磋 商 响 应 文 件

（正本）

采购项目名称：西宁市人大代表网络履职平台软件运维项目

采 购 单 位：西宁市人民代表大会常务委员会办公室

采 购 方 式：竞争性磋商

采 购 预 算：15.7 万元

供应商（公章）：青海秦云信息科技有限公司

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

二〇二六年十月十日

目　　录

第一部分　资格性审查文件**.....3**

一、磋商函.....4

二、法定代表人证明书.....5

三、法定代表人授权书.....6

四、供应商承诺函.....7

五、供应商诚信承诺书.....8

六、供应商资格证明文件.....9

七、无重大违法记录声明.....11

八、财务状况、缴纳税收和社会保障资金证明.....12

第二部分　符合性审查文件**.....13**

九、磋商最初报价表.....14

十、服务要求响应表.....15

十一、供应商的类似业绩证明材料.....22

十二、供应商认为在其他方面有必要说明的事项.....23

12.1　关于“18.3 评审标准和分值分配”的响应说明.....23

12.2　总体运维服务方案.....27

12.3　应急响应服务方案.....37

12.4　项目团队人员配置.....42

12.5　履约能力.....43

12.6　开发运维能力（软件著作权）.....44

12.7　以往业绩.....44

12.8　本地化服务能力.....44

12.9　“（二）运维项目采购需求”逐条响应对照.....46

12.10　其他需要说明的事项.....48

十三、最终磋商报价表.....51

第一部分　资格性审查文件

一、磋商函

致：西宁市人民代表大会常务委员会办公室

我们收到西宁市人民代表大会常务委员会办公室磋商文件，经研究，法定代表人＿＿＿＿＿＿（姓名、职务）正式授权＿＿＿＿＿＿（委托代理人姓名、职务）代表供应商青海秦云信息科技有限公司（供应商名称、地址＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）提交磋商响应文件。

据此函，签字代表宣布同意如下：

1、我方已详阅磋商文件的全部内容，包括澄清、修改条款等有关附件，承诺对其完全理解并接受。

2、磋商有效期自磋商之日起 60 天内有效。如果在规定的磋商时间后，我方在磋商有效期内撤回磋商文件或成交后不签约的，承担相应法律责任。

3、我方同意按照贵方要求提供与磋商有关的一切数据或资料，理解并接受贵方制定的评标办法。

4、与本磋商有关的一切正式往来通讯请寄：

地址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿　　邮编：＿＿＿＿＿＿

电话：＿＿＿＿＿＿＿＿＿＿＿＿＿＿　　传真：＿＿＿＿＿＿＿＿＿＿

法定代表人姓名：＿＿＿＿＿＿　　职务：＿＿＿＿＿＿

供应商名称：青海秦云信息科技有限公司

统一社会信用代码：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

二、法定代表人证明书

法定代表人证明书

致：西宁市人民代表大会常务委员会办公室

＿＿＿＿＿＿（法定代表人姓名）现任我单位＿＿＿＿＿＿职务，为法定代表人，特此证明。

法定代表人基本情况：

性别：＿＿＿＿　　年龄：＿＿＿＿　　民族：＿＿＿＿

地址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

身份证号码：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

附法定代表人第二代身份证双面扫描（或复印）件：

【此处粘贴法定代表人身份证正、反面复印件，并加盖供应商公章】

磋商响应单位：青海秦云信息科技有限公司（公章）

2026 年 10 月 10 日

三、法定代表人授权书

法定代表人授权书

致：西宁市人民代表大会常务委员会办公室

青海秦云信息科技有限公司系中华人民共和国合法企业，法定地址＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿。

＿＿＿＿＿＿（法定代表人姓名）特授权＿＿＿＿＿＿（委托代理人姓名）代表我单位全权办理西宁市人大代表网络履职平台软件运维项目（采购项目名称）的磋商、答疑等具体工作，并签署全部有关的文件、资料。

我单位对被授权人的签名负全部责任。

被授权人签署的所有文件（在授权书有效期内签署的）不因授权的撤销而失效。

授权期限：自磋商之日起 60 天。

被授权人联系电话：＿＿＿＿＿＿＿＿＿＿＿

授权人（法定代表人）签字或盖章：＿＿＿＿＿＿

职务：＿＿＿＿＿＿

被授权人（委托代理人）签字或盖章：＿＿＿＿＿＿

职务：＿＿＿＿＿＿

附被授权人第二代身份证双面扫描（或复印）件：

【此处粘贴被授权人身份证正、反面复印件，并加盖供应商公章】

磋商响应单位：青海秦云信息科技有限公司（公章）

2026 年 10 月 10 日

四、供应商承诺函

供应商承诺函

致：西宁市人民代表大会常务委员会办公室

关于贵方 2026 年 9 月 28 日西宁市人大代表网络履职平台软件运维项目（项目名称）采购项目，本签字人愿意参加磋商，提供采购一览表中要求的所有服务，并证实提交的所有资料是准确的和真实的。同时，我代表青海秦云信息科技有限公司（供应商名称），在此作如下承诺：

1、完全理解和接受磋商文件的一切规定和要求；

2、若成交，我方将按照磋商文件的具体规定与采购人签订采购合同，并且严格履行合同义务，按时提供优质的服务。如果在合同执行过程中，发现质量、数量出现问题，我方一定尽快处理，如果对甲方造成经济损失的，承担相应的经济责任。

3、我方保证甲方在使用该产品或其任何一部分时，不受第三方提出的侵犯专利权、著作权、商标权和工业设计权等知识产权的起诉，若有违犯，愿承担相应的一切责任。

4、我方承诺，除磋商文件中规定的进口产品外，所投的产品均为国产产品，且均符合国家强制性标准。若有不实，愿承担相应的责任。

5、在整个磋商过程中我方若有违规行为，贵方可按磋商文件之规定给予处罚，我方完全接受。

6、若成交，本承诺将成为合同不可分割的一部分，与合同具有同等的法律效力。

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

五、供应商诚信承诺书

供应商诚信承诺书

致：西宁市人民代表大会常务委员会办公室

为了诚实、客观、有序地参与采购活动，愿就以下内容作出承诺：

一、自觉遵守各项法律、法规、规章、制度以及社会公德，维护廉洁环境，与同场竞争的供应商平等参加采购活动。

二、参加本次采购活动时，严格按照磋商文件的规定和要求提供所需的相关材料，并对所提供的各类资料的真实性负责，不虚假应标，不虚列业绩。

三、尊重参与采购活动各相关方的合法行为，接受采购活动依法形成的意见、结果。

四、依法参加采购活动，不围标、串标，维护市场秩序，不提供“三无”产品、以次充好。

五、积极推动采购活动健康开展，对采购活动有疑问、异议时，按法律规定的程序实名（加盖单位章和法定代表人签名）反映情况，不恶意中伤、无事生非，以和谐、平等的心态参加政府采购活动。

六、认真履行成交供应商应承担的责任和义务，全面执行采购合同规定的各项内容，保质保量地按时提供采购物品。

若本企业（单位）发生有悖于上述承诺的行为，愿意接受相关处理。

本承诺是采购项目磋商文件的组成部分。

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

六、供应商资格证明文件

根据磋商文件要求，我方提交下列资格证明文件（扫描件或复印件均加盖我方公章），所提供的全部资料真实、有效、合法：

序号	材料名称	份数	备注
1	营业执照（统一社会信用代码）副本复印件	1	经营范围涵盖本项目采购内容
2	开户许可证（或基本存款账户信息表）复印件	1	
3	法定代表人身份证双面复印件	1	
4	法定代表人授权委托书原件及被授权人身份证双面复印件	1	法定代表人本人参加磋商时免于提供
5	经审计的 2025 年度财务状况报告（含资产负债表、利润表、现金流量表及附注、审计机构及人员资质证明）	1	
6	近半年内任意 1 个月依法缴纳税收的证明材料	1	
7	近半年内任意 1 个月为职工缴纳社会保障资金的证明材料	1	
8	参加采购活动前 3 年内在经营活动中没有重大违法记录的书面声明	1	见本册“七”
9	“信用中国”网站无任何不良记录的查询截图	1	查询时间为磋商截止时间前 10 天内
10	中国政府采购网“政府采购严重违法失信行为记录名单”查询截图	1	查询时间为磋商截止时间前 10 天内
11	ISO27001 信息安全管理体系认证证书复印件	1	对应评审“履约能力”
12	ISO20000 信息技术服务管理体系认证证书复印件	1	对应评审“履约能力”

序号	材料名称	份数	备注
13	ITSS 信息技术服务标准符合性证书（运行维护四级）复印件	1	对应评审“履约能力”
14	计算机软件著作权登记证书复印件（5 项）	5	对应评审“开发运维能力”
15	类似项目合同业绩证明材料（含合同首页、内容及金额页、签字盖章页）	3 份以上	对应评审“以往业绩”
16	拟派项目团队人员身份证、资格证书复印件及在职证明	1 套	对应评审“团队人员”
17	本地化服务能力相关证明材料（本地服务机构、人员、场地等）	1 套	对应评审“本地化服务能力”
18	其他资质、荣誉证书（如有）	1 套	

【以上材料按顺序装订于本册之后，复印件均须加盖供应商公章】

七、无重大违法记录声明

无重大违法记录声明

致：西宁市人民代表大会常务委员会办公室

我单位青海秦云信息科技有限公司郑重声明：参加本次采购活动前 3 年内，我单位在经营活动中没有重大违法记录，未被列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，不存在因违法经营受到刑事处罚或者责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚的情形。

我方已通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）进行自查，查询结果无任何不良记录，查询时间为本次磋商截止时间前 10 天内，查询截图已装订于本册之后。

我方对本声明的真实性负责。如有不实，愿承担相应法律责任并接受采购人及相关监督部门的处理。

【此处粘贴“信用中国”网站无不良记录查询截图并加盖公章】

【此处粘贴中国政府采购网政府采购严重违法失信行为记录名单查询截图并加盖公章】

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

八、财务状况、缴纳税收和社会保障资金证明

按照《政府采购法》第 22 条规定，我单位提供以下相关材料：

1、我单位提供经审计的 2025 年度财务状况报告，包括资产负债表、利润表、现金流量表及其附注，并列示审计方的营业执照、执业证书及审计人员的执业证书复印件。

2、我单位提供近半年内任意 1 个月依法缴纳税收和职工社会保障资金记录的证明材料。我单位依法纳税、依法为职工缴纳社会保险，不存在欠缴、漏缴情形；依法免税或不需要缴纳社会保障资金的，我方将提供相应文件证明。

以上材料复印件均加盖供应商公章，原件备查。

【此处装订：2025 年度审计报告全本复印件（含附注及审计机构、审计人员资质）】

【此处装订：近半年内任意 1 个月纳税证明（税收完税证明或纳税申报表）】

【此处装订：近半年内任意 1 个月职工社会保险费缴纳证明（社保缴费明细或参保凭证）】

磋商响应单位：青海秦云信息科技有限公司（公章）

2026 年 10 月 10 日

第二部分　符合性审查文件

九、磋商最初报价表

磋商最初报价表

供应商名称（盖章）：青海秦云信息科技有限公司　　日期：2026 年 10 月 10 日

项目名称	磋商总价（人民币：元）	服务期	备注
西宁市人大代表网络履职平台软件运维项目	大写： 小写：	自合同签订生效之日起至 2027 年 9 月 4 日	详见报价说明

注：1.填写此表时不得改变表格形式。

2.磋商报价为总报价。必须包括：包括项目编制费、服务费、税金及其他不可预见费等全部费用。

3.“服务期”是指完成服务所需的具体时间。

4.我方承诺：本次磋商报价为闭口价，成交后在合同有效期内价格不变；最终报价不出现两个或两个以上的报价方案；我方报价未超出采购预算控制额度（15.7 万元）。

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

十、服务要求响应表

服务要求响应表

供应商名称：青海秦云信息科技有限公司

采购需求服务指标			磋商响应服务指标		偏离
序号	名称	服务要求、指标	名称	服务要求、指标	
1.1	网络优化检测服务	保障平台平稳安全运行，随时监控硬件以及软件使用情况。	网络优化检测服务	完全响应。建立7×24小时运行监控体系，对主机、数据库、中间件、应用服务的关键指标秒级采集与阈值告警，专人值守监控大屏，每日两次汇总软硬件运行情况并形成《平台运行状态日报》报送甲方，发现异常立即按应急处置流程介入。（详见12.2.3.1）	0
1.2	网络优化检测服务	采用软件自动化实时对硬件进行检测服务，合理分析硬件使用情况后再做出最优规划。	网络优化检测服务	完全响应。部署自动化巡检工具，按小时、日、周周期自动采集服务器、存储、网络设备的使用率与健康状态，每季度出具《硬件资源使用分析报告》，量化分析资源利用率、增长趋势与瓶颈点，提出扩容、调优、替换等最优规划建议报甲方确认后执行。	0
1.3	网络优化检测服务	软件优化检测服务，通过人工配合优化监测软件完成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测试数据，调整、优化软件建设规划。	网络优化检测服务	完全响应。采用人工配合优化监测软件的方式，定期对应用系统开展参数梳理与压力、负载测试，测定平台在安全边界内的最高性能负载；结合测试数据编制《软件性能测试与优化报告》，	0

采购需求服务指标			磋商响应服务指标		偏离
				同步调整优化软件建设规划，测试环境验证通过后于业务低峰期上线。	
1.4	网络优化检测服务	结合硬件与软件检测报告，统计分析数据，逐步优化完善人大代表网络履职平台。	网络优化检测服务	完全响应。建立运维数据台账，将硬件巡检报告与软件检测报告合并分析，按季度形成《平台运行综合分析报告》，识别性能瓶颈与安全隐患，制定并落实优化措施，持续迭代优化完善人大代表网络履职平台。	0
2.1	平台计算资源维护	保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服务器的维护工作，包括系统安装，系统补丁更新；对网络故障进行判断和排查。	平台计算资源维护	完全响应。建立服务器及网络设备资产台账，统一编号标记（责任人、用途、位置、IP、维保期）；定期开展系统安装、补丁更新、账户权限核查与日志清理；网络故障按“发现—定位—处置—复核—归档”闭环处理，一般故障 2 小时内恢复，重大故障不间断处置直至恢复。	0
2.2	平台计算资源维护	使用安全措施处理包括但不限于 DDOS 攻击在内的系统安全问题。	平台计算资源维护	完全响应。部署抗 DDoS 流量清洗、云防护联动、WAF、IPS/IDS 及防火墙策略优化等安全措施，配置异常流量监测与自动封禁策略，制定 DDoS 攻击专项处置方案，与云服务商、运营商建立流量清洗绿色通道，保障攻击期间平台可用。	0
2.3	平台计算资源维护	需要定期测试系统安全性，根据	平台计算资源维护	完全响应。每季度开展一次安全	0

采购需求服务指标			磋商响应服务指标		偏离
		现有系统架构规划、调整安全防护措施。		自查（漏洞扫描、弱口令核查、配置基线核查、渗透测试），每年配合完成等保测评；依据测试结果及现有系统架构动态规划调整安全防护策略，形成《安全测试报告》《安全加固方案》并落实整改。	
2.4	平台计算资源维护	实时的对网络流量进行监控，处理异常问题。	平台计算资源维护	完全响应。通过流量分析设备与流量镜像对南北向、东西向流量实时监控，设置流量基线，对异常连接、异常外联、异常上传等行为实时告警并及时定位处置，流量日志留存不少于 6 个月以备审计。	0
3.1	平台软件维护	根据《中华人民共和国网络安全法》要求，服务器主机、应用平台软件应满足《信息安全技术网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整改。	平台软件维护	完全响应。依据《网络安全法》及 GB/T 22239 第三级要求逐项开展差距分析，对不满足项建立整改清单，在甲方规定时限内完成整改并复测，确保服务器主机、应用平台软件持续满足等保三级要求。	0
3.2	平台软件维护	乙方应配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等工作的情况；对测评过程中需要乙方提供包括但不限于文字资料、技术支持的情况。	平台软件维护	完全响应。指定专人作为测评对接人，配合甲方完成安全管理制度建设、测评方案编写、资料收集、现场测评、渗透测试与整改复测等各环节工作，按要求及时提供文字资料与技术支持，并承担与平台软件相关的整改工作。	0

采购需求服务指标			磋商响应服务指标		偏离
3.3	平台软件维护	在使用过程中需要对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、数据库出现漏洞的，需及时修复。漏洞来源包括但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。	平台软件维护	完全响应。建立7×24小时漏洞信息渠道，完整覆盖国家、省、市网信或公安部门发布，平台涉及软件所属厂家发布，国内外知名安全厂家发布，乙方上级部门通知，甲方通知五类来源；建立漏洞台账，按高危24小时内、中危3个工作日内、低危7个工作日内完成修复，修复前做好备份与回退预案，形成《漏洞修复记录表》。	0
3.4	平台软件维护	定时完成对系统程序、数据库进行备份、恢复、临时数据统计分析。	平台软件维护	完全响应。按日增量、周全量、月归档策略完成系统程序与数据库备份，备份数据异机异地保存并定期校验可用性，每季度至少开展一次恢复演练；按甲方要求完成临时数据统计、报表导出与分析。	0
3.5	平台软件维护	根据网站优化检测结果对网站进行持续优化，提出优化方案。	平台软件维护	完全响应。结合网站性能与安全检测结果，从前端加载、页面渲染、数据库索引、缓存策略、静态资源等方面持续优化，每半年提交《网站优化方案》，经甲方确认后实施并跟踪成效。	0
3.6	平台软件维护	对西宁人大平台进行持续的优化和维护升级。	平台软件维护	完全响应。服务期内持续对平台功能、性能、兼容性与界面体验进行优化和维护升级；对国家、省、市政策和人大工作要求引起的架构调整与软	0

采购需求服务指标			磋商响应服务指标		偏离
				件开发需求及时响应，与甲方协商实施，服务期内不降低服务质量。	
3.7	平台软件维护	平台内无效或者问题链接定期处理，并对平台的网络安全进行防护做出相关措施。	平台软件维护	完全响应。每月对全站链接开展一次有效性扫描（首页、栏目页、详情页、附件、外链），形成《错链死链清单》并修复或下线；同时通过WAF、防篡改、防注入、访问控制、日志审计等措施持续强化平台网络安全防护。	0
4.1	页面分布及内容修改	采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技术措施进行内容安全检测，确保信息发布准确无误。	页面分布及内容修改	完全响应。部署内容安全检测系统，全年至少开展一次全站内容安全检测（政治性差错、敏感词、错别字、违规外链、暗链、挂马等）并出具《全站内容安全检测报告》；每篇信息发布前经技术检测通过、并经人工复审后方可发布，确保发布内容准确无误。	0
4.2	页面分布及内容修改	根据甲方的要求对页面分布、数据、内容进行适当调整。	页面分布及内容修改	完全响应。建立“需求提出—确认—实施—验证—反馈”工作流程，按甲方要求对栏目结构、页面布局、模板样式、数据呈现与内容适时调整，一般调整24小时内完成，较大调整3个工作日内完成，紧急调整即时响应。	0
4.3	页面分布及内容修改	根据甲方的需要，建设1-2个专题栏目。	页面分布及内容修改	完全响应。按甲方需要，服务期内完成1-2个专题栏目的策划、	0

采购需求服务指标			磋商响应服务指标		偏离
				页面设计、模板制作、栏目配置与内容填充，视觉风格与西宁人大网整体一致，并同步做好移动端适配。	
5.1	微信公众号及门户网站信息发布	根据甲方需求，负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审。	微信公众号及门户网站信息发布	完全响应。配备专职新媒体编辑与内容审核人员，负责“西宁人大”微信公众号日常内容更新与维护（选题、编辑、排版、图片处理、发布、后台维护、数据统计）及门户网站各栏目内容更新与维护；严格执行“三审三校”和发布前人工复审制度，做到政治性、事实性、表述性差错零发生，重要会议活动信息按甲方要求第一时间发布。	0
6.1	培训	供应商需对甲方业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。	培训	完全响应。运维服务期内为甲方业务操作人员、技术维护人员提供不少于一次业务、技术及安全培训，内容涵盖平台业务操作、日常维护、常见故障处理、网络安全与保密要求等，提供培训方案、课件、现场或线上授课、实操演练、培训考核及《培训总结报告》。	0

注：1.本表已按照磋商文件第五部分“（二）运维项目采购需求”中序号的指标逐项填写，共 6 类 20 项，无遗漏。

2.本表以招标项目参数要求为基本磋商响应要求，我方响应指标全部满足招标项目参数要求，偏离栏全部列“0”，不存在“+”“-”偏差。

3.我方响应内容具体、明确，不含糊、不伪造，与所附证明材料一致。

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

十一、供应商的类似业绩证明材料

我方提供自 2025 年以来的类似业绩证明材料。类似业绩是指与采购项目在服务类型、使用功能、合同规模等方面相同或相近的项目。我方提供的每份业绩材料均包含合同首页、合同内容及金额所在页、供货合同签字盖章页的扫描件（或复印件），并加盖我方公章。

我方 2025 年以来同类平台开发与运维业绩情况如下：

序号	项目名称	采购人	合同金额（元）	签订时间	服务内容
1	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿年＿＿月	平台软件开发与运维
2	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿年＿＿月	政务网站及新媒体运维
3	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿年＿＿月	人大（党政）业务平台运维
4	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿＿＿＿＿	＿＿＿＿＿＿	＿＿＿＿年＿＿月	信息系统运行维护

注：上表所列业绩的数量与金额以所附合同扫描件为准，我方保证真实、有效；每提供一份合同得 2 分，我方提供的合同份数满足评审上限要求。

【此处装订：合同一（首页、合同内容及金额页、签字盖章页）复印件并加盖公章】

【此处装订：合同二（首页、合同内容及金额页、签字盖章页）复印件并加盖公章】

【此处装订：合同三（首页、合同内容及金额页、签字盖章页）复印件并加盖公章】

【此处装订：合同四（首页、合同内容及金额页、签字盖章页）复印件并加盖公章，如有）】

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

十二、供应商认为在其他方面有必要说明的事项

为便于磋商小组全面了解我方对本项目采购需求的理解深度与履约能力，我方就磋商文件“18.3 评审标准和分值分配”及第五章“磋商及采购项目服务要求（二）运维项目采购需求”作如下完整响应与说明。本章内容与第十部分“服务要求响应表”互为补充，如二者表述有差异，以本章详细说明为准。

12.1 关于“18.3 评审标准和分值分配”的响应说明

我方已逐项研读磋商文件“18.3 评审标准和分值分配”，本项目综合评分总分 100 分，其中磋商报价 10 分、商务部分 20 分、技术部分 70 分。我方对各评审因素均具备响应条件，并已在磋商响应文件相应位置提供证明材料。现逐项说明如下。

12.1.1 评审分值构成与响应情况总览

类别	子项	满分	评审标准要点	我方响应情况	证明材料所在位置
磋商报价	报价	10	满足磋商文件要求且最后报价最低的供应商的价格为磋商基准价，其价格分为满分；其他供应商报价得分 =（磋商基准价／最后磋商报价）×价格权值（10%）×100。	我方按磋商文件规定格式完整填报磋商最初报价表，接受现场最终报价；报价为包含服务费、税金及不可预见费等全部费用的闭口价，未超出采购预算控制额度 15.7 万元，不存在两个及以上报价方案。	本册“九、磋商最初报价表”“十三、最终磋商报价表”
商务部分	履约能力	9	具有 ISO27001 信息安全管理体系证书得 3 分；ISO20000 信息技术服务管理体系认证证书得 3 分；ITSS 信息技术服务标准符合性证书四级得 3 分。须提供证明材料复印件并加盖公章。	我方持有 ISO27001 信息安全管理体系认证证书、ISO20000 信息技术服务管理体系认证证书、ITSS 信息技术服务标准符合性证书（运行维护四级），三项证书均在有效期内，可完整取得本项 9 分。	第六部分“六、供应商资格证明文件”第 11、12、13 项
商务部分	开发运维能力	5	具有国家版权局颁发的①资源分发系统②内容动态管理系统③手机 APP 平台④云	我方拥有与上述五类系统功能相对应的自主计算机软件著作权共５项，可完整取	12.6 节及所附软件著作权登记证书

类别	子项	满分	评审标准要点	我方响应情况	证明材料所在位置
			平台点播直播系统⑤干部基础信息管理子系统软件著作权，每提供一个得 1 分，最多得 5 分。	得本项 5 分。	
商务部分	以往业绩	6	以 2025 年至今类似项目合同业绩为评审依据，每提供一份合同得 2 分，最多得 6 分。需提供包含合同首页、合同内容及金额所在页、签字盖章页的扫描或复印件。	我方提供 2025 年以来政务信息化平台开发与运维类合同业绩不少于 3 份，均包含完整的合同首页、内容及金额页、签字盖章页，可取得本项 6 分。	11 部分及 12.7 节
技术部分	团队人员	10	项目负责人具有信息系统项目管理师（高级）证书得 2 分；项目运维经理具有系统集成项目管理工程师（中级）证书得 2 分；核心技术团队每提供 1 名具有信息安全工程师（中级）或高级网络信息安全工程师（NEACE）或注册信息安全专业人员相关证书的得 2 分、具有工业和信息化行业专项技术证书（国产化操作系统高级运维）的得 2 分，最高 4 分。提供身份证、证书复印件及在职证明并加盖公章。	我方拟派项目负责人具备信息系统项目管理师（高级）资格、项目运维经理具备系统集成项目管理工程师（中级）资格；核心技术团队成员具备信息安全工程师（中级）、注册信息安全专业人员（CISP）、工业和信息化行业专项技术证书（国产化操作系统高级运维）等资格，可完整取得本项 10 分。	12.4 节及所附人员证书、在职证明
技术部分	总体运维服务方案	35	针对网络优化检测服务、平台计算资源维护、平台软件维护、页面分布及内容修改、微信公众号及门户网站信息发布、培训提供总体运维服务方案，根据方案的延续性、完整	我方方案完整覆盖六个服务模块，对采购需求 20 项指标逐条响应，方案包含服务概述、需求分析、具体措施、质量保证与延续性说明，完整详细、科学合理、可操作性强。	12.2 节

类别	子项	满分	评审标准要点	我方响应情况	证明材料所在位置
			性、可行性综合评审。		
技术部分	应急响应服务方案	20	针对应急响应服务要求提供应急响应服务方案，根据方案的针对性、可行性综合评审。	我方方案明确应急组织体系、分级响应时限、监测预警、八类典型突发事件处置流程、资源保障、重要时间节点保障和演练修订机制，针对性强、可行性高。	12.3 节
技术部分	本地化服务能力	5	在西宁市有本地服务能力的得 5 分，没有的不得分。需提供相关证明材料。	我方在西宁市设有本地服务机构与本地技术服务团队，具备本地办公场所、本地技术人员与本地备品备件保障能力，可实现现场响应与驻场服务，并提供相应证明材料。	12.8 节及所附证明材料

12.1.2 关于磋商报价（**10** 分）

我方磋商报价为完成本项目全部服务内容的总报价，包含服务费、验收费、手续费、安装费、调试费、培训费、售前售中售后服务费、设计费、保险费、税金及不可预见费等全部费用，已充分考虑西宁市人大代表网络履职平台运维的实际工作量、服务频次、驻场与现场服务成本以及重要时间节点保障投入，报价真实、合理、可执行。

我方承诺：磋商报价为闭口价，成交后在合同有效期内价格不变；报价不超出采购预算控制额度 15.7 万元；最终报价不出现两个或两个以上的报价方案；在提交最后报价之前不撤回磋商响应文件。

12.1.3 关于履约能力（**9** 分）

我方持有 ISO27001 信息安全管理体系认证证书、ISO20000 信息技术服务管理体系认证证书、ITSS 信息技术服务标准符合性证书（运行维护四级），三项证书均在有效期内且运行有效。上述体系文件已在我方日常运维服务中落地执行，覆盖信息安全管理制度、服务级别管理、事件与问题管理、变更与配置管理、连续性管理等方面，能够为西宁市人大代表网络履职平台运维服务提供规范、可控的管理保障。相关证书复印件已加盖我方公章，装订于本册材料之后。

12.1.4 关于开发运维能力（**5** 分）

我方拥有与本项目运维对象功能密切相关的自主计算机软件著作权，覆盖资源分发、内容动态管理、移动终端应用、云平台点播直播、干部基础信息管理等方向，具备对西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统进行持续开发优化与维护升级的技术能力。软件著作权清单及登记证书复印件详见 12.6 节。

12.1.5 关于以往业绩（**6** 分）

我方自 2025 年以来承接并完成多项政务信息化平台软件开发与运维服务项目，服务对象包括党政机关、人大政协及事业单位，服务内容涵盖平台软件开发、系统运行维护、内容与新媒体运维、网络安全防护等，合同履约情况良好，无质量投诉和违约记录。业绩合同材料详见第十一部分及 12.7 节。

12.1.6 关于团队人员（**10** 分）

我方针对本项目组建了专业运维服务团队，项目负责人具备信息系统项目管理师（高级）资格，具有大型政务平台项目管理经验；项目运维经理具备系统集成项目管理工程师（中级）资格，熟悉 IT 服务管理流程；核心技术团队成员持有信息安全工程师（中级）、注册信息安全专业人员（CISP）、工业和信息化行业专项技术证书（国产化操作系统高级运维）等资格，并具有人大业务系统、网站群、微信公众号运维的实操经验。同一人员仅适用于一条评分项，不重复计分。人员配置详见 12.4 节，身份证、资格证书复印件及在职证明一并附后。

12.1.7 关于总体运维服务方案（**35** 分）

我方总体运维服务方案（12.2 节）按“服务概述—服务需求分析—各项服务的具体措施—运维服务质量保证措施—方案的延续性与知识转移”五个层次编写，对网络优化检测服务、平台计算资源维护、平台软件维护、页面分布及内容修改、微信公众号及门户网站信息发布、培训六个模块逐项提出可落地的措施，并明确了服务级别（SLA）、服务报告、考核评价、知识库与文档管理等内容，方案完整详细、科学合理、可操作性强。

12.1.8 关于应急响应服务方案（**20** 分）

我方应急响应服务方案（12.3 节）立足西宁市人大代表网络履职平台“两会”及重大政治活动期间不可中断的运行要求，建立了应急组织体系与 7×24 小时值守机制，明确了事件分级与响应时限，针对断网、页面篡改、病毒木马、DDoS 攻击、数

据库故障、设备故障、漏洞入侵、数据泄露等八类突发事件给出了具体处置流程、责任分工与恢复目标，并配套应急资源保障、重要时间节点专项保障和年度演练修订机制，方案针对性强、可行性高。

12.1.9 关于本地化服务能力（5 分）

我方为青海省内注册企业，在西宁市设有本地服务机构，拥有本地办公场所、本地技术人员与本地技术支撑资源，能够为西宁市人大常委会办公室提供快速现场响应、驻场服务和就近技术支持。本地化服务能力说明及承诺详见 12.8 节，相关证明材料一并附后。

12.2 总体运维服务方案

12.2.1 服务概述

（一）项目理解

西宁市人大代表网络履职平台是市人大代表依法履职、密切同人民群众联系、参与监督工作的重要信息化载体，由西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统四个模块构成，具有政治敏感度高、业务连续性强、内容安全要求严、重要时间节点访问集中的突出特点。平台一旦发生中断、篡改或数据安全事件，将直接影响人大依法履职和公众形象。我方充分理解本项目“稳定运行、安全可靠、内容准确、响应及时”的核心要求，将本项目作为重点项目予以保障。

（二）服务范围

依据磋商文件第五章“（二）运维项目采购需求”，本次运维服务范围包括六项内容：一是网络优化检测服务；二是平台计算资源维护；三是平台软件维护；四是页面分布及内容修改；五是微信公众号及门户网站信息发布；六是培训。

（三）服务对象

服务对象为西宁市人民代表大会常务委员会办公室及市、区（县）各级人大代表、平台业务操作人员、技术维护人员，服务范围覆盖西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统全部模块。

（四）服务期与服务地点

服务期：自合同签订生效之日起至 2027 年 9 月 4 日（具体以合同约定为准）。服务地点：西宁市（采购人指定地点）。

（五）服务团队与服务方式

组建“项目负责人 + 项目运维经理 + 核心技术团队 + 专业运维工程师”的项目团队，实行“后台集中监控 + 远程技术支持 + 本地现场服务 + 重要节点驻场值守”的服

务方式，提供 5×8 小时日常技术支持与 7×24 小时应急技术支持，电话支持即时响应，必要时提供现场技术支持。

（六）服务级别承诺

服务项目	响应方式	响应时限	承诺目标
一般咨询与业务协助	电话、远程、现场	即时响应	30 分钟内答复
一般故障（单点功能异常）	电话、远程、现场	15 分钟内响应	4 小时内恢复
重大故障（核心功能不可用）	电话、远程、现场	10 分钟内响应	2 小时内恢复或提供临时替代方案
紧急事件（断网、篡改、攻击、数据安全）	7×24 电话、不间断处置	立即响应	1 小时内控制影响，不间断处置直至恢复并提交事件报告
内容发布请求	人工复审后发布	按甲方要求	一般信息 24 小时内发布，重要信息即时发布

12.2.2 服务需求分析

结合平台架构与业务特点，我方对六项采购需求逐项开展需求分析，明确运维要点与风险控制点。

（一）网络优化检测服务

需求要点是“随时监控、自动检测、性能测定、持续优化”。平台由多套系统与多类设备构成，人工巡检难以及时发现隐性故障，需建立自动化监控与巡检机制；同时需通过负载与性能测试摸清平台性能边界，为扩容与优化提供数据依据。风险控制点在于监控缺失导致的故障发现滞后、性能瓶颈未及时识别。

（二）平台计算资源维护

需求要点是“设备台账与标记、系统维护与补丁、故障排查、攻击防护、安全测试、流量监控”。服务器与网络设备是平台的运行基础，需要资产化管理与周期性维护；面对 DDoS 等攻击和异常流量，需要具备发现、抑制与恢复能力。风险控制点在于资产不清、补丁滞后、流量异常未发现。

（三）平台软件维护

需求要点是“等保三级符合性、配合测评、程序与数据库维护、漏洞及时修复、备份恢复、持续优化升级、链接与安全防护”。这是本项目技术难度最高、工作量最大的模块，既要求满足等保三级的合规底线，又要求建立覆盖五类漏洞来源的快速修复机制，并保障数据可恢复。风险控制点在于漏洞修复不及时被通报、备份不可用、无效链接长期存在。

（四）页面分布及内容修改

需求要点是“全站与逐篇内容安全检测、页面与内容调整、专题栏目建设”。人大网站内容政治性、政策性强，内容安全是底线要求，需要技术手段与人工复审双重保障；同时页面与栏目需要随人大工作要求灵活调整。风险控制点在于发布内容出现政治性、事实性差错。

（五）微信公众号及门户网站信息发布

需求要点是“公众号与网站内容更新维护、发布前人工复审”。新媒体时效性强、传播面广，需配备专职编辑与审核人员，实行“三审三校”；同时要保证发布内容与人大工作口径一致。风险控制点在于表述不规范、口径不一致、发布不及时。

（六）培训

需求要点是“服务期内不少于一次业务、技术及安全培训”。培训对象为甲方业务操作人员与技术维护人员，需要贴合实操、便于掌握，形成可查阅的培训资料，提升甲方自主使用与初步处置能力。风险控制点在于培训流于形式、无考核无资料。

12.2.3 各项服务的具体措施

以下按磋商文件第五章“（二）运维项目采购需求”序号逐条给出响应措施，各项措施均为完全响应，不存在偏离。

12.2.3.1 网络优化检测服务

采购需求 1.1：保障平台平稳安全运行，随时监控硬件以及软件使用情况。

响应措施：（1）建立 7×24 小时运行监控体系，部署 Zabbix、Prometheus 等监控平台，对平台主机、数据库、中间件、应用服务的 CPU、内存、磁盘、端口、进程、服务可用性等指标进行秒级采集，设置分级阈值告警。（2）安排专人值守监控大屏，每日 9:00、17:00 两次汇总软硬件运行情况，形成《平台运行状态日报》报送甲方。（3）建立告警分级处置规则，告警 10 分钟内确认、30 分钟内反馈处置意见，异常情况立即按应急处置流程介入，确保西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统持续平稳安全运行。

采购需求 1.2：采用软件自动化实时对硬件进行检测服务，合理分析硬件使用情况后再做出最优规划。

响应措施：（1）部署自动化巡检工具，按小时、日、周三个周期自动采集服务器、存储、网络设备的 CPU 与内存使用率、磁盘 IO、磁盘余量、温度、风扇、电源、链路状态等硬件指标，自动生成巡检报告并留存不少于一年。（2）建立硬件健康度评分模型，对异常趋势（如磁盘坏道增长、内存错误、链路丢包）提前预警。（3）每季度出具《硬件资源使用分析报告》，对资源利用率、增长趋势、寿命周期

与瓶颈点进行量化分析，提出扩容、调优、替换等最优规划建议，报甲方确认后执行。

采购需求 1.3：软件优化检测服务，通过人工配合优化监测软件完成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测试数据，调整、优化软件建设规划。

响应措施：（1）采用“人工＋工具”方式开展软件优化检测，由运维工程师配合优化监测软件逐项梳理应用配置参数（连接池、缓存、线程、超时、日志级别、数据库参数等），形成参数基线。（2）定期在测试环境开展压力测试与负载测试，分级加压测试软件在安全边界内可承受的最高性能负载，记录 TPS、响应时间、错误率、资源占用等数据。（3）编制《软件性能测试与优化报告》，据此调整优化软件建设规划，优化内容经测试环境验证通过后于业务低峰期上线实施，并跟踪上线后效果。

采购需求 1.4：结合硬件与软件检测报告，统计分析数据，逐步优化完善人大代表网络履职平台。

响应措施：（1）建立运维数据台账，将硬件巡检报告、软件检测报告、告警与故障记录、性能测试数据统一归集，形成可追溯的数据链。（2）按季度对上述数据开展统计分析，识别平台性能瓶颈、安全隐患与高频故障点，形成《平台运行综合分析报告》。（3）根据分析结论制定优化措施清单，明确责任人、完成时限与验收标准，逐项落实并回访验证，逐步优化完善人大代表网络履职平台，实现运维工作的闭环管理。

12.2.3.2 平台计算资源维护

采购需求 2.1：保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服务器的维护工作，包括系统安装，系统补丁更新；对网络故障进行判断和排查。

响应措施：（1）建立服务器及网络设备资产台账，对设备统一编号并粘贴标记（含责任人、用途、部署位置、IP 地址、系统版本、维保期限等），每半年核对更新一次，做到资产清晰、责任到人。（2）按周开展服务器维护，包括系统安装与重装、系统与安全补丁更新、账户与权限核查、日志清理与归档、磁盘空间整理、时间同步校验等，形成《服务器维护记录表》。（3）建立网络故障处理流程，按“发现—定位—处置—复核—归档”闭环执行，一般网络故障 2 小时内恢复，重大网络故障不间断处置直至恢复，事后提交故障分析报告。

采购需求 2.2：使用安全措施处理包括但不限于 DDOS 攻击在内的系统安全问题。

响应措施：（1）部署抗 DDoS 防护措施，采用流量清洗与云防护联动方式，在互联网出口配置异常流量识别与自动压制策略，并保留一定的人工干预通道。（2）配置 WAF、IPS/IDS、防火墙访问控制策略，收紧暴露面，关闭非必要端口与服务，限制管理端口访问来源。（3）制定 DDoS 攻击专项处置方案，明确攻击识别、流量牵引、清洗、业务切换与事后加固步骤，并与云服务商、通信运营商建立流量清洗绿色通道，确保攻击期间平台可用。

采购需求 2.3：需要定期测试系统安全性，根据现有系统架构规划、调整安全防护措施。

响应措施：（1）每季度开展一次系统安全性测试，内容包括漏洞扫描、弱口令核查、安全配置基线核查、渗透测试与安全加固验证，测试范围覆盖操作系统、中间件、数据库、应用系统与网络设备。（2）出具《安全测试报告》，对中高危问题建立整改台账，按高危 24 小时内、中危 3 个工作日内、低危 7 个工作日内完成整改并复测。（3）依据测试结果和现有系统架构，动态规划、调整安全防护措施与安全策略，形成《安全加固方案》报甲方确认后实施。

采购需求 2.4：实时的对网络流量进行监控，处理异常问题。

响应措施：（1）通过流量分析设备与交换机流量镜像，对南北向与东西向流量进行实时监控，建立正常业务流量基线（带宽、并发连接数、请求特征等）。（2）对异常连接、异常外联、异常上传下载、异常时段访问、疑似扫描与爆破行为实时告警，疑似事件 30 分钟内定位确认。（3）发现异常流量立即处置，必要时采取限速、封禁、隔离、溯源等措施，处置过程与结论记入《网络安全事件处置记录》，流量日志留存不少于 6 个月以备审计。

12.2.3.3 平台软件维护

采购需求 3.1：根据《中华人民共和国网络安全法》要求，服务器主机、应用平台软件应满足《信息安全技术网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整改。

响应措施：（1）依据《中华人民共和国网络安全法》及 GB/T 22239《信息安全技术 网络安全等级保护基本要求》第三级要求，按安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个方面逐项开展差距分析。（2）对不满足项建立整改清单，明确整改措施、责任人与完成时限，在甲方规定时限内完成整改并复测验证。（3）建立等保合规状态跟踪表，每半年复核一次，确保服务器主机、应用平台软件持续满足等保三级要求。

采购需求 3.2：乙方应配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等工作的情况；对测评过程中需要乙方提供包括但不限于文字资料、技术支持的情况。

响应措施：（1）指定专人作为等保测评对接人，全程配合甲方及测评机构开展测评工作，配合内容包括前期材料准备、安全管理制度与测评方案编写协助、现场测评配合、渗透测试与整改复测配合、测评报告确认等。（2）按测评要求及时提供系统拓扑图、资产清单、配置说明、安全策略、日志记录等文字与技术资料，并加盖我方公章确认。（3）对测评发现的与平台软件相关的问题，由我方负责整改并复测，整改结果书面反馈甲方。

采购需求 3.3：在使用过程中需要对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、数据库出现漏洞的，需及时修复。漏洞来源包括但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。

响应措施：（1）建立 7×24 小时漏洞信息收集渠道，完整覆盖国家、省、市网信或公安部门发布，平台涉及软件所属厂家发布，国内外知名安全厂家（如 CNNVD、CNVD、厂商安全公告等）发布，乙方上级部门通知，甲方通知五类来源，指定专人每日巡查并形成漏洞情报台账。（2）建立漏洞分级处置机制：高危漏洞 24 小时内完成修复或采取临时缓解措施，中危漏洞 3 个工作日内修复，低危漏洞 7 个工作日内修复；确需延期的，书面说明原因并报甲方同意。（3）漏洞修复前完成数据与程序备份并制定回退预案，修复后在测试环境验证，于业务低峰期上线，形成《漏洞修复记录表》，逐条留痕可追溯。

采购需求 3.4：定时完成对系统程序、数据库进行备份、恢复、临时数据统计分析。

响应措施：（1）制定并执行备份策略：数据库每日增量备份、每周全量备份、每月归档备份；系统程序与配置文件变更时即时备份；备份文件加密存放、异机异地保存，保留周期满足甲方与等保要求。（2）每季度对备份数据开展一次可恢复性校验与恢复演练，形成《备份恢复演练报告》，确保备份数据真实可用；发生数据误删除或损坏时，按恢复预案在约定时限内完成数据恢复。（3）按甲方要求及时完成临时数据统计、报表导出与数据分析工作，统计结果经复核后提交甲方。

采购需求 3.5：根据网站优化检测结果对网站进行持续优化，提出优化方案。

响应措施：（1）定期对西宁人大网开展性能与安全检测，检测内容包括首页与栏目页加载速度、首屏时间、资源体积、并发承载能力、数据库慢查询、缓存命中率等。（2）结合检测结果，从前端资源压缩与合并、图片与静态资源优化、页面渲染优化、缓存策略优化、数据库索引与 SQL 优化、服务参数调优等方面持续优化。

（3）每半年提交《网站优化方案》，明确优化目标、措施、实施计划与预期效果，经甲方确认后组织实施并跟踪成效，形成优化前后对比数据。

采购需求 3.6：对西宁人大平台进行持续的优化和维护升级。

响应措施：（1）在服务期内对平台功能、性能、兼容性、界面体验、移动端适配等方面持续开展优化和维护升级，建立优化需求台账，按优先级排期实施。（2）对国家、省、市政策和人大工作要求需要对系统进行架构调整和软件开发的，我方及时响应并提出技术方案，与甲方协商实施，保障平台与政策要求同步。（3）实施前制定方案与回退预案，实施后进行回归测试与用户确认；我方承诺合同签订后在任何情况下（不可抗力因素除外）不降低服务质量。

采购需求 3.7：平台内无效或者问题链接定期处理，并对平台的网络安全进行防护做出相关措施。

响应措施：（1）每月对平台开展一次链接有效性扫描，范围覆盖首页、栏目页、详情页、附件下载、友情链接与外链，形成《错链死链清单》，逐条修复、替换或下线，扫描与修复结果报甲方备案。（2）持续强化网络安全防护，落实 WAF 防护、网页防篡改、防 SQL 注入与 XSS、访问控制与身份认证、防暴力破解、日志审计与安全监测等措施。（3）针对页面篡改、暗链、挂马等风险，部署页面完整性监测与定时比对机制，发现异常立即处置并留存证据、上报甲方。

12.2.3.4 页面分布及内容修改

采购需求 4.1：采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技术措施进行内容安全检测，确保信息发布准确无误。

响应措施：（1）部署内容安全检测系统，对全站历史与存量内容全年至少开展一次全量检测，检测内容包括政治性差错、敏感词与敏感表述、错别字、不规范简称与标点、违规外链、暗链、挂马与非法内容等，出具《全站内容安全检测报告》，对问题内容建立清单并逐一整改。（2）建立发布前技术检测前置机制，每篇信息发布前必须经内容安全检测系统检测通过，未通过的一律不得发布；同时对重大、敏感内容实行人工二次复核。（3）建立内容安全检测记录台账，留存检测时间、检测人、检测结果与处理意见，做到可追溯、可审计，确保信息发布准确无误。

采购需求 4.2：根据甲方的要求对页面分布、数据、内容进行适当调整。

响应措施：（1）建立“需求提出—确认—实施—验证—反馈”的工作流程，指定专人接收甲方需求，明确调整内容、完成时限与验收标准。（2）按甲方要求对栏目结构、页面布局、模板样式、配色与字体、数据呈现方式、栏目内容进行适时调

整，调整前备份原文件，调整后在测试环境验证并请甲方确认，一般调整 24 小时内完成，较大调整 3 个工作日内完成，紧急调整即时响应。（3）所有调整均记录归档，形成页面与模板变更台账，便于回溯与还原。

采购需求 4.3：根据甲方的需要，建设 1-2 个专题栏目。

响应措施：（1）按甲方工作需要，在服务期内完成 1-2 个专题栏目的建设，工作内容包括专题策划、栏目结构设计、页面视觉设计、模板制作、栏目配置、栏目上线与内容填充。（2）专题栏目视觉风格与西宁人大网整体风格保持一致，符合党政网站视觉规范，不使用建筑、宗教等不当配图元素；同步完成移动端适配与无障碍基本要求校验。（3）专题栏目上线后提供不少于一次巡检与优化，并按甲方要求配合做好专题内容的更新维护。

12.2.3.5 微信公众号及门户网站信息发布

采购需求 5.1：根据甲方需求，负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审。

响应措施：（1）配备专职新媒体编辑与内容审核人员，负责“西宁人大”微信公众号的日常内容更新与维护，包括选题策划、文稿编辑、版面排版、图片处理、发布推送、留言与后台维护、粉丝与阅读数据统计分析等；负责西宁人大门户网站各栏目内容的更新与维护，包括信息录入、编辑校对、图片与附件处理、栏目推送与页面更新等。（2）严格执行“三审三校”制度和发布前人工复审制度，坚持“先审后发、不审不发”，重点核查政治性、事实性、表述规范性与敏感信息，确保做到政治性差错、事实性差错、表述性差错零发生。（3）建立内容发布台账与例行报送机制，重要会议、重大活动和领导活动信息按甲方要求第一时间发布，重大敏感信息一律经甲方确认后发布；每月提交公众号与网站内容运维情况统计报告。（4）严格遵守保密要求，不擅自发布未经甲方确认的信息，不泄露甲方工作秘密与内部资料。

12.2.3.6 培训

采购需求 6.1：供应商需对甲方业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。

响应措施：（1）在运维服务期内为甲方业务操作人员、技术维护人员提供不少于一次业务、技术及安全培训，培训内容涵盖平台各模块业务操作、日常管理与维护、常见故障判断与初步处理、数据备份与恢复常识、网络安全与个人信息保护、信息发布与内容安全规范等。（2）培训前提交培训方案与课件报甲方确认，培训采取“集中授课 + 上机实操 + 答疑”方式，可根据甲方要求提供现场培训或线上培训，

并配套提供操作手册、常见问题手册等培训资料。（3）培训结束后组织培训效果考核与满意度评价，形成《培训总结报告》报甲方备案，确保参训人员学得会、用得上；甲方另有培训需求时，我方积极配合开展补充培训。

12.2.4 运维服务质量保证措施

（一）组织保障

本项目实行项目负责人负责制。项目负责人对项目整体质量与进度负总责；项目运维经理负责日常运维组织、任务分派、质量检查与甲方沟通；核心技术团队负责网络优化、平台软件维护、安全防护等内容的技术支撑；本地驻场工程师负责现场服务与日常巡检。实行“每周例会、每月质量分析会、每季度总结汇报”的运行机制，确保各项服务工作有部署、有落实、有检查、有改进。

（二）制度保障

依据 ISO20000 信息技术服务管理体系和 ISO27001 信息安全管理体系要求，落实事件管理、问题管理、变更管理、配置管理、发布管理、服务级别管理、可用性管理与业务连续性管理等流程，做到每项服务动作有流程、有记录、有责任人。

（三）技术保障

配置运行监控（Zabbix/Prometheus）、日志分析、自动化巡检、漏洞扫描、流量分析、网页防篡改与内容安全检测等工具平台，实现对平台状态的可视化监控与事件的可追溯管理；建立运维知识库，沉淀故障处理经验与操作规范，提升问题处置效率。

（四）服务报告制度

报告类型	主要内容	提交周期
平台运行状态日报	监控指标、告警与处置情况、当日服务事项	每个工作日
运维服务周报	本周服务事项、故障与处理、变更记录、下周计划	每周
运维服务月报	服务量统计、故障统计与分析、安全检查情况、优化建议	每月
季度与年度运维报告	设备与资源分析、安全测试与合规情况、重要节点保障情况、年度总结与改进建议	每季度、每年
专项报告	安全事件处置报告、漏洞修复记录、备份恢复演练报告、培训总结报告等	按要求及时提交

（五）考核与持续改进

我方接受甲方对服务质量的监督与考核，实行月度自评与甲方评价相结合的考核方式，考核结果与内部绩效挂钩，对未达标的服务事项限期整改并跟踪闭环。

考核指标	考核内容	考核标准	未达标处理
服务响应及时率	各等级服务事件的响应时限达标情况	≥98%	限期整改，连续两个月不达标启动专项整改并追究责任
故障恢复及时率	一般故障 4 小时、重大故障 2 小时内恢复情况	≥95%	限期整改并提交原因分析
平台可用率	平台各模块月度可用性	≥99.9%	提交专项改进方案并落实
内容发布准确性	发布内容政治性、事实性、表述性差错情况	零差错	立即更正并追究责任，形成通报
安全合规	漏洞修复时限达标、等保三级符合性、安全检查无通报	100%达标	限期整改，接受甲方相应处理

（六）文档与保密管理

建立项目文档清单（方案、记录、报告、台账、清单等），实行统一命名与版本管理，服务期满或甲方要求时完整移交甲方。全体项目人员签署保密承诺，严格遵守甲方保密与安全生产管理规定，不擅自复制、摘抄或带走甲方资料及数据，服务过程中形成的全部数据与文档归甲方所有。

（七）沟通机制

指定项目联系人并保持手机 7×24 小时畅通；建立例行沟通机制，每周向甲方报送服务周报，每月召开一次服务质量沟通会，重大事项即时上报；人员或联系方式变更时提前 5 个工作日书面通知甲方。

12.2.5 方案的延续性与知识转移

（一）业务与经验的延续性。我方具有人大业务平台、政务门户网站、微信公众号、履职服务平台等同类系统的开发与运维经验，熟悉人大代表履职业务场景、栏目体系、内容审核规范与重要时间节点保障要求，能够快速进入服务状态，最大限度缩短交接磨合期，保障平台运维工作的连续稳定。

（二）交接期安排。成交后，我方在合同约定时间内完成与原运维方的交接，内容包括系统架构与部署情况、设备资产台账、账号与权限、备份与恢复方案、监测告警配置、故障与处理记录、内容与模板资料等，形成《交接清单》并经甲方确认，做到“交接有清单、过程有记录、责任有界定”。

（三）知识库与文档移交。服务期内建立并持续完善运维知识库（含操作手册、常见问题库、故障处置手册、应急预案、配置文件与拓扑资料等），实行文档与配置的统一版本管理，甲方可随时查阅调用；服务期满时按甲方要求完整移交。

（四）人员稳定性保障。项目团队成员在服务期内保持稳定，项目负责人与核心技术团队成员不随意更换；确需更换时提前报甲方同意，并保证接替人员的资历与能力不低于原有人员，交接期间实行“新老并行”，避免服务中断。

12.3 应急响应服务方案

12.3.1 应急响应目标与适用范围

（一）工作目标。针对西宁市人大代表网络履职平台可能发生的网络中断、页面篡改、病毒攻击、数据损坏等突发事件，建立“统一指挥、反应快速、处置高效、保障有力”的应急响应机制，实现“早发现、早报告、早处置、早恢复”，最大限度降低突发事件对人大代表依法履职和人大工作的影响，保障平台安全稳定运行。

（二）适用范围。本方案适用于西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统在运维服务期内发生的各类安全与运行突发事件，包括但不限于网络中断、网站页面篡改、病毒木马与勒索软件、大规模 DDoS/CC 攻击、数据库故障与数据损坏、服务器与存储设备故障、漏洞被利用与网络入侵、数据泄露与信息安全事件，以及全国和省市“两会”、国庆、重大节庆等重要时间节点的安全保障工作。

（三）工作原则。坚持“预防为主、平战结合；统一指挥、分级负责；快速反应、协同处置；确保安全、优先恢复”；坚持“先保业务、后查原因”“先控制影响、后彻底解决”“先恢复运行、再追溯责任”，做到处置过程全程留痕、可追溯、可复盘。

12.3.2 应急组织体系与职责分工

成立项目应急处置小组，实行项目负责人负责制，7×24 小时值班响应。

角色	由谁担任	主要职责
应急总指挥	项目负责人	负责应急响应的统一指挥与决策，重大事件第一时间向甲方报告，协调资源投入，批准处置与恢复方案，对应急处置结果负责
现场处置组	项目运维经理及本地驻场工程师	负责现场故障排查、设备与系统处置、业务切换与恢复操作、现场配合甲方工作
技术支持组	核心技术团队成员（安全、数据库、应用方向）	负责远程技术分析、漏洞与攻击处置、数据恢复、代码与配置修复、技术方案编写
安全与情报组	信息安全工程师	负责安全事件监测预警、攻击溯源、漏洞情报收集、安全加固与等保相关事宜
内容与发布组	新媒体编辑与内容审核人员	负责紧急情况下网站与微信公众

角色	由谁担任	主要职责
		号内容的核实、更正、下线与发布口径统一
联络与保障组	项目联系人	负责与甲方、云服务商、通信运营商及设备厂商的对外联络协调，后勤与资料保障

同时明确 7×24 小时应急联系电话，值班人员实行首问负责制；值班表每月报甲方备案，人员变更及时更新。

12.3.3 应急响应分级与响应时限

事件级别	判定情形	响应时限	恢复时限	处置要求
Ⅰ级（特别重大）	平台全面不可用、数据被篡改或泄露、遭受大规模网络攻击、页面出现严重违法有害信息	立即响应（10 分钟内到场或接管）	2 小时内恢复核心业务	不间断处置，30 分钟内报告甲方，成立专项处置组，处置过程全程留痕，事后 2 个工作日内提交事件报告
Ⅱ级（重大）	核心功能模块不可用、数据库异常、重要数据无法访问	10 分钟内响应	4 小时内恢复	1 小时内报告甲方，指定专人处置并每 1 小时通报进展
Ⅲ级（较大）	部分功能异常、单台设备故障、性能明显下降、一般安全告警	30 分钟内响应	8 小时内恢复	4 小时内报告甲方，按流程处置并记录
Ⅳ级（一般）	个别用户操作问题、轻微告警、无业务影响的问题	1 小时内响应	24 小时内解决	按日常运维流程处理，纳入周报

发生Ⅰ级、Ⅱ级事件时，我方立即启动应急响应并同步报告甲方；事件处置完成后 48 小时内提交《应急处置报告》，内容包括事件经过、影响范围、处置措施、恢复情况、原因分析和整改措施，并按甲方要求配合进一步调查。

12.3.4 监测预警与信息报告

（一）监测预警。依托运行监控平台、流量分析、日志审计、网页防篡改与内容安全检测系统，对平台可用性、资源占用、异常流量、异常登录、异常外联、页面完整性、内容安全等进行 7×24 小时监测，建立分级告警阈值，告警信息同步推送至值班人员手机与工作群，做到异常早发现。

（二）预警发布。对可能引发突发事件的苗头性问题（如漏洞预警、攻击预警、极端天气与停电风险、重要节日活动期间访问高峰），提前发布内部预警，落实加固措施与值守安排，并视情况向甲方报告。

（三）信息报告。实行“即时快报—进展续报—结果终报”的三段式报告制度：突发事件发生后按分级时限要求向甲方电话或书面快报；处置过程中每 1 小时续报进展（Ⅰ、Ⅱ级）；处置结束后提交终报。报告内容客观准确，不迟报、不漏报、不瞒报。

12.3.5 典型突发事件应急处置流程

12.3.5.1 网络中断（断网）

处置流程：（1）接到告警或甲方通知后，值班人员 10 分钟内确认影响范围，判定为互联网出口、专线链路、网络设备还是局部线路问题。（2）本地驻场工程师立即检查网络设备指示灯、链路状态与配置，远程工程师同步开展链路测试与路由追踪；必要时联系通信运营商与云服务商协同排查。（3）对可切换的业务，按预案启用备用链路或临时网络通道，优先保障核心业务可用。（4）故障定位后立即修复，涉及设备硬件故障的启用备机替换。（5）恢复后进行全链路连通性与业务功能验证，形成故障分析报告，提出链路冗余优化建议。

12.3.5.2 网站页面篡改

处置流程：（1）发现或接报后立即启动Ⅰ级响应，第一时间对可疑页面采取临时下线或只读保护措施，防止影响扩大；同时保留现场证据（页面截图、访问日志、服务器日志、文件时间戳等）。（2）安全工程师开展入侵痕迹排查，定位篡改入口（弱口令、漏洞利用、上传漏洞、第三方组件漏洞等），封堵攻击路径，清理恶意文件与暗链。（3）从安全备份或可信版本中恢复被篡改页面与数据，逐页比对校验完整性与内容准确性。（4）恢复前经内容安全检测与人工复审确认无误，恢复后持续监测不少于 7 天。（5）按等级保护与网络安全事件报告要求，配合甲方完成事件报告与整改，出具《页面篡改事件处置报告》。

12.3.5.3 病毒木马与勒索软件

处置流程：（1）发现异常进程、异常外联或文件被加密后，立即隔离受感染主机（断开网络或下线），防止横向扩散，必要时对相关业务启用备用环境。（2）使用杀毒与专杀工具清除病毒木马，样本留存用于分析；确认无残留后方可恢复接入网络。（3）勒索软件事件优先保护未被加密的备份数据，评估数据可恢复范围，禁止支付赎金；从离线备份中恢复业务与数据，并核验数据完整性。（4）全面排查入侵途径，修补漏洞、重置口令、加固终端与服务器，出具事件报告并组织复盘。

12.3.5.4 大规模 **DDoS/CC** 攻击

处置流程：（1）监测到流量突增或业务响应变慢后，立即确认攻击类型（流量型、连接型、应用层）与攻击规模。（2）启动流量清洗与云防护联动，将流量牵引至清洗中心，配置限速、黑白名单与 CC 防护策略；同时启用备用出口或镜像站点保障信息发布类业务可用。（3）与云服务商、运营商启动绿色通道协同处置，必要时临时限制非核心端口与服务，优先保障核心业务。（4）攻击缓解后逐步放开策略，持续观察不少于 24 小时，防止二次攻击。（5）出具《攻击事件处置报告》，提出带宽扩容、防护策略优化等加固建议。

12.3.5.5 数据库故障与数据损坏

处置流程：（1）发现数据库不可用或数据异常后立即启动Ⅱ级响应，暂停相关写入操作，避免数据进一步损坏，同时保留故障现场日志。（2）判断故障类型（实例宕机、表空间满、主从异常、误删除、数据损坏），优先尝试实例恢复与日志恢复。（3）无法原地恢复时，按备份策略从最近可用的全量或增量备份中恢复数据，恢复前评估数据丢失范围（RPO）并报告甲方确认。（4）数据恢复后开展数据一致性与业务功能校验，确认无误后恢复对外服务。（5）分析故障原因，落实监控告警、容量管理与权限审计等改进措施，出具故障处置报告。

12.3.5.6 服务器与存储设备故障

处置流程：（1）接到硬件告警或宕机告警后，10 分钟内确认故障设备与影响范围，通知甲方。（2）具备冗余或集群能力的系统，按预案完成业务自动或手工切换，保障业务连续；单点设备故障的启用备机或备件替换。（3）硬件故障联系厂商或云服务商开展维修或更换，涉及数据恢复的按备份方案执行。（4）业务恢复后回补故障期间的数据并核验一致性。（5）建立硬件健康档案，对接近寿命或故障频发的设备提出更换建议，避免同类故障重复发生。

12.3.5.7 漏洞被利用与网络入侵

处置流程：（1）发现入侵迹象（异常账号、异常进程、异常定时任务、异常外联、日志异常）后立即开展应急处置，必要时断开受影响主机的对外连接。（2）安全工程师开展入侵取证与溯源，确定入侵路径与影响范围，评估数据是否被窃取或篡改。（3）封堵漏洞、清除后门与恶意程序、重置相关账号口令、加固安全策略。（4）修复后开展全面安全检查与漏洞复测，确认无残留威胁后恢复服务。（5）出具安全事件报告，按监管要求配合甲方完成上报与整改。

12.3.5.8 数据泄露与信息安全事件

处置流程：（1）确认事件后立即启动I级响应，第一时间报告甲方并采取阻断措施（下线涉事接口或页面、封禁账号、回收权限），防止泄露范围扩大。（2）固定证据（访问日志、操作日志、导出记录等），评估泄露数据范围、敏感程度与影响对象。（3）配合甲方按法律法规与上级要求开展情况报告、影响评估与告知处置，涉及公安、网信部门要求的按规定配合。（4）开展原因分析，落实权限最小化、数据加密、操作审计、敏感数据脱敏等整改措施。（5）出具事件处置报告与整改报告，并组织全员复盘与专项培训。

上述各类事件处置全过程均做到“有记录、有报告、有整改、有复盘”，处置记录纳入运维知识库，作为预案修订与人员培训的依据。

12.3.6 应急资源保障

（一）人力资源保障。应急小组 7×24 小时值班，本地驻场工程师 1 小时内可到达现场；核心技术团队远程即时支撑；建立后备人员名单，主备联动，确保人员休假、出差期间应急力量不减。

（二）技术资源保障。配备必要的服务器、网络设备备件与备机（或依托云资源快速开通），配备应急笔记本电脑、移动存储、专用工具软件与专杀工具；保持测试环境可用，用于紧急验证与演练。

（三）数据资源保障。严格执行备份策略，备份数据异机异地保存并定期验证可用性，确保极端情况下数据可恢复；建立系统镜像与配置基线，支持快速重建运行环境。

（四）外部资源保障。与云服务商、通信运营商、服务器与安全设备厂商建立联络机制与联系方式台账，明确故障报修与技术支持渠道；建立专家咨询渠道，重大事件可快速获得厂商与原厂支持。

（五）通信与资料保障。建立应急通讯录（甲方、我方、云服务商、运营商、厂商、监管单位）并每季度更新；准备应急资料包（系统拓扑、资产清单、账号与端口说明、应急预案、联系人表），确保断网情况下仍可离线使用。

12.3.7 重要时间节点保障方案

针对全国和省市“两会”、国庆、重大节庆等重要时间节点，实行“事前加固、事中值守、事后总结”的专项保障机制。

（一）事前（节点前 7 个工作日）。制定并向甲方报送专项保障方案；开展系统全面检查与安全加固，完成漏洞修复、口令与权限核查、备份与恢复演练、监控告警

阈值复核；开展压力测试与容量评估，按需扩容；确认应急资源与人员到位；关闭非必要的变更与发布窗口。

（二）事中（节点期间）。实行 7×24 小时双人值守与领导带班，本地驻场工程师现场值守；加强监控频次，对平台可用性、流量、内容安全进行加密巡检；暂停非紧急变更操作；内容发布严格执行“三审三校”与人工复审，重要信息第一时间发布；异常情况按应急分级即时处置。

（三）事后（节点结束后 3 个工作日内）。开展平台运行与安全状况复盘，汇总值守与处置情况，形成《重要时间节点运行保障总结报告》报甲方，提出改进措施并纳入年度预案修订。

12.3.8 应急演练与预案修订

（一）应急演练。服务期内每年至少组织一次应急演练，演练场景从断网、页面篡改、数据恢复、攻击处置等典型场景中选择，演练做到有方案、有脚本、有记录、有评估、有改进；邀请甲方参与或观摩，形成《应急演练报告》。演练结果作为预案修订与人员培训的重要依据。

（二）预案修订。每年对应急预案进行一次全面评审与修订，遇以下情况及时修订：平台架构或业务发生重大变化、国家法律法规与监管要求更新、上级或甲方提出新要求、发生重大事件或演练发现预案缺陷。修订后的预案报甲方确认备案。

（三）应急培训。将应急处置能力纳入团队日常培训内容，新入职人员上岗前完成应急流程培训，确保每名成员熟悉自身职责、处置流程与联络方式。

12.4 项目团队人员配置

我方针对本项目组建专业运维服务团队，人员配置如下（同一人员仅适用于一条评分项，不重复得分）：

序号	拟任岗位	姓名	职称与资格证书	主要职责
1	项目负责人	_ _ _ _	信息系统项目管理师（高级）	全面负责项目组织与管理、资源调配、质量与进度控制、重大事项决策与甲方沟通，对项目整体履约负责
2	项目运维经理	_ _ _ _	系统集成项目管理工程师（中级）	负责日常运维组织与任务分派、运维流程执行与质量检查、服务报告编制、应急现场处置组织
3	核心技术团队成员	_ _ _ _	信息安全工程师（中级）	负责安全测试与加固、漏洞修复、等

序号	拟任岗位	姓名	职称与资格证书	主要职责
				保三级符合性与测评配合、安全事件应急处置
4	核心技术团队成员	_ _ _ _	注册信息安全专业人员（CISP）	负责安全监测预警、攻击溯源与安全事件分析、安全策略与管理制度建设
5	核心技术团队成员	_ _ _ _	工业和信息化行业专项技术证书（国产化操作系统高级运维）	负责国产化操作系统环境的部署配置、运行维护、性能调优与故障处置
6	本地驻场运维工程师	_ _ _ _	相关专业技术资格及在职证明	负责本地现场巡检、设备与系统日常维护、内容发布协助、现场故障处置与甲方现场支持
7	内容编辑与审核人员	_ _ _ _	相关专业技术资格及在职证明	负责西宁人大网与“西宁人大”微信公众号内容更新维护、人工复审与发布

说明：1.上述人员均为我单位正式在职员工，已提供身份证、资格证书复印件及在职证明并加盖公章，装订于本册之后。2.项目负责人与核心技术团队成员在服务期内保持稳定，确需更换时提前报甲方同意，接替人员资历与能力不低于原有人员，交接期间实行新老并行。3.所有人员均签署保密承诺，并接受甲方关于安全生产与保密的各项管理规定。

12.5 履约能力

我方持有与本项目运维服务直接相关的管理体系与标准符合性证书，各项证书均在有效期内，且体系要求已在我方日常服务中落地执行：

序号	证书名称	证书编号	发证机构	有效期	对应评审得分
1	ISO27001 信息安全管理体系认证证书	_ _ _ _ _ _	_ _ _ _ _ _	_ _年_ _月	3 分
2	ISO20000 信息技术服务管理体系认证证书	_ _ _ _ _ _	_ _ _ _ _ _	_ _年_ _月	3 分
3	ITSS 信息技术服务标准符合性证书（运行维护四级）	_ _ _ _ _ _	_ _ _ _ _ _	_ _年_ _月	3 分

上述证书复印件已加盖我方公章并装订于本册之后（见“六、供应商资格证明文件”第 11、12、13 项）。我方承诺所提供证书真实有效，如有不实，愿承担相应法律责任。

12.6 开发运维能力（软件著作权）

我方拥有与本项目运维对象功能密切相关的自主计算机软件著作权，具备对西宁人大网、履职服务管理平台、移动终端 APP 及平台基础支撑系统进行持续开发优化与维护升级的技术能力：

序号	软件著作权名称	登记号	著作权人	取得方式	对应评审得分
1	资源分发系统	———————	青海秦云信息科技有限公司	原始取得	1 分
2	内容动态管理系统	———————	青海秦云信息科技有限公司	原始取得	1 分
3	手机 APP 平台	———————	青海秦云信息科技有限公司	原始取得	1 分
4	云平台点播直播系统	———————	青海秦云信息科技有限公司	原始取得	1 分
5	干部基础信息管理子系统	———————	青海秦云信息科技有限公司	原始取得	1 分

上述计算机软件著作权登记证书复印件已加盖我方公章并装订于本册之后（见“六、供应商资格证明文件”第 14 项）。我方承诺所提供证书真实有效，著作权权属清晰，不存在权属争议。

12.7 以往业绩

我方自 2025 年以来承接多项政务信息化平台开发与运维服务项目，服务类型、使用功能与合同规模均与本项目相同或相近，合同履约良好，无质量投诉与违约记录。业绩情况详见第十一部分“供应商的类似业绩证明材料”，并按磋商文件要求提供包含合同首页、合同内容及金额所在页、供货合同签字盖章页的扫描件（或复印件）并加盖我方公章。

我方承诺：所提供的业绩材料真实、有效，不存在虚列业绩情形；如有不实，接受采购人及相关监督部门按无效响应处理并承担相应法律责任。

12.8 本地化服务能力

（一）本地化服务能力说明。我方为青海省内注册的独立法人企业，注册地与实际服务机构均位于青海省西宁市，在西宁市设有固定办公场所与技术服务团队，

具备本地化的服务实施条件。能够为西宁市人大常委会办公室提供快速现场响应、本地驻场服务、就近技术支持与本地化沟通协作，有效降低沟通成本与响应时间，保障重要时间节点现场值守到位。

（二）本地化服务内容。一是本地驻场与现场服务：在服务期内根据甲方需要安排本地工程师现场值守与巡检，一般现场服务请求 2 小时内到达现场；重要时间节点实行现场值守。二是本地化沟通机制：本地联络人与甲方保持日常对接，每周报送服务周报，每月召开服务质量沟通会，重大事项即时上门沟通。三是本地资源保障：本地办公场所、工具设备、备品备件与技术资料就近可用，应急处置不受跨区域路途影响。四是本地化培训服务：培训在甲方指定地点现场开展，便于更多业务人员参加。

（三）本地化服务承诺函。我方郑重承诺：如本项目成交，我方将在合同签订后按承诺在西宁市配置本地服务力量，保障本地化服务能力在服务期内持续有效，不因人员变动、办公场所调整等原因降低本地化服务水平；如甲方认为本地化服务能力不足，我方在收到书面通知后 3 个工作日内整改到位。

本地化服务能力承诺函

致：西宁市人民代表大会常务委员会办公室

我方青海秦云信息科技有限公司系在西宁市注册并实际经营的独立法人企业，在西宁市设有办公场所与技术服务团队，具备为本项目提供本地化服务的条件和能力。我方承诺：如本项目成交，将在服务期内为本项目配置不少于 2 名本地技术人员，安排本地驻场与现场服务，一般现场服务请求 2 小时内到达现场；保持本地办公场所与技术支撑资源持续可用；不因人员变动或场所调整降低本地化服务水平。特此承诺。

【此处装订：营业执照（体现注册地）复印件并加盖公章】

【此处装订：本地办公场所产权证明或租赁合同复印件并加盖公章】

【此处装订：本地在职技术服务人员名册及社保缴纳证明（加盖公章）】

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

2026 年 10 月 10 日

12.9 “（二）运维项目采购需求”逐条响应对照

我方对磋商文件第五章“磋商及采购项目服务要求（二）运维项目采购需求”所列六类共 20 项服务指标逐条响应如下，全部完全响应招标项目参数要求，不存在遗漏与偏离（偏离栏统一列“0”）。

序号	采购需求服务指标（原文）	磋商响应服务指标	偏离
1.1	保障平台平稳安全运行，随时监控硬件以及软件使用情况。	完全响应。建立 7×24 小时运行监控体系，关键指标秒级采集与分级告警，专人值守、每日两次运行情况汇总报送，异常即时介入处置。	0
1.2	采用软件自动化实时对硬件进行检测服务，合理分析硬件使用情况后再做出最优规划。	完全响应。部署自动化巡检工具按小时、日、周周期自动巡检，每季度出具硬件资源使用分析报告并提出扩容调优规划建议。	0
1.3	软件优化检测服务，通过人工配合优化监测软件完成，通过对软件参数设置取得的使用效果，测试软件承受范围内达到最高性能负载。根据测试数据，调整、优化软件建设规划。	完全响应。人工配合优化监测软件梳理参数基线，定期开展压力与负载测试测定最高性能负载，据测试数据调整优化软件建设规划。	0
1.4	结合硬件与软件检测报告，统计分析数据，逐步优化完善人大代表网络履职平台。	完全响应。建立运维数据台账，按季度统计分析并形成平台运行综合分析报告，制定优化措施清单逐项闭环落实。	0
2.1	保证平台硬件设备长期、正常运转，需要对服务器和相关设备的统计和标记工作；定时检查和保障服务器的维护工作，包括系统安装，系统补丁更新；对网络故障进行判断和排查。	完全响应。建立设备资产台账并统一编号标记；按周开展系统安装、补丁更新、权限核查与日志清理；网络故障闭环处置，一般故障 2 小时内恢复。	0
2.2	使用安全措施处理包括但不限于 DDOS 攻击在内的系统安全问题。	完全响应。部署流量清洗与云防护联动、WAF、IPS/IDS 及防火墙策略优化，制定 DDoS 专项处置方案并与云服务商、运营商建立清洗绿色通道。	0
2.3	需要定期测试系统安全性，根据现有系统架构规划、调整安全防护措施。	完全响应。每季度开展漏洞扫描、弱口令核查、基线核查与渗透测试，每年配合完成等保测评，据测试结果动态调整安全防护措施。	0
2.4	实时的对网络流量进行监	完全响应。通过流量分析	0

序号	采购需求服务指标（原文）	磋商响应服务指标	偏离
	控，处理异常问题。	设备与流量镜像对南北向、东西向流量实时监控并设置流量基线，异常行为实时告警、30 分钟内定位确认并及时处置。	
3.1	根据《中华人民共和国网络安全法》要求，服务器主机、应用平台软件应满足《信息安全技术网络安全等级保护基本要求》第三级安全要求（以下简称“等保三级”），对不满足等保三级标准的，及时发现，及时整改。	完全响应。按等保三级十个方面逐项差距分析，不满足项建立整改清单并在甲方规定时限内完成整改复测，确保持续符合等保三级要求。	0
3.2	乙方应配合甲方进行等保三级测评工作。包括但不限于甲方需建立安全管理制度、方案编写等工作的情况；对测评过程中需要乙方提供包括但不限于文字资料、技术支持的情况。	完全响应。指定专人全程配合测评，协助安全管理制度与测评方案编写，及时提供文字与技术资料，承担与平台软件相关的整改工作。	0
3.3	在使用过程中需要对系统程序本身、中间件、数据库、数据等进行维护保证平台正常运行。对程序本身、操作系统、中间件、数据库出现漏洞的，需及时修复。漏洞来源包括但不限于国家、省、市网信或公安部门发布、平台涉及软件所属厂家发布、国内外知名安全厂家发布、乙方上级部门通知，甲方通知。	完全响应。建立 7×24 小时漏洞信息渠道，完整覆盖五类漏洞来源；建立漏洞台账，高危 24 小时内、中危 3 个工作日内、低危 7 个工作日内完成修复，形成漏洞修复记录表。	0
3.4	定时完成对系统程序、数据库进行备份、恢复、临时数据统计分析。	完全响应。按日增量、周全量、月归档策略备份并异机异地保存，每季度开展恢复演练，按甲方要求完成临时数据统计与分析。	0
3.5	根据网站优化检测结果对网站进行持续优化，提出优化方案。	完全响应。结合性能与安全检测结果持续优化前端加载、页面渲染、数据库索引与缓存策略，每半年提交网站优化方案并跟踪成效。	0
3.6	对西宁人大平台进行持续的优化和维护升级。	完全响应。服务期内持续优化维护升级平台功能、性能与兼容性，对政策与工作要求的架构调整和开发需求及时响应，不降低服务质量。	0

序号	采购需求服务指标（原文）	磋商响应服务指标	偏离
3.7	平台内无效或者问题链接定期处理，并对平台的网络安全进行防护做出相关措施。	完全响应。每月全站链接有效性扫描并修复或下线，落实 WAF、防篡改、防注入、访问控制与日志审计等防护措施。	0
4.1	采用技术措施全年完成至少一次全站内容安全检测，每篇信息发布前采用技术措施进行内容安全检测，确保信息发布准确无误。	完全响应。全年至少一次全站内容安全检测并出具报告；每篇信息发布前经技术检测通过并经人工复审后方可发布，检测记录可追溯。	0
4.2	根据甲方的要求对页面分布、数据、内容进行适当调整。	完全响应。按“需求提出—确认—实施—验证—反馈”流程适时调整，一般调整 24 小时内完成，较大调整 3 个工作日内完成，紧急调整即时响应。	0
4.3	根据甲方的需要，建设 1-2 个专题栏目。	完全响应。服务期内完成 1-2 个专题栏目的策划、设计、模板制作、配置与内容填充，风格统一并适配移动端。	0
5.1	根据甲方需求，负责“西宁人大”微信公众号的日常内容更新与维护、负责西宁人大门户网站的内容更新与维护，发布前进行人工复审。	完全响应。配备专职编辑与审核人员负责公众号及门户网站内容更新维护；严格执行“三审三校”与发布前人工复审，做到政治性、事实性、表述性差错零发生。	0
6.1	供应商需对甲方业务操作人员、技术维护人员运维服务期内进行不少于一次业务、技术及安全培训。	完全响应。服务期内提供不少于一次业务、技术及安全培训，配套方案、课件、实操演练、考核与培训总结报告。	0

综上，我方对西宁市人大代表网络履职平台软件运维项目采购需求的服务范围、服务内容、服务标准、服务时限及质量要求全部无偏离响应，偏离栏合计为“0”。若磋商过程中采购需求发生实质性变动，我方承诺按照磋商小组书面通知的变动内容重新作出响应。

12.10 其他需要说明的事项

12.10.1 无实质性偏离承诺

我方郑重承诺：本次提交的磋商响应文件已按磋商文件规定的格式、内容与顺序编制，对磋商文件第一至第五章的全部条款（包括供应商资格条件、磋商响应文件构成、服务要求、合同条款等）均无实质性偏离或保留，不存在任何采购人不能

接受的条件。磋商响应文件中所载全部内容真实、准确、完整，并作为成交后签订合同的依据。

12.10.2 履约与服务质量承诺

我方承诺：（1）成交后按合同约定投入合格、充足的运维技术人员，服务期内始终保持项目团队稳定，不降低服务质量；（2）提供 5×8 小时日常技术支持与 7×24 小时应急技术支持，一般故障 4 小时内恢复、重大故障 2 小时内恢复，紧急事件 1 小时内控制影响；（3）按时向甲方提交日报、周报、月报及专项报告，主动接受甲方监督与考核；（4）对由于日常操作造成的数据及安全问题及时进行维护，对平台软件本身存在的瑕疵及时修补；（5）按国家、省、市政策和人大工作要求需要进行架构调整和软件开发的，及时响应并与甲方协商实施。

12.10.3 廉洁自律承诺

我方承诺严格遵守国家法律法规和政府采购相关规定，在参与本项目磋商及履约过程中，不向采购人、磋商小组成员及相关工作人员进行任何形式的利益输送、请托说情或其他不当行为；不以行贿、串标、围标等违法方式谋取成交；自觉接受采购人及纪检监察、财政等部门的监督。如有违反，愿接受取消磋商（成交）资格、依法处罚等处理。

12.10.4 知识产权与成果归属承诺

我方承诺：本项目服务过程中形成的全部文档、源代码、配置资料、数据及工作成果，其知识产权与所有权归采购人所有；我方保证所提供的产品与服务不侵犯任何第三方的知识产权，如发生第三方权利主张，由我方负责处理并承担全部责任与费用；未经甲方书面同意，我方不将上述成果用于本项目以外的用途。

12.10.5 保密承诺

我方承诺：严格遵守《中华人民共和国保守国家秘密法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等法律法规及甲方保密管理规定；对在服务过程中知悉的甲方业务数据、工作秘密、内部资料、账号口令等信息严格保密，不擅自复制、摘抄、留存、外传或用于其他用途；项目人员全部签署保密承诺书，离场时按要求交回全部资料并清除本地数据；保密义务在服务期满后继续有效。

12.10.6 项目联系方式

为便于磋商与履约沟通，我方指定本项目联系方式如下（如有变更，我方将提前 5 个工作日书面通知甲方）：

项目联系人	_ _ _ _ _ _
联系电话（7×24 小时）	_ _ _ _ _ _ _ _ _ _ _ _
电子邮箱	_ _ _ _ _ _ _ _ _ _ _ _
传真	_ _ _ _ _ _ _ _ _ _ _ _
公司地址	_ _
计量单位与计量方式	全部采用国家法定计量单位，以人民币（元）为计价结算单位

十三、最终磋商报价表

最终磋商报价表

供应商名称（盖章）：青海秦云信息科技有限公司　　日期：　　年　　月　　日

项目名称	最后磋商总价（人民币：元）	服务期	备注
西宁市人大代表网络履职平台软件运维项目	大写： 小写：	自合同签订生效之日起至 2027 年 9 月 4 日	最终确定的服务承诺：

注：此表不需装订在磋商响应文件中，供应商事先须盖章、签字。在磋商期间，由磋商小组确定合格的供应商按要求现场填写。

特别说明：本表按磋商文件要求不需装订入册，我方已事先盖章、签字并单独持至磋商现场，在磋商小组确定后按要求现场填写最终报价。我方最终报价为闭口价，包含磋商文件规定的全部费用，且不超出采购预算控制额度（15.7 万元）。

磋商响应单位：青海秦云信息科技有限公司（公章）

法定代表人或委托代理人：＿＿＿＿＿＿（签字或盖章）

年　　月　　日