

# 报价文件



项目名称：来宾市电子政务外网三期服务采购

项目编号：LBZC2026-G3-990053-CGZX

投标人名称：中国电信股份有限公司广西分公司

所投分标：标项 1

2026年7月8日

## 目录

1	▲开标一览表（报价表） .....	2
2	中小企业声明函 .....	23
3	关于符合本国产品标准的声明函 .....	24
4	关于符合本国产品标准的产品成本之和占所提供的全部产品成本之和的比例达到 80%以上的声明函 .....	28
4.1	关于符合本国产品标准的声明函 .....	29



# 1 ▲开标一览表（报价表）

来宾市政务服务和大数据发展局、北海市政府采购中心：

按你方招标文件要求，我们，本投标文件签字方，谨此向你方发出要约如下：  
如你方接受本投标，我方承诺按照如下开标一览表（报价表）的价格完成来宾市  
电子政务外网三期服务采购【招标编号：LBZC2026-G3-990053-CGZX】的实施。

## 开标一览表（报价表）（单位均为人民币元）

序号	服务名称	服务要求	数量	单位	价格（元）	备注（如果有）
(一)	网络服务	采购网络服务，提供以下配置设备，保障电子政务外网的稳定运行。	/	/	/	无
1	核心路由器	<p>服务提供 2 台核心路由器，提供三年服务。核心路由器满足如下配置：</p> <p>▲1、设备安全可靠，设备具有国产自主知识产权（提供证明材料）；</p> <p>2、采用控制、交换、转发物理分离设计，具备独立主控、交换矩阵、业务转发板卡，主控卡插槽 2 个，交换槽位 2 个，整机子卡槽位 16 个，电源模块插槽 2 个；设备主控板卡、业务转发板卡、业务子卡、风扇、电源等全部支持热插拔。</p> <p>3、设备配置主控卡 2 个，交换卡 2 个，业务母板卡 2 个，模块化电源 4 个，风扇 2 个；提供万兆光口（含模块）8 个，千兆光口（含模块）20 个；</p> <p>★4、交换容量 240Tbps，包转发率 86400Mpps；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>5、具备静态路由、RIP/RIPng、OSPFv2/v3、ISISv4/v6、BGP4/4+、兼容 EIGRP；</p> <p>6、IPsec 支持国家密码管理局商密 SM1、SM2、SM3、SM4 加密算法；</p> <p>7、具备 100G、50G、40G、25G、10G、GE、155M/622M/2.5G POS、E1/CE1、155M CPOS 等广域网接口</p> <p>8、具备 OSPF、BGP4、IS-IS 路由协议 SM3 认证；</p> <p>9、具备对配置文件、日志、操作记录文件进行 SM4 国密加密功能；</p>	1	项	436000	无

	<p>10、具备 FlexE 网络切片，支持信道化子接口的网络切片，具备 IFIT 随流检测，支持基于时延、带宽、安全性和可靠性等网络切片服务；</p> <p>11、具备 FIFO、PQ、FQ、WFQ、CBWFQ、LLQ、RSVP、CAR、HQoS、流量整形，HQoS 层数 5；</p> <p>12、具备 OSPFv2、OSPFv3、RIPv2、RIPng、ISISv4、ISISv6、BGP、BGP4+协议国密（SM3）安全认证功能；</p> <p>13、设备具备 GRE、IPSEC、NAT、L2TP 等多业务功能，如果需要配置相应的 LICENSE 和硬件板卡才支持则配置；</p> <p>★14、具备 ISIS for SRv6、OSPFv3 for SRv6、BGP for SRv6 具备 SRv6 BE、SRv6 TE Policy，支持 SRv6 业务链，具备 SRv6 Flex-algo 功能（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>★15、实际配置支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+；支持 IPv4 和 IPv6 双协议栈，具备静态路由、RIPng、OSPFv3、ISISv6、BGP4+等路由协议，具备 DHCPv6，支持 IPv4 向 IPv6 的过渡技术，包括 IPv6 手工隧道、6to4 隧道、GRE 隧道等；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>16、具备 SDWAN 控制器管理，提供网络 SDN 控制功能、网络管理功能、网络分析功能。配合控制器提供配置管理、网络设备状态/路由状态/宗流量状态采集、流量调度、路径调优、策略订制、网络切片、分片管理、业务保障、智能分析、故障定位等集中管控功能；</p> <p>17、采用双 WAN 口及以上设计，具备链路聚合与智能选路功能；具备双 WAN 双活/主备模式，并可实现策略路由；</p> <p>18、在 5 部委（安全认证和安全检测结果）目录内以及提供《网络关键设备证书》。</p>				
2	<p>汇聚路由器</p> <p>服务提供 5 台汇聚路由器，提供三年服务，满足汇聚需求。汇聚路由器满足如下配置：</p> <p>▲1、设备核心元器件 CPU，内存安全可靠，设备具有国产自主知识产权（提供证明材料）；</p> <p>★2、具备主控板卡和业务转发板卡；主控卡插槽 2 个，业务处理卡插槽 1 个，线卡插槽 8 个，电源模块插槽 2 个；配置主控卡 2 个，业务转发卡 1 个，100G 接口 1 个，万兆光口（含模</p>	1	项	220270	无

		<p>块) 4 个, 千兆光口 (含模块) 20 个, 千兆电口 8 个, 冗余双电源; (提供官网截图或产品彩页等证明材料)</p> <p>★3、交换容量 160Gbps , 包转发率 120Mpps; (提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告)</p> <p>4、具备 10G、GE、155M/622M/2.5G POS、E1/CE1、155M CPOS 等广域网接口;</p> <p>5、具备静态路由、静态路由、RIP、OSPF、BGP4、IS-IS、兼容 EIGRP;</p> <p>6、具备 IPSEC 国密 SM1、SM2、SM3、SM4 加密算法;</p> <p>7、具备 OSPF、BGP4、IS-IS 路由协议 SM3 认证;</p> <p>8、安全功能具备 CPU 保护、配置文件加密、日志加密功能;</p> <p>9、QOS 具备 FIFO、PQ、FQ、WFQ、CBWFQ、LLQ、RSVP、CAR、HQoS、流量整形, HQoS 层数 5。</p> <p>10、具备 PIM-SM/DM、PIM-SSM/SDM、MSDP、MVPN 组播路由协议;</p> <p>11、设备具备 GRE、IPSEC、NAT、L2TP 等多业务功能, 如果需要配置相应的 LICENSE 和硬件板卡才支持, 则配置;</p> <p>12、可靠性具备 IP FRR、MPLS FRR;</p> <p>13、具备 ISIS for SRv6、OSPFv3 for SRv6、BGP for SRv6 具备 SRv6 BE、SRv6 TE Policy, 具备 SRv6 业务链, 具备 SRv6 Flex-algo 功能, 具备 IFIT 随流检测, 具备 FlexE 网络切片、信道化子接口 支持基于时延、带宽、安全性和可靠性等网络切片服务;</p> <p>14、实际配置支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+; 具备 IPv4 和 IPv6 双协议栈, 具备静态路由、RIPng、OSPFv3、ISISv6、BGP4+等路由协议, 具备 DHCPV6, 支持 IPv4 向 IPv6 的过渡技术, 包括 IPv6 手工隧道、6to4 隧道、GRE 隧道等;</p> <p>15、采用双 WAN 口及以上设计, 具备链路聚合与智能选路功能; 具备双 WAN 双活/主备模式, 并可实现策略路由;</p> <p>16、在 5 部委 (安全认证和安全检测结果) 目录内以及提供《网络关键设备证书》。</p>				
3	接入路由器	提供满足 350 家委办局接入和 55 家重点单位备用线路需求, 提供三年服务。提供服务的设备	1	项	526600	无

配置满足如下要求：

▲1、路由器主机 CPU、内存等设备核心元器件安全可靠，设备具有国产自主知识产权（提供证明材料）；

▲2、路由器主机提供个万兆 SFP+光口 2 个，千兆电口 4 个，千兆光口 2 个，LAN 千兆电口 24 个，业务板槽位数 4 个，1 个 console 接口，交流电源。（提供官网截图或产品彩页等证明材料）

★3、交换容量:100Gbps,包转发率 40Mpps；  
（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）

4、具备千兆光、千兆电、E1/CE1、高速串口，155M POS 等接口，设备所有业务板卡支持热插拔；

5、具备配置文件加密功能，支持 history 文件加密功能；

6、具备静态路由、RIP、OSPF、BGP4、IS-IS、RIPng、OSPFv3、BGP4+、兼容 EIGRP；

7、具备并实配 RIPv2 和 OSPFv2 国密（SM3）认证功能；

8、具备 ACL 安全过滤、MPLS、PPP 加密、L2TP、GRE、策略路由、AAA、SSH、IPSec VPN；

9、QoS 具备 FIFO、PQ、FQ、WFQ、CBWFQ、LLQ、RSVP、CAR、流量整形，HQoS 层数 4；

10、设备具备双 Boot、双 IOS 备份功能；

11、设备主机系统不存在高、中风险级别安全漏洞；

12、具备 IPv4 和 IPv6 双协议栈，具备 IPv4 向 IPv6 的过渡技术，包括：IPv6 手工隧道、自动隧道、6to4 隧道、GRE 隧道、ISATAP 等；具备 IPv6 ND，IPv6 PMTU，IPv6 FIB，IPv6 ACL，SRv6，SRv6 Policy，ICMPv6，DNSv6，DHCPv6 等；

13、实际配置具备 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+；具备 IPv4 和 IPv6 双协议栈，具备静态路由、RIPng、OSPFv3、ISISv6、BGP4+等路由协议，具备 DHCPV6，具备 IPv4 向 IPv6 的过渡技术，包括 IPv6 手工隧道、6to4 隧道、GRE 隧道等；

14、采用双 WAN 口及以上设计，具备链路聚合与智能选路功能；具备双 WAN 双活/主备模式，并可实现策略路由。

4	网络控制器	<p>服务提供 1 套网络控制器，提供三年服务。网络控制器满足如下配置：</p> <p>1、平台架构：产品支持物理机及虚拟机部署，支持单节点、集群部署，支持集群任一节点出现故障后，业务不中断，本次实际采用单节点物理机部署，提供配套国产芯片硬件服务器 1 台；</p> <p>2、产品应具备一套软件，最大管理规模 20W 网元设备，及 70W 在线终端。具备单集群平滑扩容到多集群；</p> <p>3、具备意图开局，产品具备场景化模板建网，具备通过图形化，拖拽式定义配置模板，灵活定义变量，并应用于网络业务的批量创建；</p> <p>4、基于 VxLAN 的虚拟网络自动化部署能力，具备基于 GUI 的 Fabric 规划、配置和发放功能，端到端 VxLAN 网络自动化部署，实现业务隔离、一网多用；</p> <p>5、具备多种身份源组合的多因子认证，如账号+RADIUS token，密码+短信，TACACS+RADIUS Token，以及 SSL VPN 方式的双因子认证；</p> <p>6、具备多链路智能选优。可实现基于链路、应用的丢包、时延作为链路切换指标；具备基于链路负载作为链路切换指标。可设置主备链路规则和策略优先级等方式，对多链路进行智能选路；</p> <p>7、具备基于应用的多路包复制技术，具备自适应前向纠错 A-FEC 功能；</p> <p>8、具备通过空口调度策略，定义 VIP 用户优先接入网络，并享有专用带宽，无 VIP 用户流量时非 VIP 用户也能使用全部带宽；</p> <p>9、网络全息可视，在一张数字地图上清晰呈现网络、用户、终端和应用等四个维度的信息；</p>	1	项	137150	无
5	网络分析器	<p>服务提供 1 套网络分析器，提供三年服务。网络分析器满足如下配置：</p> <p>1、平台架构：产品具备物理机及虚拟机部署，具备单节点、集群部署，具备集群任一节点出现故障后，业务不中断，本次实际采用单节点物理机部署，提供配套国产芯片硬件服务器 1 台；</p> <p>2、数据采集：具备通过 Telemetry 采集数据，具备 GRPC 协议，支持 NetStream；</p> <p>3、具备基于分级区域查看多维度数据统计视图，系统具备设备环境、设备容量、网络性能、网络状态和网络协议五大有线类问题的智</p>	1	项	154150	无

		<p>能识别，提供问题列表，以及根因分析；</p> <p>4、接入回放：具备基于所有用户接入的关联、认证、DHCP 三个阶段，进行协议级别的过程呈现，提供用户接入过程问题的精细化分析，并提供用户接入失败的根因与排障建议；</p> <p>5、网络问题自动识别，主动预测，具备基于大数据分析和机器学习算法，自动识别常见网络问题：连接类、空口性能类、漫游类，以及设备环境、设备容量、网络性能和网络状态问题，包括认证失败、弱信号覆盖、非 5G 优先、网络拥塞等；</p> <p>6、具备基于应用/流配置 iPCA2.0/iFIT 实现对网络中丢包和时延进行实时监控；</p> <p>7、主流应用分析：系统具备精准识别 1K+主流应用，具备基于多种维度的应用流量统计，具备感知主流应用质量，识别质差应用，并对质差应用流进行故障定界。应用可视和质量感知具备边缘设备检测，可识别和感知东西、南北向应用及其质量，应用故障定界通过 IPCA 技术，进行应用路径呈现和应用故障定界定位。具备对接 Zoom、Teams 视频会议服务器，可对会议状态及与会人终端侧情况进行质量监控和分析。</p>				
6	管理交换机	<p>服务提供 2 台管理交换机，提供三年服务。管理交换机满足如下配置：</p> <p>1、全千兆三层交换机，千兆光口 24 个，万兆 SFP+光口 4 个，业务扩展槽(可扩展 10G、40G 接口)1 个，模块化电源插槽 2 个，Console 接口 1 个，2 个电源模块；</p> <p>2、交换容量 880Gbps；包转发率 330Mpps；</p> <p>3、CPU 使用国产自主安全 CPU, 交换芯片使用国产自主安全交换芯片；</p> <p>4、具备端口的负载均衡、具备 LACP，每个链路聚合组最少具备 32 个成员端口；</p> <p>5、MAC 地址容量 256K，FIB 表容量 80K；</p> <p>6、具备静态路由、RIP、OSPF/OSPFv3、ISIS/IS-ISv6、BGP/BGP4+等动态路由协议；</p> <p>7、具备 MPLS L3 VPN, MCE；</p> <p>8、QOS 支持 SP, WRR, WDRR, RR, SP+WRR, SP+WDRR 调度方式，支持流量整形；</p> <p>9、具备并实配横向、纵向虚拟化功能，具备分布式设备管理、分布式链路聚合，统一路由管理；</p> <p>10、具备并 VXLAN 功能，具备二层, 三层 VXLAN</p>	1	项	13120	无

		<p>网关，具备集中式分布式网关，支持 BGP-EVPN 协议；</p> <p>11、具备 CPU 保护功能，如 ICMP Flood 拦截、SYN Flood 攻击拦截等，具备 CPU 根据不同协议进行限速保护。</p> <p>12、安全可靠支持配置文件加密，保护设备配置信息泄露；</p> <p>13、具备并实配 RIP、OSPF 路由协议的国密认证功能；</p> <p>14、具备 IPFIX 或 sflow 或 Netstream；具备通过 Netconf 配置；支持 ZTP，零配置自动下发；</p> <p>15、具备 IPv4/IPv6 双协议栈、具备 IPV4-in-IPV6、IPV6-in-IPV4、IPV6-in-IPV6，具备 IPv6 over IPv4 隧道（手工隧道/6to4 隧道/ISATAP/GRE 隧道）。</p>				
7	网络安全等级保护测评	根据桂财建（2023）102 号，提供系统等保第三级每年测评报告，本次需提供 3 年服务。	1	项	150000	无
(二)	运维管理服务	提供运维管理服务，部署一套符合《广西电子政务外网技术规范（2022 年修订版）》要求的运维管理平台，提供三年维保服务；提供 1 名驻场服务人员，保障电子政务外网相关设备的正常运行。	/	/	/	无
1	运维管理平台	<p>服务提供 1 套运维管理平台，提供三年服务。运维管理平台满足如下要求：</p> <p>含 2 台国产化服务器，服务器的要求响应：单台配置 2.4GHZ/16C 32 线程，32G 内存，硬盘 A500G，硬盘 B 1T，网口 1000M；</p> <p>1、运维管理平台包括但不限于功能如下：提供资源管理、统一网络管理、服务器、数据库管理、虚拟化平台管理、存储管理、拓扑管理功能，告警管理、数据仓库、发现管理、策略管理、模型管理、采控管理、通知管理、权限认证管理报表管理等，提供三年维保服务。</p> <p>2、配置资源授权包含但不限于：资源授权（PC、云/虚拟化主机、存储、操作系统、中间件、数据库、web 服务、IPMI 服务器硬件的授权）50 个。网络设备授权 200 个。</p> <p>3、根据《广西电子政务外网技术规范（2022 年修订版）》中对广西电子政务外网运维管理系统要求，所提供运维管理系统需按照自治区相关文件以及《广西电子政务外网一体化运维</p>	1	项	314490	无

管理平台对接技术方案》要求进行无缝对接，确保数据传输安全、稳定。

#### 一、系统架构

1. 为保证系统平台的统一性，软件/模块使用同一品牌，所有软件/模块拥有完全自主知识产权，能独立研发、自主可控，全中文界面，提供友好、直观、易懂的图形呈现。

2. 部署安装符合国家安全可靠测评的操作系统产品及型号，确保系统安全性；具备主流浏览器及对应的版本，兼容国产核心浏览器产品、Firefox94 等

3. 部署的服务器芯片支持国产和非国产主流产品。

#### 二、健康检查

为了减轻系统运维人员的重复工作，系统应提供设备自动巡检功能。

1、巡检内容包括服务器、网络设备、应用、无线、虚拟化、存储、机房环境等所有管理对象。

2、巡检的计算方式应包括：符合条件的次数达到设定的阈值、连续的值符合设置的阈值、最后一次值符合设定的阈值、最后一次值与上一次值是否相同

3、巡检应支持自定义多个巡检任务面向不同的管理对象，设定巡检时间。巡检结束后应生成巡检报告

#### 三、IP 地址管理

为了支撑网络运维进行有序、合理的 IP 地址规划、IP 地址分配与回收，需支持以下需求：

1、具备通过自动发现的方式，自动汇聚网段，支撑 IP 地址的规划管理。

2、具备通过手动方式进行 IP 地址网段的录入，以实现规划管理。

3、IP 地址的属性需要支持自由扩展，以便于应对日后的业务变化。

#### 四、报表中心

为了满足常见的数据分析和汇报场景，应具备系统全数据统计分析能力，具体需求如下：

1、应能内置数据分析模板和组件，模板和组件的统计对象包括但不限于资源、告警、流量、链路等。具备基于模板或组件一键生成报表。

2、应能对系统可监控的资源、组件进行全类型、全属性、全指标的统计分析。

3、指标支持按平均值、最大值、最小值等不同

		<p>方式计算和统计。 </p> <p>4、能够在同一组件完成多个资源的指标趋势比对分析，也能够同一组件下分析同一资源的多个相关指标趋势。</p> <p>五、关键链路监控</p> <p>为了帮助运维人员快速排查关键链路故障，系统需具备以下能力：</p> <p>1、当关键链路中断时，系统能在 30 秒内产生告警</p> <p>2、当关键链路产生中断告警后，如果链路两端接口同样中断，可以将告警关联呈现</p> <p>3、支持在关键链路告警详情中对可能引起故障的指标进行关联分析，如端到端 ping 时延、端到端 ping 丢包率、端到端 ping 状态、端到端 ping 抖动、两端接口的丢包数、错包数等</p> <p>4、支持在关键链路告警详情中自定义关联分析的指标，如选择其他链路的指标进行趋势分析</p> <p>六、分级管理</p> <p>为了满足多级组织的管理需求，满足上级对下级的管理，提供以下能力：</p> <p>1、可以提供查看所有下级上报单位的重要设备告警信息。</p> <p>2、对于重点关注告警，可以提供列表进行单独呈现。</p>				
2	驻场服务	提供 1 名驻场人员，提供 3 年驻场服务，保障网络设备、安全设备、密码设备等正常运行。服务内容包括但不限于负责对电子政务外网、互联网等各类型网络的运维保障；负责网络设备、安全设备、密码设备等设备的运行安全监测等。	1	项	10000	无
(三)	安全服务	<b>采购安全服务，提供以下配置的设备，保障电子政务外网的稳定运行。</b>	/	/	/	无
1	态势感知分析平台（安全监测平台）	<p>服务提供 1 套态势感知分析平台（安全监测平台），提供三年服务。平台满足如下要求：</p> <p>硬件服务器以及操作系统，配置：国产化 CPU：2 颗（16 核心 32 线程，主频 2.5GHz）；内存：256G（总容量）DDR4；硬盘 1：2 块 960G SSD 固态硬盘组成 Raid 1；硬盘 2：12*4TB 企业级 SATA 3.5 寸硬盘，总容量 48T；服务器操作系统；</p> <p>1、系统软件基础功能，包含威胁检测、分析中心、响应中心、资产中心、统计报表、仪表盘、系统管理、态势感知（综合安全态势、安全运营态势、外部威胁态势、内网威胁态势、</p>	1	项	255240	无

威胁预警态势、攻击者态势、资产态势、资产风险态势、脆弱性态势)等功能,包含3年授权及软件基础维保服务。

★2、按照《广西电子政务外网安全监测技术及级联接口规范要求》要求,实现与自治区安全监测平台进行对接,提供政务监测数据对接的自治区安全监测平台定制功能,通过级联管理类接口、监测数据上报接口、信息共享与通报接口3类接口与下级平台实现级联互通,数据共享,同时对所有下级平台上报的数据进行管理。(提供详细技术对接方案)

3、提供3年件威胁情报失陷情报库更新服务,3年漏洞知识库更新服务。

3.具备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.具备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.威胁具备按照威胁事件视图、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. 在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。				
2	态势感知流量探针	<p>服务提供 4 台国产化态势感知流量探针，提供三年服务。态势感知流量探针满足如下配置要求：</p> <ol style="list-style-type: none"> <li>1. 标准 2U 机架式设备，配置 6 个千兆电口，2 个万兆光口，2 个接口扩展插槽，硬盘存储 4TB，2 个 USB3.0 接口，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；</li> <li>2. 系统应用层吞吐量 3Gbps，并发会话数 300 万/s，新建会话数 3 万/s；</li> <li>3. 能够支持对常见扫描以及远控木马的检测；</li> <li>4. 能够通过双向流量检测的方式发现可被利用的 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；</li> <li>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；</li> <li>★6. 具备对 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；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</li> <li>★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；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</li> <li>8. 具备对流量中出现文件传输行为进行发现和还原，将文件 MD5 发送至分析平台；</li> <li>9. 具备对 HTTP、SMTP、POP3、IMAP、FTP、MSSQL、MYSQL、ORACLE、POSTGRESQL、LDAP、DNS、SSL、TDS、TFTP 等协议的分析还原；</li> <li>10. 具备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；</li> <li>11. 具备对常见可执行文件的还原：EXE、DLL、OCX、SYS、COM、apk 等；</li> <li>12. 具备对常见压缩格式的还原：RAR、ZIP、GZ、7Z 等；</li> </ol>	1	项	305000	无

		13. 在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。				
3	抗拒绝服务系统	<p>服务提供 2 台抗拒绝服务系统，提供三年服务。抗拒绝服务系统满足如下配置要求： 国产化抗拒绝服务系统，流量清洗能力为 4Gbps，64 字节小包处理能力为 568 万，主机防护数量为 20 万，新建连接数为 39 万，并发连接数 1100 万，标准 2U 机箱，64G SSD 硬盘，单电源，2 个独立 MGT 管理口，配置 4 个 10/100/1000M 自适应电口、2 个万兆光口，8 个 SFP 插槽，1 个扩展卡插槽，1 个 console 口，2 个 USB 口，包含 3 年软件质保服务，3 年硬件质保服务。</p> <p>在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。</p>	1	项	126000	无
4	政务外网防火墙	<p>服务提供 2 台政务外网防火墙，提供三年服务。政务外网防火墙满足如下配置要求：</p> <p>★1. 标准 2U 设备，配置 1 个管理网口，1 个 HA 接口，4 个千兆电口、4 个万兆光口，另有 2 个扩展板卡插槽，冗余电源；采用国产化 CPU 和国产化操作系统；配置三年硬件维保及三年应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>★2. 网络层吞吐量：最大吞吐量 60Gbps，并发连接数 3000 万，每秒新建连接数 70 万/秒，配置 IPSec VPN 及 SSL VPN 60 个；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>3. 产品支持路由、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>4. 具备静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、OSPF、BGP 等；</p> <p>5. 具备防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗；</p> <p>6. 具备在 IPv6 环境下配置安全策略、SSL 解密策略等规则，实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮</p>	1	项	156000	无

	<p>件过滤、行为管控及带宽管理；</p> <p>7. 产品具备基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并具备警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）等多种防护措施；</p> <p>8. 具备上传、下载、双向的文件内容过滤；内容过滤支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等多种常见文件类型；</p> <p>9. 产品具备灵活的服务链编排功能，支持串联和旁路链，支持网元组的方向和位置设置；</p> <p>10. 具备冗余策略分析功能，系统可自动检测别列出与某一策略存在冗余关系的其他策略；</p> <p>11. 具备全面的 NAT 转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；</p> <p>12. 具备虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计；</p> <p>13. 具备与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；</p> <p>14. 在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。</p>				
5	<p>互联网出口防火墙</p> <p>服务提供 2 台互联网出口防火墙，提供三年服务。互联网出口防火墙满足如下配置要求：</p> <p>★1. 标准 2U 设备，配置 1 个管理网口，1 个 HA 接口，4 个千兆电口、4 个万兆光口，另有 2 个扩展板卡插槽，冗余电源；采用国产化 CPU 和国产化操作系统；配置三年硬件维保及三年应用识别库、URL 分类特征库、病毒防护特征库、入侵防御特征库升级服务及威胁情报订阅服务；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>★2. 网络层吞吐量：最大吞吐量 60Gbps，并发连接数 3000 万，每秒新建连接数 70 万/秒，配置 IPSec VPN 及 SSL VPN60 个；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p>	1	项	156000	无

		<p>3. 产品支持路由、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>4. 具备静态路由、动态路由、策略路由，动态路由包括 RIP v1/v2/ng、OSPF、BGP 等；</p> <p>5. 具备防御 IP 地址欺骗，可将 IP 与安全域关联，即指定 IP 或网段从特定安全域流量流入，否则视为 IP 地址欺骗；</p> <p>6. 具备在 IPv6 环境下配置安全策略、SSL 解密策略等规则，实现漏洞防护、间谍软件防护、URL 过滤、反病毒、内容过滤、文件过滤、邮件过滤、行为管控及带宽管理；</p> <p>7. 产品支持基于不同安全区域防御 SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood 攻击，并具备警告、丢弃、普通防护（首包丢弃）、增强防护（TC 反弹技术）等多种防护措施；</p> <p>8. 具备上传、下载、双向的文件内容过滤；内容过滤支持 html、doc、docx、xls、xlsx、ppt、pptx、chm、7z 等多种常见文件类型；</p> <p>9. 产品具备灵活的服务链编排功能，支持串联和旁路链，支持网元链的方向和位置设置；</p> <p>10. 具备冗余策略分析功能，系统可自动检测并列出与某一策略存在冗余关系的其他策略；</p> <p>11. 具备全面的 NAT 转换能力，支持对源目的地址、端口的转换；包括一对一，一对多，多对一，多对多地址转换方式；</p> <p>12. 具备虚拟防火墙功能，支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL 过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计；</p> <p>13. 具备与云端联动，实现病毒云查杀、URL 云识别、应用云识别、云沙箱等功能，以通过安全云系统提升识别库数量级，补充本地识别库；</p> <p>14. 在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。</p>				
6	互联网出口上网行为管理	<p>服务提供 2 台互联网出口上网行为管理，提供三年服务。互联网出口上网行为管理满足如下配置要求：</p> <p>1. 2U 硬件设备，标配 6 个千兆电接口（其中含 1 个管理接口和 1 个 HA 接口），4 个千兆光接</p>	1	项	155200	无

口，4个万兆光接口，提供1个扩展插槽，2T机械硬盘，冗余交流电源，配置国产化CPU，国产化操作系统；提供三年硬件质保及三年URL库、应用协议库软件升级服务；

2. 适合2G带宽/25000人以下网络环境使用；最大并发连接数为300万，最大新建连接数为90000/秒；

3. 应用协议库包含的应用数量7100种，应用规则总数30000种，URL数据1.5亿条，移动应用1000种；

4. 可识别用户上网设备类型并作为策略条件，可将IP、IP段、VLAN作为策略条件；

★5. 具备基于用户、时间、应用、源IP、目的IP和服务创建流量控制策略；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）

6. 可以基于IP、MAC、终端类型等多因素进行用户认证、识别；

7. 可以为用户添加多属性，并根据用户的属性（如职位、部门、电话、邮件等）自动进行用户分类，根据分类的结果做审计、控制策略；

8. 具备对QQ账号制定策略，对聊天、登录及文件传输的行为进行记录与控制；

9. 提供对微信PC版进行行为和内容的审计，记录发送/接受信息的微信账号；

10. 当用户的网页访问被网页浏览策略封堵时，用户如果发现分类错误能够在页面中向管理员进行反馈；不同网页被阻塞后会跳转不同的阻塞页面，支持用户完全自定义；

11. 支持与终端杀毒软件联动，为终端杀毒软件配置推送部署策略，并能够通过终端杀毒软件获取到PC系统信息、漏洞情况，并具备对这些信息进行准入策略设置；

12. 具备利用微信公众号进行网络接入的身份准入认证；

13. Webmail基于发件人、收件人、主题、内容、附件名、附件大小维度进行记录、告警；支持根据邮件主题、正文关键字进行阻塞并进行告警；

★14. 可审计Oracle, MySql, SqlServer, PostgreSQL等数据库的访问与操作，包括添加、删除、修改、查询等；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）

		15. 在 5 部委（安全认证和安全检测结果）目录内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。				
7	日志收集与分析系统	<p>日志收集与分析系统：服务提供 1 台日志收集与分析系统，提供三年服务。日志收集与分析系统满足如下配置要求：</p> <p>1、硬件规格：国产 CPU，国产操作系统，标准 2U 机箱，提供 6 * 千兆自适应电口，4 * 千兆光口，2 个扩展插槽，1 个 Console 接口。包含 300 个日志源授权，内置 256GB mSATA 卡，提供可插拔 4TB SATA 硬盘存储海量日志。3 年硬件维保服务和 3 年软件升级维护服务。</p> <p>2、性能：综合日志处理性能 3000EPS，日志采集处理均值 6000EPS；</p> <p>3、配置国密卡，支持 SM1、SM2、SM3、SM4 等国密算法；</p> <p>★4、具备对各类网络设备、安全设备、工作站、存储设备、机房设备、其他设备、中间件、数据库、防病毒系统、服务器系统的日志、事件、告警等安全信息进行全面的审计；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>★5. 具备通过 Syslog、SNMP Trap、NetFlow V5、JDBC、WMI、文件\文件夹读取、Kafka 等多种方式完成各种日志的收集功能；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>6. 具备对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警；</p> <p>7. 具备对资产 IP 地址（含内网 IP）的地理信息进行管理，设置单 IP 及 IP 段行政区及经纬度，支持地图显示；</p> <p>8. 具备对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证；</p> <p>9. 具备日志范化策略，针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配；</p> <p>10. 具备对日志中的源和目的 IP 地址进行自动补全，补全 IP 地址的资产、国家、区域和城市等信息；</p> <p>11. 在 5 部委（安全认证和安全检测结果）目录</p>	1	项	78780	无

		内以及《网络安全专用产品安全检测证书》，或《网络关键设备和网络安全专用产品安全认证证书》在有效期内。				
8	国密综合安全网关	<p>服务提供 1 台综合安全网关，提供三年服务。</p> <p>网关满足如下配置要求：</p> <p>机箱规格：标准 2U 机架式；网络接口：默认 6 个千兆电口，3 个前置扩展插槽；（每个扩展槽可扩展 2/4 个千兆电口，2/4 个千兆光口，2/4 个万兆光口）其他接口：2 个 USB 接口；电源：220V，550W 冗余电源，支持热插；</p> <p>SSL 最大并发数：10,000；SSL 每秒新建数：2,000；SSL 吞吐率：600Mbps。IPSec 隧道数：5,000；IPSec 每秒新建隧道：2,000；IPSec 吞吐率：1Gbps；明文最大并发连接数：50 万；明文每秒新建连接数：50,000。</p> <p>功能指标：</p> <p>1、具备 IPSec VPN 功能，支持国际 RSA 和国密 SM2 算法的隧道建立；</p> <p>2、具备 NAT 穿透功能；支持 IKEv1.0、IKEv1.1、IKEv2.0 标准协议；</p> <p>3、具备 SSL VPN 功能，支持 TUN 模式和 TAP 模式；</p> <p>4、具备配置服务端路由表，以同步到客户端设备，支持配置 lzo 压缩模式；</p> <p>5、具备单向及双向 SSL 卸载功能，且单个 SSL 服务可同时兼容国际算法及国密算法套件，并可通过管理界面进行切换或自适应切换；</p> <p>6、采用多芯片嵌入式密码模块装置，内置 16 个国密局认证安全芯片，芯片采用集群调度，单个芯片故障不影响整机运行；</p> <p>7、提供设备可视化监控功能，包括密钥数据、CPU/内存/硬盘占用率、服务状态、设备密码运算状态等资源的实时监控；</p> <p>8、提供设备自检功能，包括随机数、算法正确性、密钥数据完整性、软固件完整性自检成功、设备产品自检，并支持设置设备定时自检；</p> <p>9、具备 IPv6 网络协议；</p> <p>10、提供 SSL 卸载网关 SDK 支持客户端 SDK，集成到客户的 C/S 和 B/S 架构应用代码，实现发起国密 SSL 请求；</p> <p>11、具备并提供商用密码检测认证中心颁发的《商用密码产品认证证书》。</p>	1	项	63000	无

(四)	密码服务	采购密码服务，提供的设备能为电子政务外网的网络层面提供基础密码保障。	/	/	/	无
1	加解密服务（服务器密码机）	<p>服务提供 1 台密码机，提供三年服务。密码机满足如下配置要求：</p> <p>1) 具备 SM1/2/3/4 等国密算法；</p> <p>2) 提供非对称密钥的签名/验签、数字信封/解信封、摘要功能，提供对称算法的 ECB/CBC/CFB/OFB 模式的加解密功能，提供 CMAC 和 HMAC 功能；</p> <p>3) 提供多种调用接口，支持 GM/T0018、GM/T0019、JCE、PKCS11 接口，支持 http 服务接口调用；</p> <p>4) 具备非对称密钥和对称密钥的安全生成、存储、销毁；</p> <p>5) 管理员、审计员等数字证书支持多 CA 信任链和多级 CA 信任链管理；</p> <p>6) 具备 javaKeystore 的创建配置、证书请求、证书导入/导出、信任证书导入，keystore 容器类型支持 TrustedCertEntry 和 PrivateKeyEntry；</p> <p>7) 设备具备密钥数据备份恢复功能，恢复时采用权限严格控制操作权限；</p> <p>8) 设备采用管理密钥-用户密钥-会话密钥的三层密钥保护结构，实现密钥安全防护；</p> <p>9) 可生成真随机数，随机数质量符合国家密码标准要求；</p> <p>★10) 集群管理：支持 HA 高可用集群配置，支持节点的单机与 HA 模式切换、主从切换；支持在集群主节点和从节点查看集群列表信息（集群名、节点 ip、节点模式、状态信息、数据迭代版本、创建时间、更新时间等）；（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>11) 具备并提供商用密码检测认证中心颁发的《商用密码产品认证证书》</p> <p>12) 产品适配国产 CPU、国产服务器操作系统、国产数据库、国产应用服务器软件。</p> <p>★13) Keystore 管理：设备支持 keystore 的配置管理功能（提供设备厂家产品说明书等证明材料或国家认可的第三方测评报告）</p> <p>14) 设备具备通过 SNMP 协议监控设备状态，支持 syslog 配置</p> <p>★15) 设备具备密钥备份恢复功能（提供设备厂家产品说明书等证明材料或国家认可的第三</p>	1	项	60000	无

		方测评报告) 性能指标: 1) SM2: 密钥生成: 120000 对/秒、签名/验 签: 120000/65000 次/秒、加密/解密: 35000/50000 次/秒 2) SM4: 870Mbps、SM3: 860Mbps、SM1870Mbps				
2	国密浏览器	服务提供 150 套国密浏览器, 提供三年服务。 国密浏览器满足如下配置要求: 1) 产品具有《商用密码产品认证证书》; 2) 浏览器使用 SM2/SM3/SM4 国密算法; 3) 可实现 SSL 单双向安全协议, 与 Web 服务器 之间建立安全通道, 保证 Web 网页访问的安全 性; 4) 具备第三方电子认证中心签发的数字证书;	1	项	24000	无
3	USBKey	服务提供 150 套 USBKey, 提供三年服务。 USBKey 满足如下配置要求: 1、全面支持 PKI 应用, 支持 SM1/SM2/SM3/SM4 系列算法 2、提供标准安全中间件接口 CSP 及国密接口; 3、适配 X.509 v3 标准证书格式, 并实现多个 密钥的存储; 4、适用于 Windows、Linux、Mac OS 以及国产 化操作系统平台; 5、支持 USB2.0、3.0、Android OTG 接口; 6、具备并提供国家密码管理局颁发的《商用密 码产品认证证书》	1	项	9000	无
4	个人证书	服务提供 150 套个人证书, 提供三年服务。个 人证书满足如下配置要求: 1、通过数字证书确认网络中传递信息的个人身 份, 确保个人线上身份同线下身份一致; 2、利用数字证书进行数字签名, 其作用与手写 的签名具有同等法律效力; 3、数字证书可以帮助发送方使用接收方的公钥 对数据加密, 而接收方则使用自己的私钥解 密, 实现信息安全传输。	1	项	67500	无
5	设备证书	服务提供 1 套设备证书, 提供三年服务。设备 证书满足如下配置要求: 第三方 CA 机构签发的设备数字证书, 使用国产 密码算法, 数字证书符合 X.509 V3 格式。CA 机构具备电子认证服务资质和电子政务电子认 证服务资质证明。	1	项	30000	无
6	商用密码应用 评估	根据桂财建〔2023〕102 号, 提供第三级信息 系统密评报告需每年测评, 本次需提供 3 年服 务。	1	项	145000	无

(五)	线路 机柜 租用 服务		/	/	/	无
1	电子政务外网专线接入服务	<p>1. 350个委办局节点网络服务；</p> <p>2. 优化电子政务外网接入，根据实际接入单位终端的使用数量合理分配带宽，保证后期满足350家单位接入。1-50台的带宽100M，51-100台的带宽200M，100台以上的带宽1000M；</p> <p>3. 接入线路采用符合《广西电子政务外网市县节点技术规范》的线路技术；</p> <p>4. 提供3年租用服务。</p>	1	项	129600	注：需接入350个单位，先行接入275个，后续根据需求增加。
2	互联网出口专线 (主)	<p>1. 3000Mbps带宽，3000M裸机互联网带宽裸机测试，上下行速率稳定在3000Mbit/s</p> <p>2. 公网ip地址56个</p> <p>3. 3年租用服务</p>	1	条	320000	无
3	机柜租用	<p>1. 提供电子政务外网合规机房，物理安全满足网络安全等级保护第三级要求和密码应用三级要求，托管设备机房有独立区域、独立门禁，监控保留6个月；</p> <p>2. 提供4个42U机柜，免费提供单个机柜满配时4千瓦·时的电力供应，以满足安装于租用机柜内的电子政务外网设备（含标段2的准入系统的设备）的动力需求；</p> <p>3. 包含机房日常巡检、空调、UPS等基础物理设施；</p> <p>4. 提供3年机柜租用服务。</p>	1	项	158400	无
4	驻场服务	服务提供1名驻场人员，提供3年驻场服务，保障机房的正常运行，服务但不限于对精密空调系统、UPS系统、新风系统、供配电系统、动环监控系统等进行日常巡检、故障检测等	1	项	3388	无
投标报价合计（小写）			¥4203888.00元			
投标报价合计（大写）			人民币肆佰贰拾万叁仟捌佰捌拾捌元整			

注：

1、投标人需按本表格式填写，否则视为投标文件含有采购人不能接受的附

加条件，投标无效。

2、有关本项目实施所涉及的一切费用均计入报价。采购人将以合同形式有偿取得货物或服务，不接受投标人给予的赠品、回扣或者与采购无关的其他商品、服务，不得出现“0元”“免费赠送”等形式的无偿报价，否则视为投标文件含有采购人不能接受的附加条件，投标无效；采购内容未包含在《开标一览表（报价表）》名称栏中，投标人不能作出合理解释的，视为投标文件含有采购人不能接受的附加条件的，投标无效。

3、特别提示：采购代理机构将对项目名称和项目编号，中标供应商名称、地址和中标金额，主要中标标的名称、服务范围、服务要求、服务时间、服务标准等予以公示。

4、符合招标文件中列明的可享受中小企业扶持政策的投标人，请填写中小企业声明函。注：投标人提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

5、符合招标文件中列明的可享受本国产品标准及相关政策的投标人，请填写《关于符合本国产品标准的声明函》或出具财政部会同有关部门规定的有关证明文件。当采购项目或者采购包中含有多种产品，投标人还应当声明其为该采购项目或者采购包提供的符合本国产品标准的产品成本之和占该供应商提供的全部产品成本之和的比例达到80%以上，提供《关于符合本国产品标准的产品成本之和占所提供的全部产品成本之和的比例达到80%以上的声明函》。注：投标人提供的《声明函》内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

6、投标报价属于本招标文件规定的政府采购异常低价情形之一，投标人应当按照评标委员会的要求提供书面说明、证明材料。投标人不能提供书面说明、证明材料，或者提供的书面说明、证明材料不能证明其报价合理性的，投标无效。

投标人名称（公章）：中国电信股份有限公司广西分公司

法定代表人（负责人）或委托代理人（签名）：黄成国

日期：2026年7月8日

## 2 中小企业声明函

无，我公司不是中小企业。

投标人名称（公章）：中国电信股份有限公司广西分公司



日期：2026年7月8日

### 3 关于符合本国产品标准的声明函

#### 关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

1. （核心路由器 NetEngine 8000E M14），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（核心路由器 NetEngine 8000E M14）的中国境内生产的组件成本占比≥（规定比例）。（核心路由器 NetEngine 8000E M14）的（关键组件）在中国境内生产。（核心路由器 NetEngine 8000E M14）的（关键工序）在中国境内完成。

2. （汇聚路由器 NetEngine 8000E M6），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（汇聚路由器 NetEngine 8000E M6）的中国境内生产的组件成本占比≥（规定比例）。（汇聚路由器 NetEngine 8000E M6）的（关键组件）在中国境内生产。（汇聚路由器 NetEngine 8000E M6）的（关键工序）在中国境内完成。

3. （接入路由器 NetEngine AR5710-S28T2S2XE4），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（接入路由器 NetEngine AR5710-S28T2S2XE4）的中国境内生产的组件成本占比≥（规定比例）。（接入路由器 NetEngine AR5710-S28T2S2XE4）的（关键组件）在中国境内生产。（接入路由器 NetEngine AR5710-S28T2S2XE4）的（关键工序）在中国境内完成。

4. （管理交换机 S5736-S24S4XC），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（管理交换机 S5736-S24S4XC）的中国境内生产的组件成本占比≥（规定比例）。（管理交换机 S5736-S24S4XC）的（关键组件）在中国境内生产。（管理交换机 S5736-S24S4XC）的（关键工序）在中国境内完成。

5. （态势感知分析平台（安全监测平台）奇安信网神安全分析与管理系  
统 V4.0），生产厂为（奇安信网神信息技术（北京）股份有限公司），厂址为  
（北京市西城区西直门外南路 26 号院 1 号楼 2 层）。（态势感知分析平台（安

全监测平台奇安信网神安全分析与管理系统 V4.0) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(态势感知分析平台(安全监测平台)奇安信网神安全分析与管理系统 V4.0)的(关键组件)在中国境内生产。(态势感知分析平台(安全监测平台)奇安信网神安全分析与管理系统 V4.0)的(关键工序)在中国境内完成。

6. (态势感知流量探针 TSS10000/V4.0)，生产厂为(奇安信网神信息技术(北京)股份有限公司)，厂址为(北京市西城区西直门外南路 26 号院 1 号楼 2 层)。(态势感知流量探针 TSS10000/V4.0)的中国境内生产的组件成本占比 $\geq$  (规定比例)。(态势感知流量探针 TSS10000/V4.0)的(关键组件)在中国境内生产。(态势感知流量探针 TSS10000/V4.0)的(关键工序)在中国境内完成。

7. (抗拒绝服务系统 HiSeeEngine AntiDDoS1000)，生产厂为(华为技术有限公司)，厂址为(深圳市龙岗区坂田华为总部办公楼)。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000)的中国境内生产的组件成本占比 $\geq$  (规定比例)。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000)的(关键组件)在中国境内生产。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000)的(关键工序)在中国境内完成。

8. (政务外网防火墙 DAS-TGFW-A1600-HU)，生产厂为(杭州安恒信息技术股份有限公司)，厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(政务外网防火墙 DAS-TGFW-A1600-HU)的中国境内生产的组件成本占比 $\geq$  (规定比例)。(政务外网防火墙 DAS-TGFW-A1600-HU)的(关键组件)在中国境内生产。(政务外网防火墙 DAS-TGFW-A1600-HU)的(关键工序)在中国境内完成。

9. (互联网出口防火墙 DAS-TGFW-A1600-HU)，生产厂为(杭州安恒信息技术股份有限公司)，厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(互联网出口防火墙 DAS-TGFW-A1600-HU)的中国境内生产的组件成本占比 $\geq$  (规定比例)。(互联网出口防火墙 DAS-TGFW-A1600-HU)的(关键组件)在中国境内生产。(互联网出口防火墙 DAS-TGFW-A1600-HU)的(关键工序)在中国境内完成。

10. (互联网出口上网行为管理 DAS-AC-A1500-HU), 生产厂为(杭州安恒信息技术股份有限公司), 厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(互联网出口上网行为管理 DAS-AC-A1500-HU)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(互联网出口上网行为管理 DAS-AC-A1500-HU)的(关键组件)在中国境内生产。(互联网出口上网行为管理 DAS-AC-A1500-HU)的(关键工序)在中国境内完成。

11. (日志收集与分析系统 DAS-LOG-A1200-FU), 生产厂为(杭州安恒信息技术股份有限公司), 厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(日志收集与分析系统 DAS-LOG-A1200-FU)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(日志收集与分析系统 DAS-LOG-A1200-FU)的(关键组件)在中国境内生产。(日志收集与分析系统 DAS-LOG-A1200-FU)的(关键工序)在中国境内完成。

12. (国密综合安全网关(型号: CWCAPN-3000-G V1.0)), 生产厂为(西部安全认证中心有限责任公司)2, 厂址为(银川市金凤区新昌西路 65 号易大紫荆花商务中心 A 座 7 层)。(国密综合安全网关)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(国密综合安全网关)的(关键组件)在中国境内生产。(国密综合安全网关)的(关键工序)在中国境内完成。

13. (服务器密码机(型号: AJSM2570 V1.0)), 生产厂为(航天信息股份有限公司), 厂址为(北京市海淀区杏石口路甲 18 号)。(服务器密码机)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(服务器密码机)的(关键组件)在中国境内生产。(服务器密码机)的(关键工序)在中国境内完成。

14. (国密浏览器(型号: HT-RLCM V5.0)), 生产厂为(北京海泰方圆科技股份有限公司), 厂址为(北京市海淀区上地九街 9 号 9 号 6 层 611 号)。(国密浏览器)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(国密浏览器)的(关键组件)在中国境内生产。(国密浏览器)的(关键工序)在中国境内完成。

15. (USBkey(型号: GM3000 2.23)), 生产厂为(北京世纪龙脉科技有限公司)2, 厂址为(北京市海淀区五道口东王庄甲 1 号 3 幢 303 号)。(USBkey)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(USBkey)的(关键组件)

在中国境内生产。(USBkey)的(关键工序)在中国境内完成。

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：中国电信股份有限公司广西分公司

日期：2026年7月8日



注：

1. 产品如有型号，请在“产品名称”栏一并填写。
2. 生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。
3. 该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填，下同。
4. 该产品的关键组件要求实施前，“关键组件”栏可不填，下同。
5. 该产品的关键工序要求实施前，“关键工序”栏可不填，下同。

## 4 关于符合本国产品标准的产品成本之和占所提供的全部产品成本之和的比例达到 80%以上的声明函

### 关于符合本国产品标准的产品成本之和占所提供的全部产品成本之和的比例达到 80%以上的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34 号）的规定，本公司（单位）本次投标所提供的符合本国产品标准的产品成本之和占我公司（单位）本次投标所提供的全部产品（全部产品是指货物或服务采购项目或采购包中包含的全部货物、服务产品）成本之和的比例达到 80%以上。

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：中国通信股份有限公司广西分公司

日期：2026 年 7 月 8 日

注：

1. 本声明函须同时提供关于符合本国产品标准的声明函或财政部会同有关部门规定的有关证明文件，否则不享受价格扣除政策。
2. 当采购项目或者采购包中含有多种产品，投标人拟享受该政策时提供。当采购项目或者采购包中仅含有单一产品时，无须提供本声明函。

## 4.1 关于符合本国产品标准的声明函

### 关于符合本国产品标准的声明函

本公司（单位）郑重声明，根据《国务院办公厅关于在政府采购中实施本国产品标准及相关政策的通知》（国办发〔2025〕34号）的规定，本公司（单位）提供的以下产品属于本国产品。具体情况如下：

3. （核心路由器 NetEngine 8000E M14），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（核心路由器 NetEngine 8000E M14）的中国境内生产的组件成本占比≥（规定比例）。（核心路由器 NetEngine 8000E M14）的（关键组件）在中国境内生产。（核心路由器 NetEngine 8000E M14）的（关键工序）在中国境内完成。

4. （汇聚路由器 NetEngine 8000E M6），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（汇聚路由器 NetEngine 8000E M6）的中国境内生产的组件成本占比≥（规定比例）。（汇聚路由器 NetEngine 8000E M6）的（关键组件）在中国境内生产。（汇聚路由器 NetEngine 8000E M6）的（关键工序）在中国境内完成。

3. （接入路由器 NetEngine AR5710-S28T2S2XE4），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（接入路由器 NetEngine AR5710-S28T2S2XE4）的中国境内生产的组件成本占比≥（规定比例）。（接入路由器 NetEngine AR5710-S28T2S2XE4）的（关键组件）在中国境内生产。（接入路由器 NetEngine AR5710-S28T2S2XE4）的（关键工序）在中国境内完成。

4. （管理交换机 S5736-S24S4XC），生产厂为（华为技术有限公司），厂址为（深圳市龙岗区坂田华为总部办公楼）。（管理交换机 S5736-S24S4XC）的中国境内生产的组件成本占比≥（规定比例）。（管理交换机 S5736-S24S4XC）的（关键组件）在中国境内生产。（管理交换机 S5736-S24S4XC）的（关键工序）在中国境内完成。

5. （态势感知分析平台（安全监测平台）奇安信网神安全分析与管理系  
统 V4.0），生产厂为（奇安信网神信息技术（北京）股份有限公司），厂址为  
（北京市西城区西直门外南路 26 号院 1 号楼 2 层）。（态势感知分析平台（安

全监测平台奇安信网神安全分析与管理系统 V4.0) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(态势感知分析平台(安全监测平台)奇安信网神安全分析与管理系统 V4.0)的(关键组件)在中国境内生产。(态势感知分析平台(安全监测平台)奇安信网神安全分析与管理系统 V4.0)的(关键工序)在中国境内完成。

6. (态势感知流量探针 TSS10000/V4.0)，生产厂为(奇安信网神信息技术(北京)股份有限公司)，厂址为(北京市西城区西直门外南路 26 号院 1 号楼 2 层)。(态势感知流量探针 TSS10000/V4.0) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(态势感知流量探针 TSS10000/V4.0) 的(关键组件)在中国境内生产。(态势感知流量探针 TSS10000/V4.0) 的(关键工序)在中国境内完成。

7. (抗拒绝服务系统 HiSeeEngine AntiDDoS1000)，生产厂为(华为技术有限公司)，厂址为(深圳市龙岗区坂田华为总部办公楼)。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000) 的(关键组件)在中国境内生产。(抗拒绝服务系统 HiSeeEngine AntiDDoS1000) 的(关键工序)在中国境内完成。

8. (政务外网防火墙 DAS-TGFW-A1600-HU)，生产厂为(杭州安恒信息技术股份有限公司)，厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(政务外网防火墙 DAS-TGFW-A1600-HU) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(政务外网防火墙 DAS-TGFW-A1600-HU) 的(关键组件)在中国境内生产。(政务外网防火墙 DAS-TGFW-A1600-HU) 的(关键工序)在中国境内完成。

9. (互联网出口防火墙 DAS-TGFW-A1600-HU)，生产厂为(杭州安恒信息技术股份有限公司)，厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(互联网出口防火墙 DAS-TGFW-A1600-HU) 的中国境内生产的组件成本占比 $\geq$  (规定比例)。(互联网出口防火墙 DAS-TGFW-A1600-HU) 的(关键组件)在中国境内生产。(互联网出口防火墙 DAS-TGFW-A1600-HU) 的(关键工序)在中国境内完成。

10. (互联网出口上网行为管理 DAS-AC-A1500-HU), 生产厂为(杭州安恒信息技术股份有限公司), 厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(互联网出口上网行为管理 DAS-AC-A1500-HU)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(互联网出口上网行为管理 DAS-AC-A1500-HU)的(关键组件)在中国境内生产。(互联网出口上网行为管理 DAS-AC-A1500-HU)的(关键工序)在中国境内完成。

11. (日志收集与分析系统 DAS-LOG-A1200-FU), 生产厂为(杭州安恒信息技术股份有限公司), 厂址为(浙江省杭州市滨江区西兴街道联慧街 188 号)。(日志收集与分析系统 DAS-LOG-A1200-FU)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(日志收集与分析系统 DAS-LOG-A1200-FU)的(关键组件)在中国境内生产。(日志收集与分析系统 DAS-LOG-A1200-FU)的(关键工序)在中国境内完成。

12. (国密综合安全网关(型号: CWCAPN-3000-G V1.0)), 生产厂为(西部安全认证中心有限责任公司)2, 厂址为(银川市金凤区新昌西路 65 号易大紫荆花商务中心 A 座 7 层)。(国密综合安全网关)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(国密综合安全网关)的(关键组件)在中国境内生产。(国密综合安全网关)的(关键工序)在中国境内完成。

13. (服务器密码机(型号: AJSM2570 V1.0)), 生产厂为(航天信息股份有限公司), 厂址为(北京市海淀区杏石口路甲 18 号)。(服务器密码机)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(服务器密码机)的(关键组件)在中国境内生产。(服务器密码机)的(关键工序)在中国境内完成。

14. (国密浏览器(型号: HT-RLCM V5.0)), 生产厂为(北京海泰方圆科技股份有限公司), 厂址为(北京市海淀区上地九街 9 号 9 号 6 层 611 号)。(国密浏览器)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(国密浏览器)的(关键组件)在中国境内生产。(国密浏览器)的(关键工序)在中国境内完成。

15. (USBkey(型号: GM3000 2.23)), 生产厂为(北京世纪龙脉科技有限公司)2, 厂址为(北京市海淀区五道口东王庄甲 1 号 3 幢 303 号)。(USBkey)的中国境内生产的组件成本占比 $\geq$ (规定比例)。(USBkey)的(关键组件)

在中国境内生产。(USBkey)的(关键工序)在中国境内完成。

本公司（单位）对上述声明内容的真实性负责。如有虚假，愿承担相应法律责任。

公司（单位）名称（盖章）：中国电信股份有限公司广西分公司

日期：2026年7月8日

注：

1. 产品如有型号，请在“产品名称”栏一并填写。
2. 生产厂名与厂址应与生产厂营业执照载明的相关信息保持一致。
3. 该产品的中国境内生产的组件成本占比相关要求实施前，“规定比例”栏可不填，下同。
4. 该产品的关键组件要求实施前，“关键组件”栏可不填，下同。
5. 该产品的关键工序要求实施前，“关键工序”栏可不填，下同。