第三章 磋商项目技术、服务、商务及其他要求

（注：带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

3.1、采购项目概况

本项目共计 1 个包，采购自然资源业务云信息安全扩展资源系统服务

3.2、服务内容及服务要求

3.2.1 服务内容

采购包 1：
采购包预算金额（元）: 1,220,000.00
采购包最高限价（元）: 1,220,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	雅安市自然资源和规划局自然资源业务云信息安全扩展资源采购项目	1.00	1,220,000.00	项	软件和信息技术服务业	否	否	否	否

3.2.2 服务要求

采购包 1：

标的名称：雅安市自然资源和规划局自然资源业务云信息安全扩展资源采购项目

参数性质	序号	技术参数与性能指标
★	1	（一）服务内容 1. 雅安市内所有自然资源和规划部门的自然资源调查监测评价、国土空间规划实施监督、行政审批、政务服务、监

		管决策等各类应用基于专有云资源，参照等级保护 2.0（三级）相关要求为相关业务系统和应用提供服务。 1.1 通信网络安全服务，保证雅安市自然资源和规划部门“一张图”、大数据平台等信息系统以及各个区县汇聚网络共同组成雅安市自然资源和规划业务边界提供高可靠性隔离与访问控制、通信完整性与保密性、入侵和病毒防范、网络安全审计服务。 1.2 计算环境安全服务，对主机和应用系统用户进行身份鉴别和访问控制、安全审计、对主机和各类终端的入侵防范和恶意代码防护、数据保密性和完整性保护、数据备份与恢复、剩余信息和个人信息保护提供相应服务。 1.3 集中安全管控服务，提供系统管理、安全管理和审计管理功能，功能权限分离，三员（系统管理员、审计管理员、安全管理员）分离，具备对三员进行身份鉴别和操作审计等运维服务能力，具备对于资产规模和部署范围庞大的业务系统，提供统一的安全管理中心服务，对全网资产、日志、事件信息进行统一的监测、检测、响应和分析，掌握全网的信息资产安全状况，及时发现和处置安全事件；并能提供自动化工具进行全网主要设备的安全策略自动下发和集中管理服务能力。 1.4 安全管理和运维服务（3 年），按照等级保护和 ISO27001 的信息安全管理体系建设要求，从安全管理制度、安全管理机构、安全管理人员、安全运维管理等几个方面提供运维期安全管理体系化服务； 1.5 无条件配合支持后续的资源拓展及服务升级等相应工作，为后续该自然资源专有云扩展提供 3 级等保或满足更多需求奠定基础。 1.6 按采购人需求提供远程运维安全技术支持。
★	2	（二）主要功能或目标 2.1 为雅安市自然资源和规划部门信息系统安全保障体系提供以“一个中

		心、三重防护、三个体系”为核心指导思想，构建集防护、检测、响应、恢复于一体的全面的安全保障体系的服务，同时采用自主可控的国产安全软硬件以及操作系统组成，最大程度降低愈发严峻的由硬件、操作系统等带来的安全威胁，符合信创、等级保护、密码测评等工作要求。 2.2 提供“一个中心”即安全管理中心，即构建先进高效的安全管理中心，实现针对系统、产品、设备、策略、信息安全事件、操作流程等的统一管理； 2.3“三重防护”是指构建安全区域边界、安全计算环境、安全通信网络三维一体的技术防御体系。 2.4“三个体系”是指形成安全技术体系、安全管理体系、安全运维体系三个体系，三个体系相互融合、相互补充，形成一个整体的安全防御体系。其中，安全管理体系是策略方针和指导思想，安全技术体系是纵深防御体系的具体实现，安全运维体系是支撑和保障。 2.5 服务提供商须保证雅安市自然资源和规划部门信息系统安全保障服务相关网络、安全系统与雅安市政务云内及该环境下的自然资源专有云的有效对接，并实现政务外网与自然资源专网数据安全交换。
★	3	（三）安全技术体系 安全技术体系设计内容主要涵盖到 “一个中心、三重防护”。即安全运维管理中心、计算环境安全、区域边界安全、通信网络安全。 3.1 安全运维管理中心 安全管理中心是安全技术体系的核心和中枢，集安全监测中心、安全运维中心、安全防御中心和安全响应中心的功能为一体。 安全监测中心：其中主要包括对系统、设备安全监测和报警，并提供基于人工或工具的多层次的安全监测服务。 安全防御中心：在构建整体的技术防御体系的基础上，通过安全防御中心加强协调联动，进行积极主动防御，提升整体安全防御水平。

		安全运维中心：实现安全运维操作的流程管理和标准化管理，实现自动化安全运维，实现运维策略可视化。 安全响应中心：采用本地服务+云端服务+专家的新型工作模式，结合云端的威胁情报、大数据提供及时的技术保障服务。 3.2 三重防护 计算环境安全：为雅安市自然资源和规划部门信息系统打造一个可信、可靠、安全的计算环境。从系统、应用的身份鉴别、访问控制、安全审计、数据机密性及完整性保护、资源控制等方面，全面提升雅安市自然资源和规划部门信息系统在系统及应用层面的安全； 区域边界安全：从加强网络边界的访问控制粒度、网络边界行为审计以及保护网络边界完整等方面，提升网络边界的可控性和可审计性； 通信网络安全：从保护局域网和广域网的数据传输安全、整体网络架构可靠可用等方面保障网络通信安全。 3.3 安全管理体系 仅有安全技术防护，无严格的安全管理相配合，难以保障整个系统的稳定安全运行。在系统建设、运行维护、日常管理中都要重视安全管理，制定并落实安全管理制度，明确责任权力，规范操作，加强人员、设备的管理以及人员的培训，提高安全管理水平，同时加强对紧急事件的应对能力，通过预防措施和恢复控制相结合的方式，使由意外事故所引起的破坏减小至可接受程度。
★	4	（四）需满足的需求： 4.1 新一代的数据中心包含越来越多的弹性业务，数据中心的服务器和存储设备也将大量增加和使用，服务器和存储的成本投入越来越大。由于业务和系统的多样性，服务器和存储资源难以实现有效整合和统一管理。融合、开放将是数据中心必经之路，数据中心需要更为快速的提供所业务和系统需要的能力。 4.2 采用专有架构，可以有效整合服务器和存储资源，为机关单位业务提供

<table>
<tr><td></td><td></td><td>弹性扩展的计算资源、存储资源和网络资源，实现应用的负载均衡和 HA 高可用。并通过统一的运维监控、告警、对平台软硬件进行持续的软硬件统一监控，有效管理和监控数据中心的设备。
4.3 遵循标准、立足需求、以先进的技术为基础，以满足雅安自然资源和规划部门提升信息化建设水平、建设一张图实施检测信息系统为目的，总体规划，统一实施。按照以下几点原则进行设计：
安全性原则
整体架构应具有完善的安全防护体系，具有多重安全防护，无单一故障点，确保数据安全，保障业务的连续性。采用多种方式，防止各种途径的非法入侵和机密信息泄露，保证系统中的数据安全。
先进性原则
架构的选择遵循先进性原则，在保证安全、可靠、使用的前提下，选择先进、实用的系统架构、网络架构、存储技术和软件体系架构，保证应用的快速上线。
可扩展性原则
建设充分考虑扩展性，计算资源和存储系统可以灵活扩展，采用弹性技术架构，根据未来业务的发展，可以快速便捷的弹性灵活扩展，同时，未来也可以将更多业务系统迁移到平台之上。</td></tr>
<tr><td>★</td><td>5</td><td>（五）提供本项目服务所需辅助设备要求
<table>
<tr><th>服务名称</th><th>辅助设备要求</th><th>数量</th></tr>
<tr><td>边界下一代防火墙服务</td><td>1. 标准机架式设备，≥1 个管理口，≥1 个 HA 口，≥6 个千兆电口，≥12 个千兆光口，≥2 个万兆光口，冗余电源，网络层吞吐量(双向)：IPv4≥15000Mbps，IPv6≥</td><td>2</td></tr>
</table></td></tr>
</table>

				15000Mbps 应用层吞吐量(单向):IPv4≥8000Mbps,IPv6≥8000Mbps ,TCP 新建连接速率: IPv4≥90 万/秒,IPv6≥90 万/秒 TCP 并发连接数:IPv4≥2000 万,IPv6≥2000 万。 2. 提供服务的产品符合信创工作要求。(需提供服务承诺函,并加盖供应商公章) 3. 提供防火墙入侵防御功能,提供防火墙防病毒功能,提供三年防护服务。	
			安全管理边界防火墙服务	4. 标准机架式设备,≥1 个管理口,≥1 个 HA 口,≥6 个千兆电口,≥4 个千兆光口,≥2 个万兆光口,冗余电源,网络层吞吐量(双向):IPv4≥11000Mbps,IPv6≥11000Mbps,	2

				应用层吞吐量(单向)：IPv4≥7000Mbps，IPv6≥7000Mbps TCP新建连接速率： IPv4≥85万/秒，IPv6≥85万/秒 TCP并发连接数：IPv4≥1800万，IPv6≥1800万。 5. 提供服务的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章） 6. 提供防火墙入侵防御功能，提供防火墙防病毒功能，提供三年防护服务。		
			入侵检测服务	7. 标准机架式设备，≥1个管理口，≥1个HA口，≥4个千兆电口，≥4个千兆光口，≥2个万兆光口，冗余电源,满检速率≥24000Mbps。TCP并发连接数≥500万，提供三年防护服务。 8. 提供服务	1	

				的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章）	
			Web 应用安全防护服务	9. 标准机架式设备,≥1个管理口，≥5个千兆电口（≥2对bypass），≥4个千兆光口，≥2万兆光口,冗余电源,HTTP吞吐量≥3800Mbps。HTTP请求速率≥5万/秒。HTTP并发连接数≥85万，提供三年防护服务。 10. 提供服务的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章）	1
			终端安全管理服务	11. 提供≥50个桌面三年防护服务。 12. 系统部署采用C/S架构，管理采用B/S架构，管理员只需通过浏览器登录控制中心，即可对系统进行管理。能够对客户端	1

				进行统一管理，统一下达指令。 13. 支持飞腾、龙芯、鲲鹏、兆芯等硬件平台和银河麒麟、中标麒麟、中科方德、统信等桌面操作系统。 14. 提供服务的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章）	
			运维安全审计服务	15. 标准机架式设备,≥6个千兆电口，≥4个千兆光口，≥2个万兆光口,冗余电源,≥1T硬盘；≥200个管控设备许可，用户数不限制；并发字符≥200，图形≥100，提供三年服务。 16. 提供服务的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章）	1
			日志审计服务	17. 标准机架式设备，提供≥1个管理口，≥2个千兆电口，≥2	1

				个万兆光口，冗余电源,日志采集处理均值≥20000EPS，峰值≥35000EPS，提供≥100 日志源，提供三年服务。 18. 支持各类日志对象的日志数据采集，其中包括安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等。 19. 提供服务的产品符合信创工作要求。（需提供服务承诺函，并加盖供应商公章）	
			数据库审计服务	20. 标准机架式设备，提供≥1 个管理口，≥1 个 HA 口，≥4 个千兆电口，≥4 个千兆光口，≥2 个万兆光口,冗余电源,记录事件能力≥5W 条/秒，抓包速率≥5Gbps，提供三年审计服务。 21. 提供服务的产品符合	1

<table>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>信创工作要求。（需提供服务承诺函，并加盖供应商公章）</td><td></td></tr>
</table>
</td></tr>
<tr><td>★</td><td>6</td><td>（六）提供专有云所在地不低于200M网络带宽的专线链路接入采购人业务专网。</td></tr>
<tr><td>★</td><td>7</td><td>（七）服务考核办法
<table>
<tr><th>序号</th><th>指标名称</th><th>考核内容及评分标准</th><th>减分项（扣完为止）</th><th>自评分</th><th>最终得分</th><th>备注</th></tr>
<tr><td colspan="7">一、组织保障部分（共16分）</td></tr>
<tr><td>1</td><td rowspan="2">服务团队（8分）</td><td>明确的机构和人员负责信创云云平台服务工作。</td><td>未有设置对应机构、人员不清楚职责的，每次扣1分。</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td></tr>
<tr><td>2</td><td>现场驻场人员熟悉云平台情况，积极参与协</td><td>现场驻场人员出现工作散漫、不严谨、处理不及时、不认真负责等</td></tr>
</table>
</td></tr>
</table>

				调，全程跟踪事件，确保服务质量满足用户要求。	**问题，每发现一次扣1分**（情节严重的每次扣2分）。				
			3	会议参与（3分）	及时参加每次会议，含安全例会、专题讨论会、各类协调会议等。	缺席一次扣1分，迟到一次扣0.5分。			
			4	热线服务（5分）	建立有专门的服务热线，热线拨打畅通、通信质量良好，接听及	1）电话无人接听一次扣0.5分，因态度、礼仪规范受投诉扣1分。 2）服			

				时、服务态度良好、接听电话符合礼仪规范。	务态度恶劣的，受到甲方点名投诉或更严重情况的，每有一人/次扣2分 3）同一人员出现三次及以上，甲方有权要求人员更换				
		二、信息管理部分（33）							
		7	信息归档（4分）	**机**房日常巡检、设备巡检等登记簿是否完整，各类日志是否完整。	提供材料不完整每次扣1分，发现错误每次扣0.5分。				
		8	平台安全	加强对云	发生一般事故				

				性（24分）	平台的安全和可用性保障。	（平台故障四级），每起扣2分；发生较大事故（平台故障三级），每起扣4分；发生重大事故（平台故障二级）每起扣6分，发生特大事故（平台故障一级），每起扣8分。（故障分类参照信息安全事件划分标准）			
			9	日常监测（5分）	定期开展平台日常监测保障工作，	未建立台账扣1分，台账中存在遗漏或漏填一项			

				建立有监测保障制度，严格执行监测措施，建立有监测台账。	扣0.5。				
		三、安全管理部分（51分）							
		10	安全风险（5分）	定期排查云平台安全脆弱性，有效管控安全风险，提交各类安全风险处理报告。按使用单位要求进行相应处置。	未提交一次扣1分，未进行全网定期排查扣2分。未按使用单位要求进行相应处置，每次扣1分。				

			11	重大事件（15分）	及时、优先处理重大事件，具有共性问题的，应对全网或全平台事件进行排查或处理；普通问题必须在2小时内、复杂问题须在4小时内。	**未在规定时间内向用户提供反馈**和结果，扣2分；因人为原因导致处理时间超期或拖延扣3分；**因未及时处理导致形成全网或全平台事件，**每次**扣5分；因人为原因造成网络安全事件，**每次**扣5分。**			
			12	日常报告（3分）	**按**时完成租户月报，特殊情况事件说明	未在规定时间内提交，一次扣0.5分；未提交一			

					文档等。月报内容应含本月云安全基本情况及特殊事件的发生与处理情况。	次扣1分。			
			13	漏洞检查（4分）	每周进行漏洞扫描，并对漏洞扫描进行研判，将研判结果形成漏扫报告上报。按使用单位要求进行相应处置。	未在规定时间内提交，一次扣0.5分；未提交一次扣1分。未按使用单位要求进行相应处置，每次扣1分。			

			14	工作配合（6分）	**配合使用单位对上云安全组件个性化策略的部署和调试。**配合网络安全隐患进行整改。配合开展网络安全等级保护、密码测评等网络安全工作。配合开展信创工作。配合开展与云平台云安全	**未**配合，每次扣2分；配合质量不符合要求，每次扣1**分。**				

				建设相关的其它技术服务性工作。					
		15	安全检查（4分）	每周巡查安全组件情况，发现高危风险及时通知甲方，并对安全风险进行研判，作出专业分析报告。按使用单位要求进行相应处置。	**发现高危风险未及时通知扣1分，未对高危风险进行研判并出具分析报告扣1分；**未按使用单位要求进行相应处置，每次扣1分。				
		16	安全组件检查	每月对云安全组件	**发现问题未及时报告**和解				

			（4分）	进行检查，是否运行正常，出现问题，及时解决并向甲方单位报告。	决，每次扣1分			
		17	安全更新（5分）	云安全组件是否正常更新，特征库是否为最新。	每更新不及时一次扣1分。			
		18	策略更新（5分）	配合甲方完成各类策略上传、更新等工作。	每错误一次扣1分。			

3.2.3 人员配置要求

采购包 1：

详见详细评审

3.2.4 设施设备要求

采购包 1：

/

3.2.5 其他要求

采购包 1：

/

3.3、商务要求

3.3.1 服务期限

采购包 1：

自合同签订之日起 1165 日

3.3.2 服务地点

采购包 1：

采购人指定地点

3.3.3 考核（验收）标准和方法

采购包 1：

采购人将严格按照采购文件要求、响应文件应答、采购合同等内容，严格按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205 号）、财政部《政府采购需求管理办法》（财库[2021]22 号）、《雅安市财政局关于规范政府采购履约验收工作的通知》（雅财采〔2021〕50 号）文件的规定以及采购项目具体要求进行验收

3.3.4 支付方式

采购包 1：

分期付款

3.3.5 支付约定

采购包 1： 付款条件说明： 预付款支付：签订合同后，供应商向采购人提交预付款所需附件（附件内容包括但不限于足额的合法发票、收款信息等采购人财务制度要求的其他资料） ，达到付款条件起 7 日内，支付合同总金额的 30.00%。
采购包 1： 付款条件说明： 供应商提供服务在签订合同后 40 天内达到履约验收标准，通过专家验收后，供应商向采购人提交付款申请书以及付款所需附件 ，达到付款条件起 7 日内，支付合同总金额的 10.00%。
采购包 1： 付款条件说明： 第一年服务期费用支付（服务期从通过专家验收之日起起算）： 服务期满 1 年，费用按年据实支付（全额年度服务费为合同金额的 20%，每年度根据服务考核结果支付相应比例），考核结果公布后，供应商向采购人提交付款申请书以及付款所需附件，达到付款条件之日起 7 个工作日内，采购人向供应商支付本年度服务费用。年度服务考核等级设定 考核满分为 100 分制，采购人根据年度考核结果，作为支付成交供应商服务费用的依据，采购人将在通报考核结果后 7 个工作日内决定支付、扣减年度服务费用。 （1）考核分数为 90 分及以上，考核结果为优秀，则全额支付年度服务费。 （2）考核分数为 80 分-89 分，考核结果为良好，扣减 5%年度服务费。 （3）考核分数为 70 分-79 分，考核结果为合格，扣减 10%年度服务费，且采购人有权终止服务合同。 （4）考核分数为 69 分及以下，考核结果为不合格，扣减 15%年度服务费，且采购人有权终止服务合同,甲方有权追究相应民事赔偿责任 ，达到付款条件起 7 日内，支付合同总金额的 20.00%。
采购包 1： 付款条件说明： 第二年服务期费用支付（服务期从通过专家验收之日起起算）： 服务期满 2 年，费用按年据实支付（全额年度服务费为合同金额的 20%，每年度根据服务考核结果支付相应比例），考核结果公布后，供应商向采购人提交付款申请书以及付款所需附件，达到付款条件之日起 7 个工作日内，采购人向供应商支付本年度服务费用。年度服务考核等级设定 考核满分为 100 分制，采购人根据年度考核结果，作为支付成交供应商服务费用的依据，采购人将在通报考核结果后 7 个工作日内决定支付、扣减年度服务费用。 （1）考核分数为 90 分及以上，考核结果为优秀，则全额支付年度服务费。 （2）考核分数为 80 分-89 分，考核结果为良好，扣减 5%年度服务费。 （3）考核分数为 70 分-79 分，考核结果为合格，扣减 10%年度服务费，且采购人有权终止服务合同。 （4）考核分数为 69 分及以下，考核结果为不合格，扣减 15%年度服务费，且采购人有权终止服务合同,甲方有权追究相应民事赔偿责任 ，达到付款条件起 7 日内，支付合同总金额的 20.00%。
采购包 1： 付款条件说明： 第三年服务期费用支付（服务期从通过专家验收之日起起算）： 服务期满 3 年，费用按年据实支付（全额年度服务费为合同金额的 20%，每年度根据服务考核结果支付相应比例），考核结果公布后，供应商向采购人提交付款申请书以及付款所需附件，达到付款条件之日起 7 个工作日内，采购人向供应商支付本年度服务费用。年度服务考核等级设定 考核满分为 100 分制，采购人根据年度考核结果，作为支付成交供应商服务费用的依据，采购人将在通报考核结果后 7 个工作日内决定支付、扣减年度服务费用。 （1）考核分数为 90 分及以上，考核结果为优秀，则全额支付年度服务费。 （2）考核分数为 80 分-89 分，考核结果为良好，扣减 5%年度服务费。 （3）考核分数为 70 分-79 分，考核结果为合格，扣减 10%年度服务费，且采购人有权终止服务合同。 （4）考核分数为 69 分及以下，考核结果为不合格，扣减 15%年度服务费，且采购人有权终止服务合同,甲方有权追究相应民事赔偿责任 ，达到付款条件起 7 日内，支付合同总金额的 20.00%。

3.3.6 违约责任及解决争议的方法

采购包 1：

1.采购人及供应商双方必须遵守采购合同并执行合同中的各项规定，保证采购合同的正常履行。2.如因供应商在履行过程中的疏忽、失职、过错等故意或者过失原因给采购人造成损失或侵害，包括但不限于采购人本身的财产损失、由此而导致的采购人对任何第三方的法律责任等，供应商对此均应承担全部的赔偿责任。 3.如供应商有提交的成果达不到相关质量要求或未按采购人时间进度安排完成成果或拒绝履行合同内容等一系列其他严重失职行为的，采购人有权不支付合同相关款项，并有权无条件提出解除采购合同，一切因此产生的所有后果及损失等均由供应商承担，采购人不承担任何责任。

3.4 其他要求

1.供应商（投标人）成交（中标）价（单价、下浮、折扣等其他方式报价时核算的总价）即为完成本项目的一切费用，包括但不限于因项目实施可能产生的设备费、组织费用、交通费、人工费、服务费、知识产权费、代理服务费、税费等，采购人不再支付成交供应商除本项目成交金额外的任何费用。（提供承诺函，格式自拟，并加盖供应商公章） 2.承诺和响应的提醒：关于供应商针对本项目提供的相关承诺以及响应，包括但不限于资格部分，符合性部分、评分以及采购文件其他部分要求的所有承诺及响应，供应商如承诺、响应均应对其承诺、响应的内容负责，采购人、采购代理机构及相关监管单位如有必要，将核实供应商承诺、响应的真实性，因虚假承诺、响应引起的所有责任和成果由供应商自行承担，与采购人、采购代理机构及相关评审人员无关。（提供承诺函，格式自拟，并加盖供应商公章。） 3.合同签订时，需约定保密条款及网络安全责任条款。