适当所需的。

(三)双方均须把保密资料的接触范围严格限制在因本协议规定目的而需接触保密资料的各自负责 代表的范围内。

(四)除经过双方书面同意而必要进行披露外,任何一方不得将含有对方或其代表披露的保密资料复印 或复制或者有意无意地提供给他人。

(五)如果合作项目不再继续进行或其中一方因故退出此项目,经对方在任何时候提出书面要求,另一 方应当、并应促使其代表在五(5)个工作日内销毁或向对方返还其占有的或控制的全部保密资料以及包含 或体现了保密资料的全部文件和其它材料并连同全部副本。但是在不违反本协议其它条款的条件下,双方 可仅为本协议第四条之目的,保留上述文件或材料的复制件一份。

(六)甲乙双方将以并应促使各自的代表以不低于其对自己拥有的类似资料的照料程度来对待对方向 其披露的保密资料,但在任何情况下,对保密资料的照料都不能低于合理程度。

第三条 知识产权

甲乙双方向对方或对方代表披露保密资料并不构成向对方或对方的代表的转让或授予另一方对其商 业秘密、商标、专利、技术秘密或任何其它知识产权拥有的权益,也不构成向对方或对方代表转让或向对 方或对方代表授予该方受第三方许可使用的商业秘密、商标、专利、技术秘密或任何其他知识产权的有关 权益。

第四条 保密资料的保存和使用

(一) 甲乙双方中的任何一方有权保存必要的保密资料，以便在履行其在合作项目工作中所承担的法律、规章与义务时使用该等保密资料。

(二) 甲乙双方有权使用保密资料对任何针对接受方或其代表的与本协议项目及其事务相关的索赔、诉讼、司法程序及指控进行抗辩，或者对与本协议项目及其事务相关的传唤、传票或其他法律程序做出答复。

(三) 任何一方在书面通知对方并将披露的复印件抄送对方后，可根据需要在提交任何市、省、中央或其他对接受方有管辖权或声称对接受方有管辖权的监管团体的任何报告、声明或证明中披露保密资料。

第五条 争议解决和适用法律

本协议受中华人民共和国法律管辖并按中华人民共和国法律解释。对因本协议或本协议各方的权利和义务而发生的或与之有关的任何事项和争议、诉讼或程序，本协议双方不可撤销地接受中华人民共和国法院的管辖。

第六条 协议有效期

(一) 本协议有效期为贰年，自甲乙双方签字盖章之日起生效。

(二) 本协议一式四份，双方各执两份，具有同等法律效力。

甲方(盖章): 贵港市覃塘区人民政府办公室

地址: 贵港市覃塘区行政中心主楼617号

法定代表人或委托代理人:

联系电话:



乙方(盖章): 中国电信股份有限公司贵港分公司

地址: 贵港市港北区中山北路11号

法定代表人或委托代理人:

联系电话:

