

合同编号：DSJJTX20250360

厅内系统安全产品租用项目

运维服务合同

甲方：贵州省自然资源技术信息中心

乙方：贵州大数据产业集团有限公司

日期：2025年6月27日

本合同由以下三方共同签署：

甲方：贵州省自然资源技术信息中心

法定代表人：申朝永

通信地址：贵阳市中华北路省政府大院五号楼

邮政编码：550004

开户名称：贵州省自然资源技术信息中心

开户银行：中国银行股份有限公司贵阳市云岩支行

账号：133013494004

纳税人识别号：12520000G72513784R

联系人：江俊

联系电话：0851-86866497

乙方：贵州大数据产业集团有限公司

法定代表人：张平

通信地址：贵州省贵阳市贵阳国家高新技术产业开发区长岭街
道黔灵山路 357 号德福中心 A4 栋 21-23 楼 1-8 号

邮政编码：550081

开户名称：贵州大数据产业集团有限公司

开户银行：中国银行贵安新区分行

账号：133032073514

纳税人识别号：91520900322471673Q

联系人：陈果

联系电话：19199817017

【注：本合同双方的账户名称、开户银行、银行账号以本合同提供的为准，如有变更，变更一方应在距合同约定的相关付款期限届满二十五天前，以加盖财务专用章的书面文件通知对方；否则视为变更无效，一切不利后果由变更方自行承担。】

甲乙双方遵照《中华人民共和国民法典》及有关法律、行政法规规定，本着诚实信用、平等双赢、长期合作、共同发展的原则，经友好协商一致，就 2025 年厅内系统安全产品租用项目签订本合同，以兹共同信守。

一、服务内容

1. 服务类型：乙方向甲方提供 2025 年厅内系统安全产品租用项目运行维护服务。
2. 服务地点：贵州省贵阳市。
3. 服务内容及要求见附件 1。

二、服务周期

1. 乙方应在以下表格中的服务期限内向甲方开展运维服务。

序号	项目名称	服务开始时间	服务结束时间
1	厅内系统安全产品租用项目	2025 年 4 月 1 日	2026 年 3 月 31 日

2. 乙方应严格按进度计划要求执行，如因乙方原因而造成运维工作延误，则乙方应承担由此造成的相应责任和损失。

3. 服务到期后，若甲方尚未进行下一年度的服务采购，在此期间乙方应继续为甲方提供服务，服务费用以本合同约定的合同总金额按服务期 12 个月计算每月单价后结算（服务费用=服务月数*月单价），其他相关权利义务参照本合同约定履行。但是该行为不视为甲方同意就下一年度服务项目与乙方续签合同或者已经以事实行为续签合同。

三、服务标准

服务标准依照本合同条款“一、服务内容”及《信息技术软件维护》(GB/T20157-2006)、《信息技术服务运行维护第 1 部分：通用要求》(GB/T28827.1-2012)、《信息技术服务运行维护第 2 部

分：交付规范》(GB/T28827.2-2012)、《信息技术服务运行维护第3部分：应急响应规范》(GB/T28827.3-2012)、《信息技术服务质量评价指标体系》(GB/T33850-2017),以及《贵州省省级政务信息系统建设管理办法》(黔府办函〔2023〕2号)等文件的规定执行。

四、合同金额及付款方式

1. 乙方服务费,由甲方以转账方式支付至乙方在本协议中所指定的账户,款项均为无息支付。

2. 本项目合同总金额为(大写):人民币肆佰玖拾贰万壹仟伍佰零贰元整(小写: ¥4921502.00元),该金额为含税总价,包含了完成本项目所需的全部费用,包括但不限于:所有人工费、材料费、测评器材、软件使用费、人员往返差旅及食宿费、设备往返运输费、管理费、利润和税金等一切费用。

3. 付款方式:

(1) 本合同签订后7个工作日内,乙方向甲方支付合同总价10%的履约保证金,即(大写):人民币肆拾玖万贰仟壹佰伍拾元贰角(小写: ¥492150.20元)。

(2) 甲方收到乙方足额支付的履约保证金,向乙方支付合同总价的60%,即(大写):人民币贰佰玖拾伍万贰仟玖佰零壹元贰角(小写: ¥2952901.20元)。

(3) 甲方在2025年9月30日前向乙方支付合同总价的30%,即(大写):人民币壹佰肆拾柒万陆仟肆佰伍拾元陆角(小写: ¥1476450.60元)。

(4) 甲方在2025年12月31日前向乙方支付合同总价的

10%，即(大写)：人民币肆拾玖万贰仟壹佰伍拾元贰角(小写：
¥492150.20元)。

(5) 服务期满，正式组织验收通过，甲方扣除乙方应当支付的赔偿金/违约金后(如有)，将剩余履约保证金(如有)无息退付给乙方。合同期内，因乙方违约导致履约保证金被扣除的，乙方应当在扣除之日起15个工作日内进行补足。乙方支付的履约保证金不足以抵扣其违约赔偿金的，乙方还应当在产生违约赔偿金之日起15个工作日内支付完毕全部违约赔偿金并补足履约保证金。

(6) 甲方每次付款前，乙方应向甲方提供等额、合法的增值税发票。因乙方开具的发票类型、金额等不符合合同约定或法律规定导致甲方付款延迟的，甲方不承担违约责任。

4. 在合同履行期间，如遇国家政策调整等因素，导致所开具发票的税率与上述约定不一致，则合同总金额相应调整。

5. 由于乙方未足额缴纳应缴税款和开具发票不真实、不合格而引起的一切责任(包括商业责任和法律责任)和损失，由乙方全部承担。由此给甲方造成的所有损失，乙方承担相应的赔偿责任。

6. 如果乙方根据本合同产生对甲方的赔偿或支付违约金的责任，甲方有权在应付款项中予以扣除，若产生违约赔偿金之时甲方应付款项已经全部支付完毕的，乙方还应当在产生违约赔偿金之日起15个工作日内支付完毕全部违约赔偿金。

7. 乙方同意，因项目资金未落实到甲方而引起的甲方延迟付款的情形，甲方不承担逾期付款的违约责任。

五、项目验收

乙方根据甲方的书面运维需求完成运维服务后，应按照合同及附件约定的内容进行成果交付，乙方在交付前应按本合同的要求进行内部自检，自检通过后书面通知甲方，所交付的文件应当是电子版和纸质版文档。乙方在交付前【15】个工作日内以书面方式或电子邮件形式通知甲方，乙方将运维成果交付甲方后，甲方应在收到运维成果之日起【10】个工作日内组织验收。

1. 验收标准：本项目采用现场/远程验收方式验收，验收标准以符合招标（采购）文件、投标（应答）文件、合同相关附件所列明的服务和甲方的要求为准。乙方所提供的服务应符合本合同条款中所述的标准；如果没有列明适用标准，则应符合中华人民共和国国家标准或行业标准；如果中华人民共和国没有相关标准的，则采用货物来源国适用的官方标准。这些标准必须是有关机构发布的最新版本的标准。乙方应向甲方提供有关标准的中文文本。本项目以贵州省大数据局验收通过为本项目验收通过的最终标准。

2. 验收人员：由【甲乙双方人员】共同参与，甲方有权聘请第三方专业机构人员参与验收，并最终报贵州省大数据局验收。

3. 项目验收：运维期满后，经乙方内部自查通过，即可按照项目进度完成并配合项目验收等工作。同时，乙方须提供验收文档包括但不限于服务总结报告、问题处理记录（若出现问题则提供）、服务考核表等资料。

4. 甲方验收不合格，应出具书面的验收不合格通知。乙方根据甲方要求，应及时加以修改纠正，直至验收合格为止。

5. 所有验收节点必须由甲方确认后（如果根据贵州省大数据局要求，节点验收需要贵州省大数据局认可确认的，还需要贵州省大

数据局认可确认)方可视为验收通过。

六、甲方的权利和义务

1. 甲方应配合乙方进行本合同约定的相关工作。

2. 甲方收到乙方的付款申请,按照合同约定支付合同费用。

3. 甲方有权在乙方按照本合同约定决定终止本合同时,立即终止本合同。

4. 甲方有权随时向乙方了解项目进度,并要求乙方提供项目相关资料(包含:服务总结报告、巡检记录、问题处理记录(若出现问题则提供)、服务考核表等资料)。

5. 甲方有权按照本合同约定或有关法律法规规定,对本项目进行监督和检查,如乙方未按照本合同约定提供服务,或乙方提供的服务违反法律法规的强制性规定的,甲方有权要求乙方按照乙方的监督检查情况制定相应措施并对违反法律法规的行为加以整改。乙方不因行使该监督和检查权而承担任何责任,也不因此减轻或免除乙方根据本合同约定或相关法律法规规定应承担的任何义务或责任。

6. 甲方有权在乙方履行合同过程中出现损害公共利益、公共安全情形时终止本合同。

7. 甲方有权将乙方履行合同情况及不符合政府购买服务相关法律法规情况,向相关部门报告并纳入不良信用记录、年检(报)、评估、执法等监管体系中。

8. 甲方应及时向乙方提供与履行本合同相关的且乙方有权提供的必要文件、资料,包括但不限于完整且正确的系统源代码、运维

日志、系统设计文件、网络拓扑设计文件及系统安装部署手册等资料等系统相关资料。

9. 甲方应为乙方履行本合同过程中与相关政府部门、原运维服务团队及其他第三方的沟通、协调提供必要的协助。

10. 甲方应向乙方提供运维专用 VPN。

七、乙方的权利和义务

1. 乙方有权按照本合同约定向甲方收取本合同价款。

2. 乙方有权自甲方处获得与提供本合同项下服务相关的所有必须的文件、资料。

3. 乙方有权要求甲方协调、组织原运维服务团队在内的其他第三方为乙方履行本合同项下的服务提供必要协助。

4. 乙方应接受甲方的监督管理。

5. 乙方应建立安全管理制度和措施，按照《中华人民共和国网络安全法》等法律法规以及政务信息系统安全管理对应规定实施项目。

6. 乙方应建立健全服务应急处置机制，保障系统日常稳定运行。

7. 乙方应根据甲方需求编制项目实施方案，并在项目结束后提交技术总结。

八、合同生效、转包、暂停及终止

（一）合同生效

1. 本合同经双方法定代表人或授权代表签字（或盖章）并加盖

单位公章或合同专用章后生效。

2. 本合同有未尽或需修改、变更事宜，必须经双方共同协商，做出书面补充协议予以确定，补充协议与本合同具有同等的法律效力，补充协议与本合同不一致的，以补充协议为准。

3. 本合同于双方各自履行了合同的全部义务，包括本项目的质保期结束和甲方付清全部合同款后终止。

4. 对本合同条款和附件的任何变更、修改或增减，须经双方协商同意后签署书面文件，作为本合同的组成部分并具有同等法律效力。

5. 本合同的所有附件及该项目的招标（采购）文件、投标（响应）文件均为本合同不可分割的组成部分，与本合同正文具有同等效力。

（二）合同转包

1. 除甲方事先书面同意外，乙方不得转让、转包、分包、转委托其应履行的合同义务。

2. 如果乙方违反本合同约定将项目全部或部分转让、转委托、转包、分包，甲方有权单方解除合同，并有权要求按合同总价的

【20%】支付违约金，违约金不足以弥补甲方损失的，乙方应承担相应的赔偿责任。同时，丙方因此所获得的收益归甲乙双方所有。

（三）合同暂停

1. 甲方有合理理由的，可以书面通知乙方暂停合同的任何部分。乙方应即时暂停，但必须继续执行未暂停的部分，并在收到甲方书面恢复通知后，即时恢复。

2. 如并非由于乙方违约导致乙方不得不暂停履行合同或合同一

部分时，乙方应立即书面通知甲方，并给出充分合理的解释。乙方必须协助甲方消除影响，以使合同得以继续履行。

（四）合同终止

1. 当服务结束且合同双方完成合同规定的责任和义务，合同自动终止。

2. 若双方同意，合同可以在任何条件下终止。这种情况下，双方均无例外地免去彼此所有的合同责任和义务。

3. 甲方可以在任何时候可以以充足的理由终止本合同，但事先必须在正式终止前【30】天以书面形式通知乙方，并说明终止理由。

4. 如因不可抗力导致合同终止，双方均不对彼此承担赔偿责任。

5. 项目采购、实施过程中，乙方存在下列行为，甲方可单方面终止合同。

（1）乙方有腐败和欺诈行为。为此目的，定义下述条件：

① “腐败行为”是指建议给、给、接受或索要任何价值的东西，以影响甲方职工在与执行合同有关的任何事情上的行为。

② “欺诈行为”是指掩盖事实真相，以不正当的手段影响合同的执行，从而对甲方造成损害，而且包括与其它方面进行勾结，以图获得不公平的好处，进而剥夺甲方正当执行合同的好处。

（2）乙方有泄密行为，经查证属实。

（3）其他行为，严重影响甲方或最终用户工作，给甲方或最终用户造成损失。

6. 如果乙方破产或无清偿能力，甲方可在任何时候以书面形式

通知乙方，提出终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取的任何行动或补救措施的权利。

九、知识产权

乙方保证对所提供的技术资料、知识产权等具有合法产权或已取得合法授权，不存在侵犯他人合法权益的情形。否则由此产生的责任、损失和费用均由乙方承担。

十、保密条款

1. 本协议双方应遵守国家有关保密的法律法规和行业规定，并对其他方提供的资料(包括但不限于数据、文档、文件等)负有保密义务。未经任何一方书面许可，不得以任何形式将履行本协议获得的政府、公民个人等各种信息资料或涉及知识产权及商业秘密的资料信息进行与本协议无关的任何形式的利用。如发生以上情况，守约方有权按照本协议违约责任条款向违约方索赔并追究法律责任。

2. 本协议保密条款长期有效，无论本协议是否生效、被撤销、变更、解除或终止，双方仍应执行本协议保密条款。

十一、不可抗力

1. 因不可抗力或者其他意外事件，使得本协议的履行不可能、不必要或者无意义的，遭受不可抗力、意外事件的一方不承担责任。

2. 不可抗力、意外事件是指不能预见、不能克服并不能避免且

对一方或双方当事人造成重大影响的客观事件，包括但不限于自然灾害如洪水、地震、瘟疫流行等以及社会事件如战争、动乱、政府行为、电信主干线路中断、黑客、网路堵塞、电信部门技术调整和政府管制等。

十二、违约责任

1. 甲方在监督检查过程中发现乙方存在以下问题的，有权要求乙方进行限期整改，乙方应按要求及时整改：

（1）与本合同约定或者相关法律法规规定不符合的。

（2）甲方提出整改要求，对乙方拒绝整改、或者出现整改事项超过三次、或者就同一整改事项经整改超过三次仍不合格的，甲方有权单方解除合同，有权另行委托，并要求乙方承担另行委托的费用和其他依据本合同和相关法律法规规定应当承担的违约责任。

2. 因乙方原因出现运维服务中断的情况，乙方应在2日内解决中断情形，乙方无法解决的，自中断情形持续第3日起，甲方有权按合同总金额每日0.1%要求乙方向甲方支付违约金，乙方还应承担由此给甲乙双方造成的全部损失。但因甲方需求变更等非乙方原因造成的服务无法进行或按期完成的，乙方不因此承担逾期违约责任。

3. 因乙方原因导致甲方被网络安全相关主管部门通报，乙方应在3日内解决相关安全问题。每发生1次，甲方将按合同总金额5%的数额扣除合同尾款金额，若发生3次以上（含3次），甲方将扣除全部尾款，并追缴全部首付款，乙方应无偿退还并支付甲方损失。若自问题持续第4日起，乙方无法解决的，甲方有权按1%/日的数额要求乙方向甲方支付违约金；若因乙方原因导致甲方发生重大安全事

件，乙方应在5日内解决相关安全问题，甲方将一次性扣除全部合同尾款金额。若扣款金额超过尾款金额的，甲方有权依据乙方履约保证函向银行向银行进行申诉赔偿，或者向乙方继续追偿。

4. 甲方应严格按照合同约定期限支付合同约定费用，逾期一日的，应按照合同总金额的1%向乙方支付违约金，超过30日的，乙方有权解除合同，并要求甲方承担相应的违约责任。

5. 任何一方由于不可抗力原因导致合同不能履行时，应在不可抗力事件发生后2日内书面通知对方并提供充分合理的证明，以减轻可能给另一方造成的损失，在取得有关机构的不可抗力证明或谅解确认后，允许相应延期履行或修订合同，并可根据具体情况部分或全部免于承担违约责任。由于不可抗力导致合同不能履行的，任何一方均有权终止合同。

6. 发生其他违约情形，违约方应赔偿由此给守约方造成的一切损失及为维护合法权益而支出的一切费用，包括但不限于诉讼费、保全费、律师费等一切费用。

7. 甲、乙双方应遵循诚实信用原则，按照合同约定充分履行合同义务，保障合同顺利履行完毕。若因非可归责于双方的原因导致项目提前终止，双方应另行商定解决方案，防止国有资产投资风险及损失。

十三、争议的解决

本协议受中华人民共和国法律管辖，在执行本协议过程中如发生纠纷，各方应及时协商解决。协商不成时，任何一方均应向甲方所在地人民法院提起诉讼。

十四、通知与送达

1. 甲乙双方共同确定，与本协议相关通知、协议、文书的送达地址、联系人、联系方式、传真号码等信息以本协议签约处约定的信息为准；如一方地址、联系人、联系电话、传真号码有变更，应在变更后的 10 日内书面通知其他方。变更方按上述约定履行变更通知义务后，以其变更后的送达地址为有效送达地址，否则视为未变更，其之前确认的送达地址仍为有效送达地址，与本协议相关的文件、文书及司法文书邮寄送达 5 日后即视为送达。

2. 本协议关于送达地址、联系人、联系方式等信息的约定，亦适用于因本协议发生纠纷时相关文件和法律文书的送达，同时包括争议进入仲裁、民事诉讼程序后一审、二审、再审和执行程序及其他程序中相关文件的送达。

3. 与本协议相关的通知、协议、文件、文书的送达以书面信函形式或各方确认的传真、电子邮件或类似的通讯方式进行。采用信函形式的应使用挂号信或者具有良好信誉的特快专递送达。如使用传真、电子邮件或类似的通讯方式，通知日期即为通讯发出日期，如使用挂号信件或特快专递，通知日期即为邮件寄出日期并以邮戳为准。

十五、附则

1. 一方变更联系人的，应当及时书面通知其他方。未及时通知并影响本协议履行或造成损失的，应承担相应的责任。

2. 本协议的附件是本协议不可分割的一部分。

3. 本协议壹式伍份，甲方执贰份，乙方执三份，每份均具有同等法律效力。

(本页无正文，系“厅内系统安全产品租用项目运维服务合同”签字盖章页)

甲方(盖章)

单位名称: 贵州省自然资源技术信息中心

法定代表人或授权代表(签字):

经办人(签字):

日期: 2015.6.27



乙方(盖章)

单位名称: 贵州大数据产业集团有限公司

法定代表人或授权代表(签字):

经办人(签字):

日期: 2025年6月27日



合 公 司 承 辦 各 項 工 程 施 工 監 理 服 務 有 限 公 司

（ 公 司 章 程 ）

（ 公 司 章 程 ）



（ 公 司 章 程 ）



附件1、服务内容及要求

贵州省自然资源厅态势感知安全扩容容灾备份（共计：2334100元）							
序号	项目名称	服务内容	参数和配置	工程 量	单位	单价	总价
1	贵州省自然资源厅态势感知安全扩容（本地化部署）	存储节点扩容（本地化部署）	1、用来存储日志，实现分布式事件存储与全文索引，从而大幅提升事件处理的性能； 2、支持集群部署、软件部署 3、系统支持对无用日志的自动过滤，过滤条件可以按照所有范式化后的字段属性来定义，包括但不限于源 IP、目的 IP、源端口目的端口、事件名称、事件类型等，减少垃圾数据数量； 4、系统支持对无用信息的自动合并，支持设定合并的时间范围容（本地化部合并条件可以按照所有范式化后的字段属性来定义，包括但不限于源 IP、目的 IP、源端口、目的端口、事件名称、事件类型等，减少垃圾数据数量。 5、系统支持统计不同采集器和不同安全域下的设备个数并以饼图展示，统计展示采集器或安全域中事件量 Top10、范式化设备数比例等； 6、可以根据日志源断点时间进行配置，并生成告警。点击单个日志源设备查看该设备最近7天的事件趋势	2	套	100000	200000
2		采集器扩容（本地化部署）	1、增加采集器，本模块为软件，采集各类网络设备、安全设备主机服务器、各类应用系统的事件和日志，用于实现分布式安全事件采集；对资产的日志信息进行采集、范式化、分类、过滤和归并，实现分布式日志采集，并统一报送安全管理与态势感知平台，实现集中化安全事件管理。 2、支持多种工控协议的解析并范式化为工控协议日志，包括采集器扩容S7、DNP3、Modbus、IEC103、IEC104、DECRPC、EtherNet/IP（本地化部IEC61850-MMS、IEC61850-GOOSE等。 3、支持以 UDP 协议将流量日志以 vflow 的格式发，将HTTP，DNS等多种协议会话数据以syslog的格式转发，将接收到的被动*flow数据以 netflowv5 的格式转发。 4、支持对日志事件依据其源目的 IP 和端口等各类字段信息进行深入的日志事件追踪调查，支持无限次数的追踪调查； 5、支持手工对日志进行响应处置，如生成告警、加入观察列表生成威胁情报等； 6、支持对选中的事件源/目的 IP 地址进行全球地图定位，包括在线定位和离线定位 7、支持对选中的事件进行事件拓扑分析，并可可视化的展示一幅描述事件之间相互关系的事件拓扑图	2	套	36000	72000

3	分流器（本地化部署）	1、1U 机箱，24 个 FP+插槽（支持 10GE，兼容 GE），整机吞吐 240G，支持流量复制、流量汇聚、流量负载均衡输出等 2、支持接收交换镜像端口或分光器的1GE、10G、40G、100G 接口输出的克隆数据，对接收的数据进行复制、汇聚、过滤、分流、报文精确处理并从万兆/千兆端口输出给后端分析设备支持流量复制/汇聚/分流功能，支持一对多，多对一，多对多的分流器（本地流量复制汇聚分流化部署） 3、设备支持镜像配置功能，即可以把设备收到的流量数据通过隧道封装的方式传输至远端设备。 支持源/目的 IP 地址、目的端口的配置。 4、设备支持系统信息显示功能，支持设备温度、风扇转速、CPU使用率、内存使用率、系统时间、运行时间、软件版本信息等设备运行状态信息的展示	2	套	93400	186800
4	威胁分析响应系统（本地化部署）	1、国产化品牌+国产化操作系统。20机箱，4个电口、4个光口、2个万兆光口，整机吞吐 4G，最大并发连接数 700W，每秒新建连接数 5W。32G 内存，8T硬盘 2、支持常见 HTTP、FTP、TFTP、SMTP、TLS、SSH、IMAP、SMB、Dcerpc、DNS、IKEV2、NFS、Krb5、DHCP、SNMP、SIP、RFB、RDP 等应用层协议。 3、系统综合分析页面提供最近 24 小时/7 天/15 天内接入流量网络中发生的整体安全态势，包括对网络内风险资产进行统计分析对攻击、受害攻击进行聚合分析输出 TOP10，同时可对网络内告警威胁分析 响应事件趋势与告警风险级别绘制柱状图与并状态，并可对告警攻击系统（本地 TOP5 进行排序便于客户直观了解脆弱点；化部署） 4、系统具备攻击链分析模型，通过被攻击者视角展示主机遭受攻击状态迁移图和攻击阶段统计，分析内部资产被外部地址攻击详情，多维度分析攻击异常开始时间，使用手段； 5、基于网络全流量分析技术，对网络所有数据进行安全分析。通过对网络链路全流量采集、全数据据分析，对网络异常行为有敏锐的感知能力，具备多维度数据索引能力，能够对网络攻击进行定位与取证。 6、支持设备系统管理，可通过页面下发诊断对设备关键进程进行监测，同时可一键恢复关键进程，增强设备易用性与运维便捷度， 7、支持设备 CPU、内存、磁盘、运行时间展示，可以手动配置 CPU、内存和磁盘资源使用的预警范围，超过配置阈值，进行页面告警。	1	套	120000	120000
5	服务器存储扩容（本地化部署）	国产化品牌：24 核 CPU，128 内存，8T 硬盘。用于安装分布式存储软件及采集器软件；国产化操作系统	5	套	55000	275000

序号	项目名称	服务内容	参数和配置	工程量	单位	单价	总价
1	贵州省自然资源厅容灾备份系统(本地化部署)	容灾备份一体机	容灾备份一体机具备 GIS(地理信息系统)的空间数据备份管理功能,涵盖数据的存储、检索、分析和可视化。主要包括:空间数据的存储与管理(数据存储、元数据管理);空间数据的检索与查询(属性查询、空间查询、复杂查询);空间数据的分析(缓冲区分析、叠加分析、网络分析、插值分析);空间数据的编辑与处理(数据编辑、拓扑关系维护、数据转换);空间数据的可视化(地图制图、三维可视化、动态图表);空间数据共享与发布(在线地图服务、数据共享、API接口);数据质量与控制(数据校验、版本控制、数据安全)等。1台机架式国产服务器用于平台节点,配置要求如下: 1) 每节点配置海光芯片 C86 及以上 CPU,单节点 CPU 物理总核数 $\geq 2*32$核,每核主频 $\geq 2.4\text{GHz}$;配置 $\geq 1024\text{GB}$DDR4内存; 2) 存储:系统盘配置 ≥ 2个1.92TB NVMeSSD 磁盘;数据磁盘使用全 NVMeSSD,裸容量 $>100\text{T}$; 3) 网口 >4个万兆以太网端口; 4) 配置滑动机柜导轨;配置独立的远程管理控制端口,支持服务器的远程控制及管理 5) 三年原厂商的免费硬件技术支持与5*8 级别的售后保修服务	1	套	680000	680000
2		数据安全软件	1、支持实时接收数据库备份对象的事务日志进行持续备份 2、平台支持一套平台同时备份多个 ORACLE/MySQL/达梦数据库 3、平台需支持文件备份功能,基于存储池的空间可以创建nfs 的共享空间给到外部使用,支持数据库备份对象5分钟快速恢复(例如具体某张表),恢复过程不依赖于外部主机,支持指定任意时间点恢复功能。 5.平台需支持数据库备份对象的快照库功能。在容灾备份云平台上可启用主库的多个快照库,不依赖于外部主机,支持应用测试和预发布等应用场景。 6.支持基于IP 网络和数据库级别的远程复制容灾,在备份云平台上展示主库和容灾备份库的容灾拓扑图。 7.支持数据库备份对象的容灾切换功能。提供一键切换功能,能实现主库宕机后的快速切换和业务支撑。	1	套	218600	218600

3	数据库安全审计	1. 对数据库的访问进行全面、精准的审计；识别 SQL 注入攻击、账号滥用、运维的风险 2. 跟踪敏感数据访问行为，及时发现敏感数据泄漏； 3. 以安全事件为中心，以全面审计和精确审计为基础实时记录 网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警。 4. 利用 OracleADG 原生复制技术，实现生产和灾备端的数据实时同步备份。 5. 支持 Oracle/达梦等数据库	1	套	290000	290000
4	数据加密	1. 对备份数据进行加密存储，确保数据在备份和传输过程中的安全性。 2. 内置于破解的 PL/SQL 直接作用于数据库，加密部分字段 3. 依赖 Redo 以数据流的方式传输，并不直接从主库拷贝文件 4. 依赖 SMB、RDP 等协议漏洞，加密文件	1	套	150000	150000
5	云管平台	1. 统一的可视化管理平台，为数据库提供了全面、端到端的数据保护生命周期视图 2. 采用虚拟化架构，提高数据库密度，整合度更高，提高设备利用率。统一的可视化管理配置平台，为数据库提供了全面、端到端的数据保护生命周期视图。 3. 支持不同的数据库根据重要级别，分配不同的硬件资源，以保证重要的数据库拥有足够的资源。 4. 支持自定义创建开发测试环境，包括任务的创建、停用、启用、删除、更新等，可根据需求自定义测试环境创建时间	1	套	140000	140000
6	数据一致性检查	人工定期进行数据一致性检查，确保本地和异地备份数据的一致性。	2	次	850	1700

自然资源厅及其下属二级单位全量防护云安全产品（不包含不动产中心）（共计：2449547元）						
电信节点-公有域-互联网云安全产品						
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量 100M	1年	单价	数量（套/台）
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	100个资产 授权	1年	19718	15
3	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	10个最大并 发	1年	28560	1
4	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法 及建议	20个IP	1年	5394	1
5	数据库审计		10个数据库	1年	34000	1
6	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	100个授权	1年	32000	1
7	杀毒		100个授权	1年	34049	1
					50000	1
电信节点-公有域-政务外网云安全产品						
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量 200M	1年	单价	数量（套/台）
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	50个授权资 产	1年	30340	5
3	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	5个最大并 发	1年	21000	1
	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法	10个IP	1年	3463	1
					27536	1
					151700	
					21000	
					3463	
					27536	

		及建议										
4												
5	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	30个授权	1年	25265	1					25265	
6	数据库审计		10个数据库	1年	32000	1					32000	
7	杀毒		20个授权	1年	28000	1					28000	
电信节点-专有域云安全产品												
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量100M	1年	21909	9					197181	
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	100个授权资产	1年	28560	1					28560	
3	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	5个最大并发	1年	3463	1					3463	
4	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议	10个IP	1年	27536	1					27536	
5	数据库审计		10个数据库	1年	32000	1					32000	
6	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	100个授权	1年	34049	1					34049	
7	杀毒		100个授权	1年	50000	1					50000	
联通（新）节点-公有域-互联网云安全产品												
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量100M	1年	24648	14					345072	
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	100个授权资产	1年	28560	1					28560	
3	web应用防火墙		防护流量100M	1年	24648	1					24648	

4	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	10个最大并发	1年	5394	1	5394
5	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议	20个IP	1年	34000	1	34000
6	数据库审计		10个数据库	1年	32000	1	32000
7	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	100个授权	1年	34049	1	34049
8	网站卫士防篡改		授权10个防篡改	1年	49400	1	49400
9	杀毒		100个授权	1年	50000	1	50000
计算资源池-公有域-政务外网云安全产品							
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量200M	1年	37925	6	227550
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	50个授权资产	1年	21000	1	21000
3	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	10个最大并发	1年	5394	1	5394
4	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议	20个IP	1年	34000	1	34000
5	数据库审计		5个数据库	1年	22000	1	22000
6	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	30个授权	1年	25265	1	25265
7	网站卫士防篡改		授权10个防篡改	1年	49400	1	49400

8		杀毒	移动（新）节点-公有域-互联网云安全产品					30个授权	1年	31770	1	31770		
													数量（套/台）	总价
1	下一代防火墙	具备传统防火墙、访问控制、应用安全防护、网络入侵检测与防御功能	防护流量100M	1年	24648	4	98592							
2	堡垒机	对资产运维进行管控，详细记录多种运维协议，为违规、误操作等提供追查依据	50个授权资产	1年	21000	1	21000							
3	SSL/VPN	提供通用安全套件，确保传输数据的机密性及完整性。实现安全、快速接入	5个最大并发	1年	3463	2	6926							
4	漏洞扫描	通过对系统进行安全脆弱性深度检测，发现可被利用漏洞，并提供漏洞修复方法及建议	10个IP	1年	27536	1	27536							
5	数据库审计		3个数据库	1年	16800	1	16800							
6	日志审计	对每天所记录的信息进行审计和检查，采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	30个授权	1年	25265	1	25265							
7	网站卫士防篡改		授权10个防篡改	1年	49400	1	49400							
8	杀毒		50个授权	1年	43000	1	43000							

数据安全服务（共计：137855元）

1	贵州省自然资源厅-数据安全服务	包含数据分类分级、数据安全评估	1次	137855	1项	137855
---	-----------------	-----------------	----	--------	----	--------

总计：4921502元