桂平市山洪灾害非工程措施维修养护服务（重）（GGZC2020-J3-50104-GXDZ（重））

谈 判 记 录

广西广播电视信息网络股份有限公司：

请承诺贵单位不低于原竞标文件的谈判项目内容、数量、服务质量及售后服务等内容，提供二次报价（即最终报价（备注：如谈判过程对项目采购需求中的技术、服务要求以及合同草案条款内容有实质性变动需要进行多次报价的，需告知供应商本次报价为最终报价）。

谈判记录应答文件请以书面密封形式于2020年7月21日16时5分前交回。

谈判小组成员签字：

2020年7月21日

应 答 文 件

承诺：我单位不低于原竞标文件的谈判项目的内容、数量、服务质量及售后服务等内容，提供二次报价（即最终报价）

最终竞标总报价（元）（大写）：陆拾贰万捌仟元

（大写参照：壹、贰、叁、肆、伍、陆、柒、捌、玖、拾、零）

谈判供应商：广西广播电视信息网络股份有限公司

谈判供应商代表签字：

日　期：2020年7月21日

第3章 工作方案

根据《桂平市山洪灾害非工程措施维修养护服务（重）》（项目编号：GGZC2020-J3-50104-GXDZ（重））竞争性谈判文件中《服务需求一览表》的要求，我公司承诺：

一、设备运维服务提供以下服务：

主要内容包括：基础服务、网络设备续保、视频会议设备续保、视频会议保障服务、其他维护服务等，包含视频系统日常维护、故障处理、一年不少于2次的定期现场巡检，及时对原厂设备固件、系统软件进行更新升级。遇到重要视频会议时，派出技术人员到会场提供技术保障。

（一）设备基础续保及维护保障：1、负责《广西山洪灾害防治项目县级监测预警平台延伸到乡镇（网络改造和视频会商）》项目采购的视频会商设备的续保。包含县、乡镇视频会议设备的1年质保和送修、维修、更换服务，项目节点的故障响应、排查、处理支持以及返修设备的调试工作。2、负责《广西山洪灾害防治项目县级监测预警平台延伸到乡镇（网络改造和视频会商）》项目采购的网络设备的续保。包含县、乡镇网络设备的1年质保和送修、维修、更换服务，项目节点的故障响应、排查、处理支持以及返修设备的调试工作。3、负责《广西山洪灾害防治项目县级监测预警平台延伸到乡镇（网络改造和视频会商）》项目采购的摄像头的续保。包含县、乡镇摄像头的1年质保和送修、维修、更换服务，项目节点的故障响应、排查、处理支持以及返修设备的上架安装、调试。

（二）视频会议保障服务：会前，按照对视频会议系统进行联调测试，保证会议前系统的稳定正常；会中，增派技术人员协助派驻工程师保证会议顺利召开；会后，对视频会议系统进行调试、检查，及时解决问题，排除故障。

（三）重大事项现场保障服务

对于水利厅突发性、特殊性、紧急性的重大事件，提供高强度全方位的现场保障服务（每季度不超过4次），增派技术骨干精英，配合派驻人员， 提供全力保障服务。

（四）增值服务

提供配套专网线路监测防护和网络均衡系统增值服务。

专网线路监测服务			单位	数量
1	网络流量监控受控端高级接入授权软（县级）	下属网络流量监控与防护网关（县）设备接入平台的授权，可以管控的统一升级配置和系统状态检测	台	1

2	网络流量监控与防护网关路由（县级）	实现县份线路的网络流量控制、监控与检测，并提供基本的转网线路防护服务，解决专线故障定位慢、缺少负荷信息及流量分析的问题； 性能要求：防火墙性能 200Mbps，流控性能 160Mbps，防火墙吞吐量（双向）200Mbps； 要求设备集成流控、防火墙、VPN； 设备必须支持单臂模式，以在不影响原有网络情况下同时能降低网络单点故障的发生概率。并在此模式下仍能实现多线路功能； 支持根据不同业务特性要求和链路实时质量状态，将业务智能调度到最合适的链路；优先保障核心业务的链路质量；	台	1
3	一体化安全网关路由器系统软件	支持基于 QOE 参数（时延、丢包、抖动）实时检测每条广域网链路的质量； 支持多连接平均负载到多条链路实现带宽叠加的效果，提高链路利用率； 当链路故障时，支持 1s 内自动切换到备用链路中的最优链路，保障业务不中断，用户无感知； 支持易部署，通过专业的集中管理平台下发邮件方式，实现分支管理人员点击邮件链接即可实现分支自动完成基础网络配置，自动连接到流量和网络监控中心，简化分支配置，实现分支快速上线。（提供设备界面截图证明，加盖厂商公章） 支持 Auto VPN，集中管理平台自动将 VPN 配置信息下发给指定的分支端设备，实现分支自动接入 VPN 总部设备（提供设备界面截图证明，加盖厂商公章）	套	1

4	内置库	详细的日志报表，包括网点流量统计、网点版本明细、用户、管理员登录统计、告警日志、错误日志、系统调试日志。支持 SNMP 协议，支持 Syslog 导出、实现上网行为记录的转储功能； 支持查看即时显示设备状态，包括 CPU、内存、磁盘占用，以及内外网接口流量；支持查看设备异常信息；查看设备版本信息，细显示设备的版本信息及同步情况 能够提供图形化的实时监控状态，并且能够清楚的区分网络设备的运行状态； 既可整体监控又可局部监控；查看整网 VPN 拓补，详细显示 VPN 网络设备的连接状态；可保存和打印监控拓扑图；在监视界面可以远程重启设备； 通过控制台界面可实时查看登录用户的用户名、IP、权限、最后操作时间，并支持冻结非法用户 可根据用户的网络应用行为、访问的网站类型、不同用户/用户组、区别的时间段进行流量管理策略 通过控制台界面可实时查看登录用户的用户名、IP、权限、最后操作时间，并支持冻结非法用户； 支持与传统的 IPSec VPN 设备进行对接（如 Cisco、华为等设备） 具有 20 多个大类、超过 850 条应用识别规则，并支持应用协议识别库实时更新	套	27
	网络均衡服务			
1	网络优化中心控制网关硬件平台（县级）	多核 AMP+架构，网络层吞吐量 8G，并发连接≥180 万，每秒新建连接数 6 万，标准 1U 机箱，单电源，标准配置 6 个 10/100/1000M 自适应电口，另有 1 个接口板卡扩展插槽，1 个 Console 口。	台	1
2	网络优化中心控制网关系统软件（县级）	支持多种形式的链路接入、负载均衡、NAT、IPv4/6 路由协议、虚拟系统、高可用性等功能，并具备扫描、DoS/DDoS、异常数据包等传统网络攻击的高性能防护能力。 IPSec VPN、SSL VPN、L2TP、PPTP、GRE、 IPSecVPN 增加 SM1、SM2、SM3、SM4 国密软算法的支持， 支持精确识别 5000 余种互联网应用，700 余种移动应用及 1000 余类文件特征，在全栈可视化的基础上，通过应用、用户、内容等多维一体的精细化访问控制。	套	1

3	网络优化中心管理分析平台接入授权（县级）	接入授权，接入水利厅管理分析平台，每套包含 1 个 License。	套	1
4	网络优化中心分中心威胁感知平台接入授权（县级）	接入授权，接入市级分中心威胁感知平台，每套包含 1 个 License。	套	1
5	网络优化中心漏洞扫描安全服务	安全扫描评估主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描，能对被评估目标进行覆盖面广泛的安全漏洞查找，能够真实、全面地反映主机系统、网络设备、应用系统所存在的网络安全问题和面临的网络安全威胁，在漏洞扫描工作实施结束后，会出具《漏洞扫描报告》，其中包括漏洞原理及相关修复建议，并提供相应的技术支持协助客户修复漏洞。	项	1
6	网络优化中心安全基线检查服务	通过“自动化工具配合人工检查”方式参考安全配置基线进行检查，主要包括网络设备、安全设备、操作系统、数据库、中间件等安全配置基线，采用主流的安全配置核查系统或检查脚本工具，以远程登录检查的方式工作，完成设备的检查，针对物理隔离或网络隔离的设备使用检查脚本工具来补充完成检查工作，在基线检查工作实施结束后，会出具《基线检查报告》，其中包括基线检查不合规项及相关修复建议，并提供相应的技术支持协助客户修复漏洞。	项	1
7	网络优化中心 Web 渗透测试服务	采用各种手段模拟真实的安全攻击，从而发现黑客入侵信息系统的潜在可能途径。渗透测试工作以人工渗透为主，辅助以攻击工具的使用。主要的渗透测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、云服务客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试、社会工程等，在初次渗透测试工作实施结束后输出《XX 系统渗透测试报告》，并协助客户修复漏洞，待漏洞修复完成后，进行复测，并输出《XX 系统渗透测试报告（复测）》。	项	1

8	网络优化中心高级威胁检测服务	威胁情报来自云端的分析成果，可对 APT 攻击、新型木马、特种免杀木马进行规则化描述。依托于云端的海量数据，通过基于人工智能自学习的自动化数据处理技术，依靠以顶尖研究资源为基础的多个国内高水平安全研究实验室为未知威胁的最终确认提供专业高水平的技术支撑，所有大数据分析出的未知威胁都会通过专业的人员进行人工干预，做到精细分析，确认攻击手段、攻击对象以及攻击的目的，通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌。对客户的全流量数据进行安全事件分析，及时发现用户网络中存在的高级安全事件并提出解决方案。服务内容包括： 1、安全事件发现：基于威胁情报，发现高级威胁、APT 攻击、异常流量行为、僵尸木马攻击等安全事件； 2、定位与溯源：对发现的安全事件定位到具体的 IP 地址； 3、安全事件处置建议：对发现的安全事件进行深度分析后给出事件处理建议，并协助客户解决问题。	项	1
9	网络优化中心产品管家服务	产品更新服务。根据客户安全域、IT 管理制度，在线或离线更新：根据客户 IT 资源，评估资源瓶颈，制定错峰更新计划。 运维策略指定服务。根据客户生产业务、IT 管理制度，制定常规安全策略，维护临时安全策略；根据客户 IT 资源，评估客户生产业务资源需求，额定安全业务资源占用，制定错峰资源占用计划。 故障排查服务。定位不符合预期的功能表现、性能表现；公司内产品进行改进，三方厂商产品协助定位。 运维成果汇报服务。根据客户安全域、IT 管理制度，制定汇报方案。	项	1
10	网络优化中心安全监察服务	产品告警监察服务。负责监控产品告警，根据告警中的线索，核实威胁、追溯来源、评估影响范围；提供单次威胁响应，不持续遏制威胁的方法。 安全播报监察服务。负责监控奇安信安全运营服务中心发布的安全播报，根据安全播报中的线索、核实威胁、追溯来源、评估影响范围；提供单次威胁响应，不持续遏制威胁的方法。 安全通告监察服务，负责监控客户上级监管单位，对客户的安全事故通告。根据通告中的线索，核实威胁、追溯来源、评估影响范围；提供单次威胁响应，不持续遏制威胁的方法。 威胁反馈监察服务。负责监控客户内部，线下反馈的威胁事件。根据反馈的线	项	1

		索，核实威胁、追溯来源、评估影响范围；提供单次威胁响应，不持续遏制威胁的方法。		
11	网络优化中心安全评估服务	安全故障评估与修复服务。负责使用公司及三方工具或产品，周期性评估满足利用条件的系统、设备、软件漏洞，或者正在进行侵害的安全威胁。 配置脆弱性评估与加固服务。负责使用公司及三方工具或产品，周期性评估容易被威胁攻破的脆弱性配置，包括操作系统配置，设备配置，软件组件配置等。 沦陷迹象评估检查服务。负责使用公司及三方工具或产品，周期性评估日志中隐含的威胁入侵的痕迹，包括系统日志、设备日志、产品日志等。 敏感信息评估检查服务。负责使用公司及三方工具或产品，周期性评估敏感信息在政企内的覆盖范围，适用于涉密行业。	项	1

（五）其他

1）每年固定时间节点（与业主商定），制定详细的售后服务方案和计划，提出优化服务建议

2） 巡检完成后提交服务总结报告；

3） 提交半年和年度服务总结报告；

4） 协助做好运行维护相关预案、制度的制定；

5） 配合水利厅做好有关信息化项目的安装调试部署工作；

6） 配合做好运行维护技术交流等服务；

7） 配合做好运行维护重大故障原因调查工作。

（六）培训：一年维保期内，开展一次项目人员（县（乡）级不少于1人，培训时间不少于2个工作日）的系统使用和设备维护集中培训，让受训人员掌握基本技术要求、熟悉操作、设备故障初步诊断、维护管理等技术，保障系统正常运行。培训人员的交通、住宿费用自理，成交供应商负责培训的场地、材料、讲师及餐费。

（七）响应时间：接到用户请求后，在1小时内给予回应；不能通过远程解决的，安排技术工程师到故障现场；对于设备损坏等严重故障，8小时内无法解决的，24小时内必须给出解决方案并用备品备件进

行更换。

承诺提供以下售后服务：

1、服务期：本次采购服务期限一年。

2、出现任何维护保养问题，接通知后 30 分钟内到达指定地点，一般故障 24 小时内解决，需厂家技术支持应在 3 天内解决，需要更换配件或维修时间较长时，及时与采购人联系，提供解决方案、预算、工期等，并及时排除故障。

3、若在维护保养过程中发现损坏的配件需购买更换的，由采购人及我公司双方现场确认再另行报价购买，我公司不收取更换配件所需人工费。

4、维护保养须提供相关记录，包括维保内容、设备现状、工作时间等并经采购人签字确认。每季度提交一次维护保养工作总结和下一季度工作计划。

5、因我公司服务技术之原因造成采购人设备损坏的，由我公司负责赔偿。

6、每次维护保养工作结束后，我公司向采购人提交维修保养合格验收单。

7、我公司在服务过程中，严格遵守采购人的保密管理制度，对技术服务严格实行保质保量优质服务。

8、我公司不定期为采购人提供技术咨询与指导服务。

9、我公司在采购人场地维保期间，应严格遵守安全规程操作，如因我公司原因造成人员伤亡责任，由我公司承担。

10、成交供应商须提供所维护设备生产厂家授权书原件

服务地点：采购人指定的地点。

二、线路运维服务提供以下服务：

市到县主线路（80M）

1、地市水利局到县水利局的 MSTP 电路，电路带宽为 50M，提供 RJ45 接口，电路为光纤接入，免费提供所有传输接入设备；

2、采用 MSTP 技术传输，提供端到端的透明传输电路，不采用 VPN 组网，为确保提供的电路为端到端透明传输电路，电路开通验收时必须采用专用测试仪表对电路进行远端环回测试；

3、电路端到端平均往返时延≤15ms，平均时延抖动≤5ms，丢包率≤0.1%。

4、数量：1 条

县到乡镇专线(10M)

1、地市/县水利局到乡镇水利站的 MSTP 电路，电路带宽为 10M，提供 RJ45 接口，电路为光纤接入，免费提供所有传输接入设备；

2、采用 MSTP 技术传输，提供端到端的透明传输电路，不得采用 VPN 组网，为确保提供的电路为端到端透明传输电路，电路开通验收时必须采用专用测试仪表对电路进行远端环回测试；

3、电路端到端平均往返时延≤15ms，平均时延抖动≤5ms，丢包率≤0.1%。

4、数量：27 条

我公司承诺提供售后服务：

1、服务期：线路采购服务期为五年。

2、我公司承诺在签订合同后 3 个工作日内实施完成

2、出现任何维护保养问题，接通知后 30 分钟内到达指定地点，一般故障 24 小时内解决，需厂家技术支持应在 3 天内解决，需要更换配件或维修时间较长时，及时与采购人联系，提供解决方案、预算、工期等，并及时排除故障。

3、若在维护保养过程中发现损坏的配件需购买更换的，由采购人及我公司双方现场确认再另行报价购买，我公司不收取更换配件所需人工费。

4、维护保养须提供相关记录，包括维保内容、设备现状、工作时间等并经采购人签字确认。每季度提交一次维护保养工作总结和下一季度工作计划。

5、因我公司服务技术之原因造成采购人设备损坏的，由成交供应商负责赔偿。

6、每次维护保养工作结束后，我公司向采购人提交维修保养合格验收单。

7、我公司在服务过程中，严格遵守采购人的保密管理制度，对技术服务严格实行保质保量优质服务。

8、我公司不定期为采购人提供技术咨询与指导服务。

9、我公司在采购人场地维保期间，应严格遵守安全规程操作，如因我公司原因造成人员伤亡责任，由成交供应商承担。

二、服务地点：采购人指定的地点。

竞标人（**公章**）：广西广播电视信息网络股份有限公司

法定代表人（负责人）或委托代理人**签名**：

日期： 2020 年 7 月 20 日

注：此函由多页构成的，应逐页加盖竞标单位公章并由法定代表人（负责人）或委托代理人签字。