16、商务标偏离表

说明：请投标人对应招标文件的“投标人须知前附表”、“用户需求书”中有关项目交货期、投标有效期、质保期、投标保证金等商务要求以及该项目技术与服务等内容的要求，如实、完整、准确的填写该表。投标文件有正、负偏离均应在下表中列明。若无偏离，请标明“完全响应”。

序号	招标文件条款	招标文件中商务要求	投标文件响应	偏离
1	采购总预算	本项目总采购预算：2504.11 万元整，其中 A 包预算：1181.21 万元；B 包预算 1322.90 万元（注：超出采购预算的报价视为无效投标）。	本项目总采购预算：2504.11 万元整，其中 A 包预算：1181.21 万元；B 包预算 1322.90 万元（注：超出采购预算的报价视为无效投标）。	完全响应
2	三、 项目工期	（二）B 包：合同签订后 12 个月。	（二）B 包：合同签订后 12 个月。	完全响应
3	2. B 包预算	B 包预算：1322.90 万元（注：超出采购预算的报价视为无效投标，如投标价低于采购预算金额的 80%，需现场提供成交合同（含合同内容、系统功能等并加盖公章）等佐证证明材料，中标后采购人有权要求投标人提供项目预算 10%的银行质保函，且有权不支付预付款和进度款，直至项目竣工验收后支付）。	B 包预算：1322.90 万元（注：超出采购预算的报价视为无效投标，如投标价低于采购预算金额的 80%，需现场提供成交合同（含合同内容、系统功能等并加盖公章）等佐证证明材料，中标后采购人有权要求投标人提供项目预算 10%的银行质保函，且有权不支付预付款和进度款，直至项目竣工验收后支付）。	完全响应
4	3.3.6.1 政务大数据安全运营监管服务周期要求	政务大数据安全运营监管服务周期为 1 年。大数据安全保障平台和云监管平台系统部署上线并完成项目初验后，经甲方确认后，正式进入服务期。	政务大数据安全运营监管服务周期为 1 年。大数据安全保障平台和云监管平台系统部署上线并完成项目初验后，经甲方确认后，正式进入服务期。	完全响应
5	3.3.6.2.2 工期要求	供应商应在签订合同后 15 个工作日内提交详细的《项目实施计划》，合同签订后 12 个月内完成项目建设。	我司在签订合同后 15 个工作日内提交详细的《项目实施计划》，合同签订后 12 个月内完成项目建设。	完全响应

海南省大数据安全体系建设项目-2021-9240-5-1-088-bb52f9066d2451...d55daaee—7.6.

6	3.3.6.6 知识产权要求	（1） 乙方为甲方开发的云监管平台和政务大数据安全保障平台权归甲方所有，乙方为实施项目而提供的资料及全部项目工作成果（包括项目计划、需求规格说明书、概要设计说明书、详细设计说明书、测试报告、安装部署手册、操作手册、培训方案、试运行报告、前台页面及软件源代码、项目验收文档等资料）的知识产权权利归甲方所有，乙方提供的具备知识产权的产品或采购具备知识产权的成熟产品（包括硬件产品和软件产品），知识产权仍归产品提供方所有；基于成熟产品进行二次开发的系统及成果的知识产权归甲方所有。 （2） 乙方保证对其销售的产品/服务拥有完全的所有权/处置权或已取得相关授权，不侵犯任何第三方的专利、商标、著作权和其他合法权利，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由乙方承担所有相关责任的同时不得耽误本项目进度。 （3） 乙方保证其提供的软件及服务不含有任何旨在破坏最终用户计算机信息系统和/或获取最终用户隐私信息的恶意代码。 （4）乙方应在项目完成时，将本项目所有文档汇集成册交付甲方。技术文档（光盘与纸质）及为本项目开发的软件系统（光盘形式，包括注释清晰明了的源代码）各两份。	（1） 我司为甲方开发的云监管平台和政务大数据安全保障平台权归甲方所有，我司为实施项目而提供的资料及全部项目工作成果（包括项目计划、需求规格说明书、概要设计说明书、详细设计说明书、测试报告、安装部署手册、操作手册、培训方案、试运行报告、前台页面及软件源代码、项目验收文档等资料）的知识产权权利归甲方所有，乙方提供的具备知识产权的产品或采购具备知识产权的成熟产品（包括硬件产品和软件产品），知识产权仍归产品提供方所有；基于成熟产品进行二次开发的系统及成果的知识产权归甲方所有。 （2） 我司保证对其销售的产品/服务拥有完全的所有权/处置权或已取得相关授权，不侵犯任何第三方的专利、商标、著作权和其他合法权利，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由乙方承担所有相关责任的同时不得耽误本项目进度。 （3） 我司保证其提供的软件及服务不含有任何旨在破坏最终用户计算机信息系统和/或获取最终用户隐私信息的恶意代码。 （4）我司在项目完成时，将本项目所有文档汇集成册交付甲方。技术文档（光盘与纸质）及为本项目开发的软件系统（光盘形式，包括注释清晰明了的源代码）各两份。	完全响应
7	4. 其他相关要求	（1）投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，	（1）我司根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的资质证书等进行核查，如发现提供虚假材	完全响应

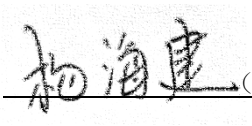
海南省大数据安全体系建设项目—202409[illegible]

		如发现提供虚假材料，按废标处理，代理机构将报政府采购主管部门严肃处理。 （2）投标技术文档需针对海南省大数据局管理局现状，编制包括但不限于项目需求分析、实施方案、技术方案、政务大数据运营监管服务方案、培训及售后方案、政务大数据安全制度方案、安全保密管理方案等内容。 （3）合同期内，提供免费升级服务，在正常条件下保证系统正常稳定运行的情况下进行更新升级服务。 （4）项目竣工验收后提供所有软件产品 2 年的免费维护。 （5）合同期内，提供免费优化服务，在正常条件下改进系统性能的各项建议，包括系统效率改进建议、软件、硬件配置规划和性能优化建议等。 （6）合同期内，提供咨询服务，系统软件应用和维护技术咨询服务。 （7）合同期内提供电话或现场技术服务。 （8）中标人对系统软件进行更新及升级时应不影响原有应用系统的正常运行和效率，不涉及到对原有应用系统重新设计。对系统软件的更新及升级时，未经招标人同意，不得改变针对本项目定制的功能。 （9）合同期内，中标人须保证所提供系统的正常运行和维护， 出现问题应及时予以维修或替换，所需费用由中标人负担。 （10）不满足上述合规性要求的产品不得投标。 （11）主体功能不允许分包。	料，按废标处理，代理机构将报政府采购主管部门严肃处理。 （2）投标技术文档需针对海南省大数据局管理局现状，编制包括但不限于项目需求分析、实施方案、技术方案、政务大数据运营监管服务方案、培训及售后方案、政务大数据安全制度方案、安全保密管理方案等内容。 （3）合同期内，提供免费升级服务，在正常条件下保证系统正常稳定运行的情况下进行更新升级服务。 （4）项目竣工验收后提供所有软件产品 2 年的免费维护。 （5）合同期内，提供免费优化服务，在正常条件下改进系统性能的各项建议，包括系统效率改进建议、软件、硬件配置规划和性能优化建议等。 （6）合同期内，提供咨询服务，系统软件应用和维护技术咨询服务。 （7）合同期内提供电话或现场技术服务。 （8）我司对系统软件进行更新及升级时应不影响原有应用系统的正常运行和效率，不涉及到对原有应用系统重新设计。对系统软件的更新及升级时，未经招标人同意，不得改变针对本项目定制的功能。 （9）合同期内，我司保证所提供系统的正常运行和维护， 出现问题应及时予以维修或替换，所需费用由中标人负担。 （10）不满足上述合规性要求的产品不得投标。 （11）我司主体功能不分包。	

海南省大数据安全体系建设项目—2024-09-24 00:5:10:38—b62fe6c6e0a43e16b045bfdcaee7168

		未列入本表的条款	全部接受	完全响应

投标单位全称（公章）：联通数字科技有限公司

法定代表人（或授权代理人）：  （签字或盖章）

注：

1、此表为样表，行数可自行添加，但格式不变。

2、根据投标文件响应情况，分别注明“正偏离”、“完全响应”、“负偏离”

3、对招标文件无偏离，视为对未列入本表的条款全部接受，注明“完全响应”。

海南省大数据安全体系建设项目—2021-09-24 00:35:10.884—bb32fe9676d2453f86bb0456d55daaee—7.6.1005.271

17 技术标偏离表

说明：请投标人对应招标文件的“投标人须知前附表”、“用户需求书”中有关项目交货期、投标有效期、质保期、投标保证金等商务要求以及该项目技术与服务等内容的要求，如实、完整、准确的填写该表。投标文件有正、负偏离均应在下表中列明。若无偏离，请标明“完全响应”。

我司对应招标文件的“投标人须知前附表”、“用户需求书”中有关项目交货期、投标有效期、质保期、投标保证金等商务要求以及该项目技术与服务等内容的要求的响应中有如下正偏离：

1. 政务大数据安全保障平台的主要功能除包括数据安全告警中心、数据安全能力中心、数据地图、数据脱敏、数据追踪溯源、数据安全审计、大数据平台组件安全检测功能外，还增加数据安全指标评估工具功能，该功能共包括评估概览、组织管理、安全评估、任务管理、权重管理、文档中心 6 个子功能.

2.政务大数据安全制度规范体系除满足招标文件制度清单的要求，还增加了三级工作流程、细则内容的编制。共增加三个三级工作流程，《业务系统上线前安全检测流程》、《安全漏洞管理细则》、《系统下线流程》。

3. 大数据安全运营监管服务驻场人员增加 1 名一线驻场人员，总共为 9 人。

序号	招标文件条款	招标文件中技术要求	投标文件响应	偏离
1	第三章（二）B 包采购需求 3.1 项目背景	为响应国家关于大数据的政策及落实相关部署要求，海 南省积极推进数字政府建设，加快海南省电子政务系统建设， 政务信息资源整合和利用，实现让“数据多跑路，群众少跑腿”，方便企业和老百姓办事，提高政府治理能力和服务水 平。随着大量政务数据归集整合与共享开放，数据应用的场景复杂多样，更多的业务应用从原先的单部门应用向跨部门 的融合业务转变，业务和数据的融合加大了数据安全防护的 难度。同时政务数据覆盖范围广泛、数据结构多样、关联关 系复杂，并会涉及	满足招标文件要求。详见投标技术方案“18.1 项目概述 18.1.1 项目背景	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.884—b32fe5676d24531e6f04f6d55d8ee—7.6.10.5.271

		大量用户个人信息数据，国家重要数据，集中后的数据安全问题更加突出。 近期国家关于数据安全相关的法律、文件持续密集出台。2020 年 4 月，我国发布了《关于构建更加完善的要素市场化配置体制机制的意见》明确将数据列为生产要素并强调要加 快数据要素市场的培育，提出加快数据要素市场培育，加强数据资源整合和安全保护。2020 年 5 月 28 日通过《中华人民共和国民法典》，针对隐私权和个人信息保护领域存在的问题，在现行法律规定基础上进一步强化。2021 年 6 月 10 日，通过《中华人民共和国数据安全法》并设立专门章节规 定政务数据安全与开放。 海南省大数据管理局承担全省大数据建设、管理和服务等职责，负责具体实施大数据开发应用监督工作，完善大数据安全保障体系，建立大数据安全评估体系等，同时应重点保障大数据建设的安全性。再此背景下，省大数据管理局启动海南省政务大数据安全保障体系建设项目。		
2	3.2 项目建设内容	1、建设海南省政务云监管平台，支撑监管部门对政务 云的整体情况的宏观把控，推动委办厅局将应用系统积极迁移上云，更有利于政务数据共享和大数据应用。 2、建设可信计算免疫平台，在公共服务平台的服务器 上部署可信计算免疫平台软件，以主动防御的方式防止了各种已知/未知病毒、木马的非法启动和注入，从源头上（云操作系统）阻止了各类恶意软件的发作和破坏，保障服务器的安全运行。 3、建设大数据安全保障平台。为数据安全运营与监管提供技术平台的支撑，利用加密、脱敏、溯源等安全技术， 针对数据全生命周期中风险，为政务数据资源提供保护手段， 为数据安全运营与监管提供技术平台的支撑，防范敏感数据 泄漏与滥用。	满足招标文件要求。详见投标技术方案 18.1.2 项目建设内容	完全响应

海南省大数据安全体系建设项目—2021-09-24 20:35:10.884+b22e9a97d245.3804b0456d55daaee—7.6.

		4.建立海南省政务安全制度规范体系。按照国家、行业 以及海南省关于网络和数据安全的要求，结合大数据管理局的实际情况，建立安全制度规范体系，涵盖网络、系统与数 据安全管理、防护和运营等方面，为日常的管理运营工作提供依据。安全制度的完善，是开展大数据安全运营监管工作的前提和基础，使政务大数据安全管控有据可依。 5.实施政务大数据安全运营监管服务。建立统一的大数据安全运营监管中心，以数据安全运营监管为核心，同时覆盖可能影响数据安全的系统和网络的安全运营的内容，通过大数据安全运营监管服务体系，降低大数据安全风险，保障 政务数据安全合规。		
3	3.3.1 云监管平台设计框架	本系统架构采用 SOA 软件架构，使用统一服务总线集中管控其他所有业务系统之间服务的交互。 云监管平台使用 ESB 企业服务总线提供服务管理、服务编排功能，并支持协议转换、数据转换、消息路由和服务编排。能够灵活支持消息队列 MQ、JMS、SOAP、RESTFUL、JDBC、HTTP、TCP 等常用协议，使得对云服务商不同类型数据的接口的适配更加方便。服务编排功能，支持云监管相关业务流程灵活编排，满足目前监管需求和后期功能扩展需要。	满足招标文件要求。详见投标技术方案 18.3.2.1.1 云监管平台总体设计。	完全响应
4	3.3.1.2 云监管平台基础版本功能清单	资源监管子系统： 1. 基于网络提供对跨机房多云环境的网络设备、安全设备、存储设备、服务器、操作系统、数据库、中间件等基础监控功能； 告警策略编辑、多节点多租户权限管理功能，结合海南省实际业务情况进行定制开发。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。	满足招标文件要求。详见投标技术方案 18.3.2.1.2 云监管平台基础版本技术功能。 18.10 重要指标（▲指标）应答	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:35:10.884—bb82fe9760245 3f80b0456d55daaee—7.6.

		业务监管子系统： 1. 监控云内运行的各个业务系统的资源分配、资源使用、逻辑拓扑和告警信息情况，再结合其他主动检测手段，获取各个业务系统的运行状态，并做统一的分析和展示。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。 安全监管子系统： 1. 收集安全事件信息，各云服务商 SOC 平台的运行功能，提供对所搜集信息的查询、展示，增强对云平台安全防护能力，确保云平台业务的安全、可靠运行。结合海南省实际业务情况进行定制开发，通过与各类云平台的标准 API 接口对接，建立统一的政务云安全展现。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。 运营管理子系统 1. 包含统一入口，实现统一管理、运维、监控、安全、计费、展示等功能。政务云运维及管理人员、厅局委办用户、领导决策人员均通过门户登录系统，获取各自角色特有的展示界面， 获取所有与其工作职责相关的最新信息如系统性能、待办事宜、作业计划、资源情况、计费情况等，并可以通过该页面办理与该用户相关的工作事宜。结合海南省服务目录管理、自服务台、业务流程定制、资源交付核对、费用分析、流量节点调整、租户账单定制、云服务商账单等需求在软件开发模块进行定制开发。 3. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服		

海南省大数据安全体系建设项目—2021-09-24 10:32:10.884—b82fe9676d215388b0456d55daaee—7.6.1005.271

		务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。 系统运维子系统 1. 面向管理维护人员，将服务、资源的各项管理功能构成一个统一的工作台，来实现管理维护人员的配置、监控、统计等功能需要。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。 报表管理子系统 1. 以多维度分析、可视化仪表盘为核心，通过丰富的 API 灵活的实现报表创建、加载，满足平台中各种报表的开发需要。 2. ▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。		
5	3.3.1.3 云监管平台软件个性化开发清单	包括资源监管子系统、业务监管子系统、安全监管子系统、运营管理子系统、监管大屏子系统、监管大屏子系统、资源监控信息对接、信管二期平台对接、OA 平台对接、云监管 Portal 定制开发、云监管平台密码应用开发共 11 个子系统，41 个模块。	满足招标文件要求。详见投标技术方案 18.3.2.1.1.5 个性化开发清单、18.3.2.1.3 资源监管子系统设计、18.3.2.1.4 业务监管子系统设计、18.3.2.1.5 安全监管子系统设计、18.3.2.1.6 运营管理子系统设计、	完全响应

海南省大数据安全体系建设项目-2021-09-24 00:35:10.884-bb32fe9376d2f5380b0456d55daaee—7.6.
1005.271

			18.3.2.1.7 系统运维子系统设计、18.3.2.1.8 报表管理子系统设计、18.3.2.1.9 监管大屏子系统设计、18.3.2.1.10 接口对接设计、18.3.2.1.11 云监管 Portal 定制开发	
6	3.3.1.4 资源监管子系统设计	资源监管子系统的主要功能包括：资源配置情况监管、资源监控、拓扑管理、监控报警分析、告警策略管理、监控指标管理、多节点多租户权限管理、统计分析报表等。	满足招标文件要求。详见投标技术方案 18.3.2.1.3 资源监管子系统设计、18.3.2.1.3.2 功能框架	完全响应
7	3.3.1.4.1 资源配置情况监管	通过多个云平台的接口对接，最终实现统一监控。 云资源运行情况属于动态信息，在云平台运行的时候实时变化，系统通过与云平台的接口将数据获取到，并将相关数据展现到 Dashboard 上，Dashboard 上的数据包括并不局限与以下数据： 资源配额：支持查看 vCpu 已用个数、已用内存、已用存储的信息。 资源详情：支持公网 ip 池个数、vpc 个数、虚拟机个数、网络个数的信息。 TOP5 排名：包括 cpu 使用 TOP5、内存使用率 TOP5、磁盘使用率 TOP5 的排名。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.3 资源配置情况监管	完全响应

海南省大数据安全体系建设项目—2021-09-24 20:35:10.884—6332fe0676d2453f864b9a3cd5daae—7.6.1005.271

		支持各种监控器，包括：安全设备、网络设备、硬件、存储、操作系统、数据库、中间件、应用等。 通过云平台接口对接，实现管理云平台虚机列表，并管理宿主机及虚拟机的逻辑关系。如：宿主机上承载哪些虚机，虚机的资源使用情况。 实现对于宿主机的实时监控，通过接口对接实现获取每个物理机上所有虚拟机的 vCPU 数量、虚拟机数量、该物理机的 CPU 总核数和预留内存大小、并做 CPU 复用比的计算及监控，并实现单台物理机上虚拟机数量、物理 CPU 复用比和剩余内存达到一定值后可以产生告警（CPU 复用比=某台物理机上所有虚拟机 vCPU 总数/该物理机 CPU 总数）。 实现对于底层存储的监控，通过云平台的对接，展示存储的使用情况，以及磁盘、存储单元、数据存储以及虚拟机之间的逻辑关系。		
8	3.3.1.4.2 资源监控	(1)各云监控节点管理 基于网络，从各云接口直接抓取监控数据来实现资源进行监控数据的采集与管理，对接态势感知平台，获取态势平台已有数据进行呈现。 (2)监控项管理 实时监控云平台内设备、虚机、数据库、应用中间件等的运行状况，当出现异常时，及时产生告警信息，并可自动触发工单系统督促相关责任人进行快速处理。支持 SNMP、Syslog、日志文件、ODBC/JDBC 等信息收集方式，并可自定义信息收集条件。 (3)网络安全设备监控 通过 SNMP、syslog 等协议实现对网络安全设备的管理，全面支持各种不同厂商、不同型号的网络与安全设备，提供各类设备的基本信息、CPU /MEM 负载状况，设	满足招标文件要求。详见投标技术方案 18.3.2.1.3.4 资源监控	完全响应

海南省大数据安全体系建设项目—2021-09-14 20:35:10.884—b82e2e9e976d2f53384b0456d55daaee—7.6.

		备可用状态、连续运行时间、响应延时、端口速率、ICMP 连通性等设备属性与监测信息，亦可自定义监测内容。实时监控网络安全设备的运行状况，当设备出现异常时，及时产生告警，通过触发工单系统督促相关责任人进行快速处理 (4)存储设备监控 通过 SMI-S、SNMP 协议实现对不同厂商存储的监控，包括运行状态和性能数据，具体包括存储的型号、设置、容量、磁盘组个数、使用率、磁盘大小、空闲磁盘大小、磁盘 IO 利用率、存储阵列状态、硬盘及磁带库状态、磁盘适配卡状态，磁盘通道状态、主机通道卡状态、光纤交换机运行状态、光纤交换机的端口状态等信息。系统实时监控存储设备的运行状况，当设备出现异常时，及时产生告警，通过触发工单系统督促相关责任人进行快速处理。 (5)操作系统监控 通过 SNMP、SSH、Telnet 等方式实现对操作系统信息的采集，包括 CPU 使用情况、内存的使用情况、磁盘空间使用情况、网络连接使用情况、进程使用情况等。系统实时监控操作系统的运行状况，当系统出现异常时，及时产生告警，支持触发工单系统督促相关责任人进行快速处理。 (5)数据库系统监控 通过 JDBC 方式实现对数据库的监控。数据库监控的指标包括数据库进程启动情况、日常运行日志、表空间的使用情况、数据库 Session 情况、数据库系统设计的文件存储空间、系统资源的使用率、配置情况、数据库当前的各种锁资源情况、监控数据库进程的状态、进程所占内存空间等。当数据库系统出现异常时，及时产生告警，支持触发工单系统督促相关责任人进行快速处理。 (6)中间件系统监控		

海南省大数据安全体系建设项目—2021-09-24 00:35:16—844-bb32e...—7.6.

		通过 JMX、SNMP 实现对中间件的监控，支持的中间件监控指标包括配置信息、连接池、线程队列、负载监测、通道情况监测等多类监测组，分析与监测中间件的各项运行状态参数。当业务系统出现异常时，及时产生告警，支持触发工单系统督促相关责任人进行快速处理。 (7)虚拟化平台监控 对虚拟化平台的监测主要以虚拟机为主。主要监测虚拟机常见的性能指标如 CPU、内存、磁盘。虚拟机监控详细指标包括： 基本信息采集：虚拟机的操作系统类型、虚拟机的总体状态、虚拟机的电源状态、虚拟机的配置文件路径、虚拟机名称、主机的基本信息或状态等。 虚拟机 CP 监测：虚拟机可使用的 CPU 数量、虚拟机的 CPU 频率、虚拟机的 CPU 使用率。 虚拟机内存监测：虚拟机的内存使用率、虚拟机可已使用的内存量。 虚拟机磁盘监测：存储置备大小、已分配使用率、未共享大小、已分配大小、虚拟机名称。 (8)负载均衡监控 以列表的方式展示政务云中所有的负载均衡信息。展示所属的云平台、云资源池、归属单位、协议类型、负载均衡式、成员数等信息。 (9)虚拟防火墙监控 以列表的方式展示政务云中所有的虚拟防火墙信息。同时提供防火墙的基本信息、告警事件等信息。		
9	3.3.1.4.3 拓扑管理	提供了网络拓扑管理功能，管理员可以从拓扑图上直观地了解当前网络的运行状况，从而判断是否存在网络隐患。拓扑管理功能包括：生成网络拓扑结构、网络拓扑监控、链路健康度监控、网络连接状况监控、设备运行健康度监控。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.5 拓扑管理	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.854 b822fe5a76d2453f854b0456d55daaee—7.6.
1905.271

10	3.3.1.4.4 监控报警分析	IT 基础设施是支撑信息系统运转的基础，为此 IT 综合监控管理系统专门设计了一个功能模块来实时监控 IT 基础设施的网络连接状况和关键运行指标。针对关键运行指标设置了符合业务特点的阈值，一旦出现阈值偏差，立即发出性能告警；针对 IT 基础设施的网络连接实时探测，针对关键进程进行实时监测，针对重要文件实时检测，一旦出现异常，立即发出故障告警。通过平台的报警分析功能，可以看到平台针对收集上来的监控指标项，经过实时归并、分析后的结果。包括：名称、类型、等级、IP 地址、IP 对应的责任单位、发生时间等。系统针对所有的 IP 地址和资产管理中的责任单位自动进行关联，在监控报警分析中实现将 IP 地址定位到责任单位，从而为后续的以责任单位进行宏观统计与分析提供了依据。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.6 监控报警分析	完全响应
11	3.3.1.4.5 告警策略管理	灵活设置告警策略，通过告警策略管理可以及时有效的发现异常监控指标。对支撑系统服务的所有网络设备和安全设备的关键运行指标进行实时监控，一旦超出所设置的阈值，及时进行告警。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.7 告警策略管理	完全响应
12	3.3.1.4.6 监控指标管理	与各云服务商的云管平台同步，将云平台上的宿主机和虚拟机信息同步到云监控平台，并形成监控目标。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.8 监控指标管理	完全响应
13	3.3.1.4.7 多节点多租户权限管理	通过租户创建的方式，对每个租户对安全、数据和系统做到了真正的隔离，每个租户以 SaaS 模式，独享系统。每个租户有多种用户角色。租户管理员可以管理自己的用户，包括组织结构，权限及策略管理等。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.9 多节点多租户权限管理	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.854—bb32fe5e76d125538b04b0456455daee—7.6.

14	3.3.1.4.8 统计分析报表	是日常工作必不可少的统计工具。系统提供了多类报表统计功能，方便管理人员查询和统计当前业务的安全状态，或者以前某个时期业务系统的安全状态。 通过配置数据源，对报表实现自定义布局（数据源、数据组件、位置、大小等），形成符合用户需求的报表。该报表可以定期生成，也可以立即生成。	满足招标文件要求。详见投标技术方案 18.3.2.1.3.10 统计分析报表	完全响应
15	3.3.1.5 业务监管子系统设计 3.3.1.5.1 系统概述	业务监管子系统通过于资源监管、系统运维等子系统对接获取到政务云内运行的各个业务系统的资源分配、资源使用、逻辑拓扑和告警信息情况，再结合其他主动检测手段，获取各个业务系统的运行状态，并做统一的分析和展示。主要包括业务系统的： (1)业务功能 业务监管功能实现对云上应用系统的运行情况的综合监控，实现对应用系统的可用性、安全性、繁忙度的监控，并以多层逻辑视图对业务系统进行透视管理，展示“租户-业务-资源”的依托关系，通过影响传递，发现资源故障对租户和业务造成的影响和威胁，帮助用户全面整体了解业务系统运行情况。 (2)业务流程 通过对应用系统的服务作周期性探测，监控业务系统响应时间和可用率，评估业务系统的可用性。 通过对应用系统占用的虚拟机的性能监控、业务资源使用量等数据的分析，评估业务系统的繁忙度。 通过对业务系统开通的安全服务的监测数据，分析业务系统的安全问题，评估业务系统的安全性。 (3)业务处理量 业务可用性和繁忙度的探测是周期性任务，用户可配探测的周期，系统自动探测应用的可用性和繁忙度。	满足招标文件要求。详见投标技术方案 18.3.2.1.4 业务监管子系统设计 - 18.3.2.1.4.1 系统概述	完全响应

海南省大数据安全体系建设项目—2021-09-24 20:35:10.851—bb22e9676d2f53804b0456d55daaee—7.6.

16	3.3.1.5.2 功能设计	业务监管子系统的主要功能包括：业务概览、业务可视化、业务可用性、资源使用分析、业务运行状态等。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.2 功能框架	完全响应
17	3.3.1.5.2.1 业务概览	通过业务概览展示云上业务系统运行状态，帮助政务云监管单位全面整体了解云上业务系统运行的状态情况。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.3 业务概览	完全响应
18	3.3.1.5.2.2 业务可视化	云监管平台以多层逻辑视图对业务系统进行透视管理，展示“租户-业务-资源”的依托关系，通过影响传递，发现资源故障对租户和业务造成的影响和威胁	满足招标文件要求。详见投标技术方案 18.3.1.5.2.2 业务可视化	完全响应
19	3.3.1.5.2.3 业务可用性	通过 http/https、ping、DNS、FTP、TCP、UDP、SMTP、POP3 等网络协议检查业务系统服务的可用性。 (1)业务可用率监管：统计业务系统可用率趋势，业务系统故障原因分析、故障时长统计。 (2)业务响应时间监控：响应时间分类统计、各时间段响应时间统计、响应时间分布范围统计。 (3)可用性事件展示：展示平台中业务系统可用性相关的事件。 支持对网站业务的可用性监管，包括 DNS 可用性、端口可用性、服务可用性；支持对网站业务性能监测，包括响应时间、加载时间等，及时发现异常；支持网站业务异常情况的及时告警功能。 租户管理员可对云上的业务系统开启可用性监管，只需要输入业务系统的 URL、监控频率等配置信息即可。作为监管用户，能看到全网所有业务系统的可用性监控信息。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.4 业务可视化	完全响应

海南省大数据安全体系建设项目-2021-09-24 09:35:10.88-9b52fe96f6d2451f6a0450d5dae7.6.

20	3.3.1.5.2.3 业务可用性	通过 http/https、ping、DNS、FTP、TCP、UDP、SMTP、POP3 等网络协议检查业务系统服务的可用性。 (1)业务可用率监管：统计业务系统可用率趋势，业务系统故障原因分析、故障时长统计。 (2)业务响应时间监控：响应时间分类统计、各时间段响应时间统计、响应时间分布范围统计。 (3)可用性事件展示：展示平台中业务系统可用性相关的事件。 支持对网站业务的可用性监管，包括 DNS 可用性、端口可用性、服务可用性；支持对网站业务性能监测，包括响应时间、加载时间等，及时发现异常；支持网站业务异常情况的及时告警功能。 租户管理员可对云上的业务系统开启可用性监管，只需要输入业务系统的 URL、监控频率等配置信息即可。作为监管用户，能看到全网所有业务系统的可用性监控信息。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.5 业务可用性	完全响应
21	3.3.1.5.2.4 资源使用分析	支持对业务系统所关联的资源分析，统计业务系统占用的云主机，每个云主机的现有规格、云主机的使用率，对资源进行长期（周报、月报）监控后，分析云主机 CPU、内存、存储使用率等配置是否合理，对每个业务系统是的资源使用情况评估后给出建议的合理配置。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.6 资源使用分析	完全响应
22	3.3.1.5.2.5 业务运行状态	帮助政务云监管人员及租户管理人员从业务系统的运行状态，评估业务系统的健康状态。	满足招标文件要求。详见投标技术方案 18.3.2.1.4.7 业务运行状态	完全响应
23	3.3.1.6 安全监管子系统设计	通过与各云服务商 SOC 平台及管理单位在建的态势感知平台对接，并真正打通各个政务云平台的安全状态信息，建立统一的	满足招标文件要求。详见投标技术方案	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:35:10.884—b32e9376d2f5f58dbb4ad55daaee—7.6.120.271

		政务云安全门户，全方位监控云平台业务系统的安全情况。	18.3.2.1.5.1 系统概述	
24	3.3.1.6.1.1 安全概览	通过与态势感知平台及各云服务商的 SOC 平台对接，实现对政务云的整体安全情况进行统一展示，如态势平台已有数据，可直接对接，以可视化方式展示系统安全状况，定制化开发安全状态可视化图表。	满足招标文件要求。详见投标技术方案 18.3.2.1.5.3 安全概览	完全响应
25	3.3.1.6.1.2 安全事件统一监控。	汇聚云服务商和态势感知平台的相关安全日志、操作日志、运行情况等信息，实现对安全事件进行统一监控与可化展现的功能	满足招标文件要求。详见投标技术方案 18.3.2.1.5.4 安全事件统一监控	完全响应
26	3.3.1.6.1.3 漏洞扫描	通过对接各个云服务商的漏洞扫描相关系统，令其对各自区域内暴露在网络上的主机进行漏洞扫描，可发现主机操作系统服务漏洞和应用程序服务漏洞，不需要用户提供主机账号信息，没有潜在的账号泄露风险。 监管人员可创建下发漏扫任务，指定虚拟机名称或 IP 段，对云主机或服务器进行漏洞扫描。 厅局委办等使用单位可申请对自己应用系统所使用的云主机进行漏洞扫描，在经过管理单位审核后下发执行。 漏洞扫描任务可周期性执行，扫描结果生成报告，可导出文件。	满足招标文件要求。详见投标技术方案 18.3.2.1.5.5 漏洞扫描	完全响应
27	3.3.1.6.1.4 漏洞管理	通过对接各个云服务商的漏洞扫描系统，获取最新隐患详情可导出存在隐患的网站信息及威胁列表，查询隐患详情，包括所属单位、网站名称、域名、区域、扫描时间、隐患个数、分级分类、隐患列表（包含隐患类型、等级、出现次数发现厂商）等；支持对存在隐患的网站发布提醒或通	满足招标文件要求。详见投标技术方案 18.3.2.1.5.6 漏洞管理	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:25:10:884—bb22b9676d2453e80b45ad55daae—7.6.
1105.21

		知限期整改和上传整改通知书附件；支持隐患录入和查看、导出网站累计隐患列表及列表报告下载。		
28	3.3.1.7 运营管理子系统设计 3.3.1.7.1 系统概述	本期所建设云监管平台的统一运营门户设在运营管理子系统，通过统一入口实现统一管理、运维、监控、安全、展示等功能。政务云运维及管理人员、厅局委办用户、领导决策人员均通过门户登录系统，获取各自角色特有的展示界面，获取所有与其工作职责相关的最新信息如系统性能、待办事宜、作业计划、资源情况、计费情况等，并可以通过该页面办理与该用户相关的工作事宜。	满足招标文件要求。详见投标技术方案18.3.2.1.6.1 系统概述	完全响应
29	3.3.1.7.2 功能设计	运营管理子系统的主要功能包括：服务目录、运营管理基础模块、业务迁移、业务开通、业务变更、业务退出、资源订单、账单管理、用户账单、服务商账单和资源清单等。	满足招标文件要求。详见投标技术方案18.3.2.1.6.2 功能框架	完全响应
30	3.3.1.7.3 服务目录	服务目录管理通过建立基础设施资源、平台资源和应用资源的逻辑视图，形成云计算及服务目录，供服务访问者与管理者查询，管理员可以添加服务，添加时需要填写服务名称、类型、计量单位，每月价格等信息。只有发布后的服务才能申请开通。	满足招标文件要求。详见投标技术方案18.3.2.1.6.3 服务目录	完全响应
31	3.3.1.7.4 运营管理基础模块	(1)自服务台 服务台的主要目标是协调客户（用户）和 IT 部门之间的联系，为 IT 服务运作提供支持，从而提高客户的满意度。它通过提供一个集中服务点，促进了组织业务流程与服务管理基础架构的集成。服务台是当用户在登录后进入的默认界面，可以认为是云使用单位登陆后看到的主界面。 在这里将显示资源申报过程中，需要处理和掌握的信息，包括已经申报的资源列	满足招标文件要求。详见投标技术方案18.3.2.1.6.4 运营管理基础模块	完全响应

海南省大数据安全体系建设项目—2021-09-4 10:35:10:884—b62e2e9e97d2453f8d4b0456455daee—7.6.

		表、正在申请资源的状态、需要处理的通知预警、用户画像等信息，通过简单的点击操作即可进入到相应的处理页面，通过自服务的方式完成对云资源的请和管理操作。 (2)基础中心 基础中心是系统提供的一组公用功能，包括系统用户管理、角色管理、权限管理、查询统计、知识库管理、云服务商管理、服务目录查询等功能。 （3）用户管理 对用户及其部门、岗位等信息进行添加、修改、删除、启用、禁用、审核等管理，并为用户分配相应的角色和权限。 （4）角色管理 针对系统业务流程，设定不同的用户角色，并为不同的用户角色分配相应的资源及功能权限。 （5）权限管理 按照用户所在的组织进行权限划分，每个用户只能查看自己所在组织下的功能菜单。 （6）查询统计 对用户数量进行统计，对内部用户的工作情况进行查询和统计。 （6）知识库管理 知识分类：在使用前和使用过程中，由管理员按照已梳理好的知识分类进行初始化。 知识入库：提供手工、导入方式，提供丰富的编辑环境，可以嵌入图片等多媒体元素，同时支持附件上传；未完成的知识可以保存为草稿。 知识检索：系统提供强大的知识库检索功能，支持主题检索、关键字检索、全文模糊等检索方式。 审核发布：知识创建人编写好知识草稿后，会提交知识审核；具备知识管理权限		

海南省大数据安全体系建设项目—2021-09-24 00:32:10.814—bb32fe9876d2453f864b0456d55daaee—7.6.1905.271

		的人员可对知识提交审核的知识草稿的内容进行审核；审核通过，该项知识将发布到正式知识库，审核失败，该项知识将退回给知识创建人重新修改，并再次进入审核流程。 云服务商管理：供应商管理是对供应商及其提供的服务进行管理的一系列活动，以确保 IT 服务提供商对最终用户提供的 IT 服务的实现，主要是指提供云计算、存储、网络及相关配套资源和服务。 云服务商管理内容包括但不限于以下内容： 基本信息：提供全面的云服务商资料信息，包括公司介绍、营业执照、地址、电话、紧急联系人等，可进行手工录入或批量导入。 资质管理：实现对云服务商资质的统一管理，如可信云认证等。 服务目录查询：服务目录查询功能与资源申报方案中接口的对接，服务目录包括服务分类、服务子类、服务项、计价单位、报价（元/月）、服务描述、备注等。 计费管理：云计算计费是使用一组预定义的计费策略从资源使用数据生成账单的过程。云计算中，直接的开销就是服务器、网络、存储等资源性设备，间接的开销就如供电系统、冷却系统和营业执照等。 制定收费服务目录类型，比如计算资源、存储资源、网络资源等等几大类收费项目的管理。 创建计费项目：项目/账户可使用发布后的计费价目进行计费；同一计费价目支持绑定多个项目/账户，无需重复创建。 查看计费项目：在计费价目界面，选择某一计费价目，展开其详情页，可查看当前创建的计费价目状态和信息。 修改计费项目：云平台支持创建多份计费价目。项目/账户可使用发布后的计费价目		

海南省大数据安全体系建设项目—2021-09-24 00:35:10 8f4-bb22fe9876d2f5f5f8d4b0456d55daaee—7.6.

		进行计费；同一计费价目支持绑定多个项目/账户，无需重复创建。 删除计费项目：在计费价目界面，点击删除按钮，可删除未被项目/账户绑定的计费价目，支持批量操作。 正在被项目/账户使用的计费价目无法删除，请为所有相关项目/账户更换计费价目再执行此操作。 绑定计费项目：在计费价目详情页的项目/账户子页面，可为本条计费价目绑定项目/账户，绑定计费价目后，所选 账户将使用此价目进行计费。项目/账户必须绑定一条计费价目；一条计费价目支持绑定到多个项目/账户。 更改计费项目：在计费价目详情页的项目/账户子页面，可将绑定本条计费价目的项目/账户更换到其他计费价目，更换计费价目后，所选账户将使用更换后的价目进行计费。 计费规则：对云上的用户进行计费规则的定义，可以按照不同的收费标准登记不同的计费规则，为了达到灵活调整 计费的目的，可以登记多种计费规则，可针对每种类别设定具体的服务内容。 资费配置：按实际使用时长，例如按分钟计费、按小时计费；按周期计费：包年、包季、包月、包周、包天。 个性化配置：有了基础的计费模板和资费策略，各云计算服务商可根据自身优势提供具有定制化特色的套餐服务，将以上的基础元素进行整合，以迎合用户使用场景的复杂多变需求。 流程配置：实现业务流程的定制化能力，提供灵活、可扩展的流程管理支持。强大的自定义功能可以让企业很方便的定制与业务规则一致工作流程，流程将按照业务规则进行流转。		

海南省大数据安全体系建设项目—2021-09-24 00:33:10 844—bb32e3e9670d253f80b0456d55daaee—7.6.

		用户中心：用户中心实现客户资料的集中管理，包含客户信息管理、角色管理、权限管理、部门管理员管理、用户组、权限管理、资源配额内容。 用户信息管理：提供用户创建、删除、查看、修改等功能，主要包括名称、联系人、地址、统一社会信用代码、法定代表人、营业执照等信息。 角色管理：提供角色创建、修改、删除及查看等功能。 权限管理：可以按照用户所在的组织进行权限划分，每个用户只能查看自己所在组织下的功能菜单。 客户审核：只有经过审核的用户才有权下单，审核对于包括对数据真实性校验。 部门管理员管理：作为资源拥有的基本单位，对作用域的资源可以进行创建、删除、等操作。账户分为部门管理员账户和普通账户。 用户组：可以通过创建用户组对一组用户进行批量的权限控制。 权限管理：主要提供了用户对系统资源的访问控制，可实现以细粒度对资源归属及权限控制的划分。 资源配额：资源配额是部门管理员对普通账户的资源总量进行控制的衡量标准。 工单管理：实现工单的统一查询、通过派单的方式进行任务的执行和部署并实行最后的交付、派单实现与统一运维管理平台对接。 服务延期：对帐号的有效期进行延期，主要适用于租户服务到期后服务的延期操作。		
32	3.3.1.7.5 业务迁移审批流程审计	依据使用单位实际部署的 OA 系统不同，分为两种情况： 1、使用单位实际部署的 OA 系统与管理单位同为新境界 OA 系统的：	满足招标文件要求。详见投标技术方案 18.3.2.1.6.5	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:33:10 84 bb32e9376d25538864b0456d55daaee—7.6.

		申请：云资源的申请在使用单位内部 OA 走完流程后，由 OA 将申请及相关审核材料电子版推送到云监管平台，使用单位在资源申请前需要在云监管平台上完成入住。 审核：管理单位 OA 系统从云监管平台收到云资源申请及相关材料的电子版后，由管理单位审核，通过管理单位审核的，由 OA 系统将审核通过的信息发送的到云监管平台；没有通过审核的，把 OA 系统返回的不通过的原因反馈给使用单位； 备案：云监管平台在收到 OA 系统的审核通过通知及资源配置要求后，按照审核后的云资源下发工单到云服务商，由云服务商完成资源配置，并在云监管系统中完成备案； 上线：由使用单位及业务系统开发商在云服务商的配合下，完成系统部署和上线； 变更：使用单位为云上系统资源变更通过 OA 系统报管理单位审核，通过后管理单位 OA 把审核后云资源调整要求发送到云监管平台，云监管平台下发工单到云服务商，由云服务商完成资源变更配置； 退出：使用单位为云上系统退出政务云申请通过 OA 系统报管理单位审核，通过后，管理单位 OA 把审核后云资源退出结果发送到云监管平台和使用单位，云监管平台下发工单到云服务商，由使用单位及业务系统开发商完成系统下线、数据回收后，云服务商回收云资源。 2、使用单位实际部署非新境界 OA 系统的： 申请：使用单位登录云监管平台，提出业务系统迁移上云申请，同时上传内部流程盖章纸质扫描件； 审核：云监管平台与管理单位 OA 系统对接，收到使用单位发起的申请后，将云资源申请及相关材料的扫描件转发给管理单位 OA 系统，由管理单位审核，通过管理单	业务迁移审批流程设计	

海南省大数据安全体系建设项目—2021-09-24 00:33:16.8 4fb32ee3e76d2453e38e4b0456d55daaee—7.6.

		位审核的，由 OA 系统将审核通过的信息发送的到云监管平台；没有通过审核的，把 OA 系统返回的不通过的原因反馈给使用单位； 备案：云监管平台在收到 OA 系统的审核通过通知后，按照审核后的云资源下发工单到云服务商，由云服务商完成资源配置，并在云监管系统中完成备案； 上线：由使用单位及业务系统开发商在云服务商的配合下，完成系统部署和上线； 变更：使用单位为云上系统资源变更在云监管平台发起变更申请，云监管平台将申请转发管理单位 OA 系统，经管理单位审核通过后，按照管理单位审核后的资源变化进行云资源调整；没有通过审核的，把 OA 系统返回的不通过的原因反馈给使用单位； 退出：使用单位为云上系统退出政务云在云监管平台发起退出申请，云监管平台将申请转发管理单位 OA 系统，经管理单位审核通过后，按照由使用单位及业务系统开发商完成系统下线、数据回收后，云服务商回收云资源。		
33	3.3.1.7.6 业务开通	政务云使用部门按照业务迁移审批流程，依据实际情况使用 OA 系统或者云监管平台向监管单位提交相关材料。新建业务系统申请，需提交项目实施方案和相关批复文件。已经业务系统迁移上云，需要提交业务系统迁移上云方案和相关批复文件，以及需要申请的资源清单。 政务云监管部门收到使用部门的申请后组织专家对相关方案进行评审。评审通过后系统将自动向云服务商派发工单开通资源。 云服务商开通资源后，用户单位开始在云上进行业务系统的部署、测试、等保测试，并向监管部门提交测评报告。监管部	满足招标文件要求。详见投标技术方案 18.3.2.1.6.6 业务开通	完全响应

海南省大数据安全体系建设项目—2021-09-14 00:38:18 844—bb2e2e9676d25f3e80fb0456d55daaee—7.6.
1005.271

		门完成材料审核后批准系统正式上线运行。		
34	3.3.1.7.7 业务变更	业务系统上线运行后，如需对已申请的资源进行变更，或新增资源，需要按照业务迁移审批流程，依据实际情况使用 OA 系统或者通过云监管平台提交业务变更申请；由监管部门依据提交的材料和实际使用情况进行审核。监管部门审核通过后，系统自动向云服务商派发资源变更工单。由服务商完成资源变更操作。	满足招标文件要求。详见投标技术方案 18.3.2.1.6.7 业务变更	完全响应
35	3.3.1.7.8 业务退出	业务系统从政务云迁出或注销时，使用部门需要按照业务迁移审批流程，依据实际情况使用 OA 系统或者云监管平台提交业务退出申请，监管部门审批通过，由使用单位在云监管平台确认完成数据备份后系统自动向云服务商派发资源销毁工单。云服务商要协助使用部门做好数据备份工作，在确保退出后信息安全的基础上，及时回收云资源、终止云服务。	满足招标文件要求。详见投标技术方案 18.3.2.1.6.8 业务退出	完全响应
36	3.3.1.7.9 资源订单	政务云使用单位通过资源订单申请资源。计费系统根据用户单位通过资源订单申请的资源数量进行计费。资源订单随业务迁移流程自动生成和流转。 基于资源订单进行计费管理，正确地计算和收取用户使用云计算服务的费用。 创建：委办厅局用户登录后，选择要订购的服务，放入订单中。 订单列表：委办厅局用户登录后，根据所选择收集信息，如使用的硬件资源、网络服务等来计算服务费用，并统一放置于订单中。 清空订单：用户将放置于订单中的信息进行一键清空。 订单提交：在订单里查看可以看到所购买服务的详细信息，包括项目名称&部门名	满足招标文件要求。详见投标技术方案 18.3.2.1.6.9 资源订单	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:35:10:884—bb22e9e970d2f53e964b04566f5daee—7.6.
105.21

		称，服务目录、价格，数量以及总价，点击“提交按钮”提交订单。 费用计算：根据订单中的服务项目数，每服务项价格的小计和订单内所有物品的服务项的总价格，将这些数字计算出来后显示在界面上。 订单管理：负责订单中心订单的管理，用户可以对商品进行添加、修改、删除信息以及提交订单等操作。 订单查询：支持以资源为粒度查看计费详细情况。 订单明细：项目/账户支持指定资源查看账单明细，点击资源账单后面的明细按钮即可查看。 订单变更：若检查订单有误，根据情况变更订单。 订单撤销：若检查订单有误，根据情况取消订单。 订单受理：海南省大数据管理局根据订单情况审批通过后，云服务商用户受理订单。 订单审核：只有经过审核的订单才会被确认为确实发的交易，对于不可信订单可以进行手动删除。 订单处理 自动处理：每天定时拉取前一天的数据，任务处理完成或失败发送微信、钉钉通知及告警。 手动处理：支持手动设置，根据某一天/时间段参数促发重跑数据。 批量处理：批量更改服务期限的操作、批量删除等操作。		
37	3.3.1.7.10 账单管理	账单管理功能由账户中心实现，是云监管平台运营管理子系统的核心功能。系统每月为各用户单位和服务商生成计费账单，账单支持导出成文件。 账务中心是围绕计费、订单的基本业务，集中到账务中心统一处理。	满足招标文件要求。详见投标技术方案18.3.2.1.6.10账单管理	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:32:10.884—bb22fe9676d2253f80fb0456d55daaee—7.6.100.2.1

		账务管理：账务管理是指对综合帐单的生成、管理及核算的过程。支持以计费项目/部门/账户为粒度查看汇总账单。 账单确认：根据账单信息，点击账单确认链接，进行此条账单状态的确认。 项目详情：项目/账户详情页支持以账户、部门、账单为粒度查看资源账单。 账户详情：账户详情页支持以资源为粒度查看资源账单。 部门详情：部门详情页支持查看直属项目计费和下级部门计费，并支持以项目列表方式查看直属项目账单。部门管理员和部门负责人支持查看部门账单。 账单详细：支持指定资源查看账单明细。 汇总月账单：对租户的账单进行汇总，可设置为每个月的1号出上个月的账单。 自定义账单：可根据用户的需求，自行定义汇总时间。 自定义定时输出：自定义定时输出账单明细，支持以资源为粒度查看计费详细情况。 账单搜索：可以根据用户名、服务目录搜索出来用户的月度、季度、年度账单。 结算管理：用户结算情况根据云服务业务进行处理，分为委办厅局、云服务商用户。 清单管理：清单管理是可以查询该用户的服务清单以及历史账单。如查询历史清单，则点击“历史清单”即可，可以根据时间区间进行查询。 账单导出：点击账单导出按钮，导出历史账单为Excel文件。 订单视图：通过可视化的方式展示租户/项目费用情况。 成本优化：提供多种方式的成本优化建议和分析，并支持通过费用月度、季度、年度趋势对比和预算告警，全方位进行成本管控。		

海南省大数据安全体系建设项目—2021-09-24 00:35:10 884 sb22fe9876d25f864b0456d55daaee—7.6.1900.Z1

		快速识别未使用的资源，对部分资源进行合理配置的推荐，大幅提高资源利用率，间接降低资源使用成本。 项目和账户：可将项目加载到部门，以部门为单位统计账单，也可以通过账户为单位统计计费账单。 账户：计费价目配置完成后，可以以部门为单位实时生成计费账单。 项目：计费价目配置完成后，即可以项目为单位实时生成计费账单。		
38	3.3.1.7.11 用户账单	系统为政务云用户单位生成的账单，账单内容包括计费周期内本单位各业务系统使用的资源清单和计费数据。计费账单按照用户的业务系统的维度来统计，统计业务使用的云资源，计算每个资源在计费周期内的费用，最后汇总后生成用户的账单。	满足招标文件要求。详见投标技术方案 18.3.2.1.6.11 用户账单	完全响应
39	3.3.1.7.12 服务商账单	系统为政务云服务商生成账单，账单内容包括结算周期内服务商为用户单位开通的资源清单和计费数据。	满足招标文件要求。详见投标技术方案 18.3.2.1.6.12 服务商账单	完全响应
40	3.3.1.7.13 资源清单	云监管平台作为政务云的监管系统，帮助政务云监管单位跟踪资源的整个生命周期。通过资源清单功能，可查看资源当前的计费状态，支付状态以及资源开通、变更、退出相关的订单信息，方便用户进行管理。 业务系统情况：业务系统概览主要包括系统名称、业务系统定级、系统虚机数量、计算资源数、存储资源数。	满足招标文件要求。详见投标技术方案 18.3.2.1.6.13 资源清单	完全响应
41	3.3.1.8 系统运维子系统设计 3.3.1.8.1 系统概述	运维管理是面向管理维护人员，将服务、资源的各项管理功能构成一个统一的工作台，来实现管理维护人员的配置、监控、统计等功能需要。其中告警是运营过程的关键信息，主要围绕系统出现异常时，快	满足招标文件要求。详见投标技术方案 18.3.2.1.7 系统运维子	完全响应

海南省大数据安全体系建设项目-2021-00-A-0.35:1088-bb32fe976d25538d10456d55daaee--7.6.1005.271

		速发现、通知相关人员，并付诸其快速评估故障影响，定位故障根源，以尽快恢复故障降低或消除影响。告警中心负责数据的实时分析处理，将多维度的数据通过管理对象统一管理，并根据不同维度的数据的特征，提供不同的处理引擎，并将处理结果存储在数据仓库中。	系统设计中18.3.2.1.7.1 系统概述	
42	3.3.1.8.2 功能设计	系统运维子系统的主要功能包括：组织机构管理、通讯录、告警管理、政务云告警情况统计、公告管理、通知管理和运维审计等。	满足招标文件要求。详见投标技术方案18.3.2.1.7.2 功能框架	完全响应
43	3.3.1.8.3 组织机构管理	以树状结构的方式管理政务云使用单位、监管单位、服务商、业务承建方的组织结构，明确各方的的职责和权限。 用户单位具有上下级关系的，在监管平台中，可配置上级单位是否需要监管下级单位的资源使用状态、业务运行状态和虚拟环境的安全状态。 运维管理子系统可与管理单位 oa 系统、云服务商的维系统进行组织架构与人员信息的同步对接，实现组织架构变更自动同步，人员变更同步与提醒。 当其他系统上的人员信息发生变动（离职、调岗），系统将自动同步，并提醒相关人员及资产管理人员监督其相关的资产交接工作。避免因日后因人员变动累积而造成资产管理的混乱。	满足招标文件要求。详见投标技术方案18.3.2.1.7.3 组织机构管理	完全响应
44	3.3.1.8.4 通讯录	运维通讯录功能用于维护政务云的使用单位、监管单位、服务商、第三方厂商相关人的联系信息。方便在政务云运维和应急响应过程中联系相关人。	满足招标文件要求。详见投标技术方案18.3.2.1.7.4 通讯录	完全响应

海南省大数据安全体系建设项目—2021-00-4 20:35:10:884—bb21:976:24:53:864bd45d5d5dae—7.6.

45	3.3.1.8.5 告警管理	控制台:将告警事件信息接入可视化管理场景，能够直接在视图中查看管理对象的视图。能根据资源监控的结果和系统日志产生预警，包含但不限于以下内容告警：	满足招标文件要求。详见投标技术方案 18.3.2.1.7.5 告警管理	完全响应
46	3.3.1.8.6 政务云告警情况统计	政务云告警情况统计：告警概况统计主要包括危急、高危、中危、低危、合计。政务云问题事件统计：问题事件情况包括事件标题、事件描述、时间等。 政务云监控故障统计：监控故障包括网络故障、主机故障、数据库故障、应用服务器故障、存储设备故障、系统设备故障、安全设备故障、硬件设备故障。 政务云防御趋势统计情况：近 3 个月共计防御趋势包括攻击情况、防御情况 告警报告：告警报告对被监控设备运行过程中产生的告警进行统计。 告警统计：主要对告警进行统计，包括了告警按类型统计、告警数量排名，告警资源 TopN、告警按级别统计、告警处理时间日统计。	满足招标文件要求。详见投标技术方案 18.3.2.1.7.6 告警统计	完全响应
47	3.3.1.8.7 公告管理	在云监管平台中提供系统公告模块，方便管理人员录入相关的公告信息，如升级维护，计费方式调整等公告通知，发送给各用户单位管理人员、维护人员、用户，公告的发送方式支持页面通告和基于角色的定向通告，并能支持定时发送的功能，用户只能进行公告信息的浏览、查询操作，系统管理员则可以进行公告信息的发布、编辑、删除等工作。 租户通过公告管理可以查看最新的公告，同时通过公告的文档下载页面可以下载各类文档模板、报表、指南等。 内容模板：系统提供了丰富的报告模板，包括维护模板、升级模板、计费调整模板等各种模板。	满足招标文件要求。详见投标技术方案 18.3.2.1.7.7 公告管理	完全响应

海南省大数据安全体系建设项目—2021-09-24 20:05:10.841—hb221e976d253f8040456d55daaee—7.6.

		规则设置：规则设置包括紧急、重要、一般、提示。 分组设置：邮件报警、电话报警、短信报警可以进行分组设置，可以将报警信息发给组内的每一个成员。 信息推送：提供信息推送工具，各部门可根据需要将部门内的数据推送给相应群体或个人。		
48	3.3.1.8.8 通知管理	云监管平台支持用户自定义告警通知策略，可配置不同类型、不同级别的告警产生后的通知方式。支持将告警通过邮件、短信、海政钉、微信、钉钉等方式实时通知到相关人。 微信提醒：为实现移动微信，则需要提供资产管理企业号，通过该企业号所有内部人员可以在通过认证的情况下进行登录微信办公平台。 短信提醒：为了实现短信通知则需要提供短信网关或短信猫，可以通过网络短信进行通知。 邮箱提醒：为了实现邮件通知，则需要提供公共的通知类邮箱。 钉钉提醒：为实现钉钉提醒，则需要提供资产管理企业号，通过该企业号所有内部人员可以在通过认证的情况下进行登录钉钉办公平台。	满足招标文件要求。详见投标技术方案18.3.2.1.7.8 通知管理	完全响应
49	3.3.1.8.9 运维审计	系统运维子系统中部署完整的日志管理模块，可以记录所有用户登录系统的时间和操作，实现所有操作留痕可追溯。	满足招标文件要求。详见投标技术方案18.3.2.1.7.9 运维审计	完全响应
50	3.3.1.9 报表管理子系统设计 3.3.1.9.1 系统概述	报表管理的主要任务是通过动态、有选择性地采集和更新服务目录的信息及云上租户外部相关信息，进行智能化地分析、处理、预测、模拟等，最终向各级决策管理	满足招标文件要求。详见投标技术方案18.3.2.1.8 报表管理子系统	完全响应

海南省大数据安全体系建设项目—2021-09-14 20:35:10.884—bb22fe9f76d2f53f80fb0456d55daaee—7.6.

		者或专业人员提供及时、科学、有效的分析报告，做好信息、智力支持工作。	设计中18.3.2.1.8.1系统概述	
51	3.3.1.9.2 功能设计	报表管理子系统的主要功能包括：统计分析、运营分析、报表导出、报表订阅和报表输出等。	满足招标文件要求。详见投标技术方案18.3.2.1.8.2功能框架	完全响应
52	3.3.1.9.3 统计分析	对电子政务云服务费用计算结果进行统计分析，分析电子政务云服务费用历史数据；分析本年度所有厅局、地市政府电子政务云服务费用；可实现按类别、按部门、按时间段等不同要求的综合统计；按租户使用云服务目录的情况；按云服务商计费情况统计。	满足招标文件要求。详见投标技术方案18.3.2.1.8.3统计分析	完全响应
53	3.3.1.9.4 运营分析	为平台运营提供各项指标的分析能力，为平台运营提供决策建议支持。	满足招标文件要求。详见投标技术方案18.3.2.1.8.4运营分析	完全响应
54	3.3.1.9.5 报表导出	根据用户自定义内容导出数据费用报表。	满足招标文件要求。详见投标技术方案18.3.2.1.8.5报表导出	完全响应
55	3.3.1.9.6 报告订阅	提供按照租户、服务目录、区域的费用详情，并可订阅相应的报告。	满足招标文件要求。详见投标技术方案18.3.2.1.8.6报告订阅	完全响应
56	3.3.1.9.7 报表输出资源报表	提供政务云资源相关报表，包含物理资产和虚拟资源两大类报表。 一、资产报表	满足招标文件要求。详见投标技术方案	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.0—bb32fe9670d25538b1b456d55dace—7.6.
1005.27

		提供物理资产相关报表数据。统计政务云资产的正常配置情况，监管方通过报表可了解合同要求配置的设备数量和当前云服务商实际交付的设备数量，已经这些设备的运行状态。 二、容量报表 物理资源负载报表：统计各资源池物理设备的负载情况，包括物理 CPU、物理内存和物理存储空间的总容量和使用率。物理资源的负载状态是判断资源池是否需要扩容的核心依据。资源使用核查报表：统计云资源池资源的使用量和实际分配给各厅局的资源总量，并对比两者之间的差距，发现云服务商不合规的资源分配。 三、分配报表 资源使用报表：统计各单位申请了多少资源，以及资源的平均使用率。帮助政务云监管人员了解资源使用大户，了解资源分配的合理性，及时通知资源配置不合理单位进行整改。 空闲云主机报表：发现系统中资源使用率很低的云主机，并以 TOPN 的方式统计哪些单位空闲云主机最多，方便督促相关单位及时调整资源配置。 没有归属的资源报表：发现不属于任何一个用户单位的资源，这类资源通常是未经正规流程开通的资源，使用单位不明。为规范政务云资源的开通和使用，资源申请和使用须经正常的申请流程。 月新增云主机报表：按月统计当月新增的云主机报表。 业务报表 1、业务运行状态报表 帮助用户单位和监管方了解业务系统上云后的运行状态，从业务角度了解云环境的可用性、性能和安全性。 2、异常业务报表	18.3.2.1.8.7 报表输出	

海南省大数据安全体系建设项目—2021-09-24 00:35:16.854—b82fe3e676d2453f864b0456d55daaee—7.6.

		统计各用户单位下面没有关联云主机的业务系统个数和没有关联业务系统的云主机个数。 运营月报 1、资源申报报表 未经申请的资源 统计用户单位未经过资源申请流程申请，但服务商已付的资源。通过该报表可发现未经过资源申请而直接交付的资源。 未交付的资源 统计用户单位已经提交了资源开通申请的流程，但服务商还未交付的资源。 规格不一致的资源 统计云服务商已交付的资源里，资源的规格与资源申请流程中对应资源的规格不一致的资源。 运维月报 运维月报反应云监管平台当月整体运行情况的报表，包括政务云平台基本情况、委办厅局资源情况、下一步工作计划等。		
57	3.3.1.10监管大屏子系统设计 3.3.1.10.1 系统概述	云监管平台提供统一大屏展示功能，在已有的庞杂的监管数据的基础上进行进一步抽象和统计分析，将监管人员最为关注的统计类信息通过大屏展示出来，便于监管人员掌握政务云整体运行情况。 监管大屏子系统与云监管平台主体共同部署在政务外网上，除了大屏幕以外，政务外网内的 PC、平板电脑终端以及手机移动端均可直接访问，同时移动端访问需和海政钉打通，能够实现海政钉内查看资源使用及各类告警信息。	满足招标文件要求。详见投标技术方案18.3.2.1.9 监管大屏子系统设计章节中18.3.2.1.9.1 系统概述	完全响应
58	3.3.2.1.9.2 功能框架	大屏展示主要涵盖政务云整体态势大屏、业务信息大屏、资源态势大屏和网络信息大屏 4 个方面。	满足招标文件要求。详见投标技术方案18.3.2.1.9.2 功能框架	完全响应

海南省大数据安全体系建设项目—2021-09-14-09:35:10-884-bb22e9676d2f5f3864b0456d55daaee—7.6.

59	3.3.1.10.3 整体态势大屏	展示系统的整体组成、资源整体配置情况、业务整体运行情况、安全态势概况等	满足招标文件要求。详见投标技术方案18.3.2.1.9.3 整体态势大屏	完全响应
60	3.3.1.10.4 租户信息大屏	展示业务上云租户的分布情况，以及租户访问云监管平台的统计分析；	满足招标文件要求。详见投标技术方案18.3.2.1.9.4 租户信息大屏	完全响应
61	3.3.1.10.5 业务信息大屏	展示业务上云状态统计分析，业务可用性统计分析，业务资源占用统计分析等；	满足招标文件要求。详见投标技术方案18.3.2.1.9.5 业务信息大屏	完全响应
62	3.3.1.10.6 资源态势大屏	按云租户的维度来展示部门的业务系统，每个业务系统分布的资源池，部署的云资源。显示各个业务系统的资源利用率，以及业务系统当前的资源配置。	满足招标文件要求。详见投标技术方案18.3.2.1.9.6 资源态势大屏	完全响应
63	3.3.1.10.7 网络信息大屏	展示云服务商平台网络连通状态，出口链路带宽利用情况以及出口带宽流量历史趋势信息等。	满足招标文件要求。详见投标技术方案18.3.2.1.9.8 网络信息大屏	完全响应
64	3.3.2 可信计算免疫平台建设 3.3.2.1 设计框架	通过在海南省电子政务外网公共服务平台核心服务器部署可信计算安全组件，以及提供的安全服务，实现以系统底层为出发点，可信计算技术为基础、访问控制为核	满足招标文件要求。详见投标技术方案18.3.2.2可 信	完全响应

海南省大数据安全体系建设项目—2021-09-24 10:55:10.884—bb321e9676d2453f864b0450d5da2ae—7.6.

		心，安全服务为辅助，构建具有主动防御能力的云计算安全防护体系，保证云计算环境的安全，形成严密的安全保护环境，有效抵御恶意代码的入侵、云计算资源越权使用等恶意行为。本次在海南省电子政务外网大数据公共服务平台 37 个节点服务器上部署可信计算免疫平台，采用主动防御手段有效保护服务器安全。采购可信计算免疫平台产品含三年服务，服务期内业务升级、业务扩容、业务重大变更时需派技术人员进行支撑保障。	计算免疫平台技术方案 18.3.2.2.1 平台总体设计	
65	3.3.2.2 可信免疫平台采购清单	1. 可信计算免疫平台管理中心 1.服务端安全管理软件：B/S 管理模式，实现客户端软件的策略统一管理、日志统一收集、软件集中管理及分发等安全管理功能。基于操作系统内核技术，是安全功能控制的一组安全模块软件，安装于需要受保护的操作系统中，其实现功能包括静态度量、动态度量、强制/自主访问控制、性能监控、可信链接、安全认证等。 2.▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。 2. 可信计算免疫平台客户端 1.客户端安全模块软件：基于操作系统内核技术，是安全功能控制的一组安全模块软件，安装于需要受保护的操作系统中，其实现功能包括静态度量、动态度量、强制/自主访问控制、性能监控、可信链接、安全认证等。服务期内业务升级、业务扩容、业务重大变更时需派技术人员进行支撑保障。服务期内公共服务平台如增加服务器数量不超过 5 台，则增加的服务器可免费安装该软件。	满足招标文件要求。详见投标技术方案 18.3.2.2可信计算免疫平台技术方案 18.10 重要指标（▲指标）应答	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:32:18 84-6132ie3fd2253f864b0456d55daaee—7.6.

		2.▲提供所涉及产品原厂商针对本项目专项授权和原厂商盖章的 3 年原厂标准服务承诺函，提供 7×24 小时热线受理，远程处理问题，上门技术支持。		
66	3.3.3 政务大数据安全保障平台 3.3.3.1 政务大数据安全保障平台软件清单	政务大数据安全保障平台的数据安全能力中心、数据安全告警中心、数据地图、数据脱敏、数据追踪溯源、数据安全审计、数据安全网关、平台组件安全检测功能的共 316 个功能点	除满足招标文件要求外，**增加数据安全指标评估工具功能，该功能共包括评估概览、组织管理、安全评估、任务管理、权重管理、文档中心 6 个功能点。** **详见投标技术方案** **18.3.2.3政务大数据安全保障平台技术方案 18.3.2.3.5 功能设计 18.3.2.3.5.2 功能清单**	**正偏离**
67	3.3.3.2 总体概述	通过政务大数据安全保障平台可以实现数据全生命周期安全防护，并且支撑数据安全管理和运营，防范敏感数据泄漏。平台聚焦于数据全生命周期，按照数据分类分级的要求，针对数据的采集、传输、存储、加工、开放、共享、销毁的全生命周期中风险，本项目利用脱敏、溯源等安全技术实现数据本身的安全防护，实现对政务数据对服务中数据对外出口统一监测与管控，确保对外服务和使用的数据安全合规，可以追踪溯源，严控数据安全风险，杜绝数据泄漏、误用与滥用。	满足招标文件要求。详见投标技术方案 18.3.2.3政务大数据安全保障平台技术方案 18.3.2.3.1 平台总体设计	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.884—bb32fe9f76125538d4b1515d5d5ae—7.6.1005.271

68	3.3.3.3 功能框架图	政务大数据安全保障平台的主要功能包括数据安全能力中心、数据安全告警中心、数据地图、数据脱敏、数据追踪溯源、数据安全审计、数据安全网关、平台组件安全检测功能。 政务大数据安全保障平台功能模块主要包括： 1. 数据安全告警中心 数据安全告警中心通过采集各平台子模块，以及其它系统提供的日志数据和告警数据，利用数据处理引擎，实现告警可视化、安全报告、操作回放、智能告警。 2. 数据安全能力中心 数据安全能力中心作为数据安全保障平台的统一门户，将本平台所有的能力组件以及其他第三方数据安全组件进行集成，实现一中心管理。 3. 数据地图 数据地图对数据资产体系化、结构化的管控视图，具备元数据、数据地图分析、结构体变更识别、血缘影响分析等能力，清晰明确展示数据存储、数据结构体发生变化、数据的来源和影响关联等情况，并及时预警。 4. 数据脱敏 数据脱敏功能通过脱敏规则和算法将敏感数据按照配置的规则和算法进行转换，保护敏感数据不被泄漏。应用于目前大数据管理局数据对外提供使用时，需要将数据中包含的敏感数据字段脱敏；在开发测试环境中，将生产数据脱敏后使用；在数据分析和数据治理过程中只需要保留原有的数据关系与格式，不需要使用原始明细数据的等场景中。可以实现对于存储数据的静态脱敏，也可以实现动态脱敏。 5. 数据追踪溯源 数据追踪溯源功能采用基于内容的数字水印技术对数据进行水印标识加注，实现对	**除满足招标文件要求外，增加数据安全指标评估工具功能，该功能共包括评估概览、组织管理、安全评估、任务管理、权重管理、文档中心6个子功能。详见投标技术方案18.3.2.3.5 功能设计**	**正偏离**

海南省大数据安全体系建设项目—2021-09-24 20:33:16 84-bb32fe9676d25f3864b456d55daaee—7.6.
1003271

		数据权属确认和泄漏者溯源等功能。水印标识包含数据所有者标识，授权的使用方标识，以及加注时间戳等信息，在数据拷贝、转换、截取等数据处理过程中，数据水印标识信息依然有效。用于大数据局管理局共享交换体系中如果流转了重要数据和敏感数据，或者其他需要外发的数据中包含了敏感数据的情况下，需要对数据进行水印标识，一旦数据发生泄漏，可以对发现的泄漏数据进行数据溯源，通过数据中的水印信息，确认数据泄露者。 6. 数据安全审计 数据安全审计功能基于大数据中心主机、数据库、安全设备告警、网络设备、VPN、堡垒机、数据接口等日志数据和流量数据的分析，对数据安全风险进行监测与审计。包括对接口传输数据的合规性进行安全监测与审计，发现是否为违规调用接口的情况、是否存在已停止服务但依旧有数据调用的情况，是否存在与接口规范不符的数据调用等风险。对系统开发运维人员操作的安全监测与审计。可以实现账号异常、用户异常、数据库访问异常、高危操作、堡垒机绕行、未授权操作、越权访问等风险的监测与审计。 7. 数据安全网关 数据安全网关功能用于需要对数据下载或外发进行强监管的场景，例如数据分析、治理人员需要下载生产环境的数据，或其他确实因为业务需要有数据下载的需求，可以通过此项功能模块实现事前审批，事中安全检测，事后审计，确保每一条对外分发的数据均安全合规。 8. 大数据平台组件安全检测 大数据平台组件大多基于开源框架开发而成，传统的基线检查工具往往不能覆盖对于大数据平台组件，大数据平台组件安全		

海南省大数据安全体系建设项目—2021-09-24 00:35:10.814—b822e3e5e5764d2f5388b4b0456d55daaee—7.6.

		检测功能可以有效检测基础配置和漏洞扫描，增强大数据平台各组件安全性。 大数据安全保障平台作为公共的安全能力，可以向公共服务平台、共享交换平台、统一开放平台等的数据、业务提供共享的安全能力。		
69	3.3.3.4 功能模块定义	政务大数据安全保障平台的主要功能包括安全运营中心、数据安全能力中心、数据安全告警中心、数据地图、数据脱敏、数据追踪溯源、数据安全审计、数据安全网关、平台组件安全检测的功能模块的定义。	**满足招标文件要求外，增加数据安全指标评估工具功能，该功能共包括评估概览、组织管理、安全评估、任务管理、权重管理、文档中心6个子功能的设计。详见投标技术方案** **18.3.2.3.6 功能模块详细设计**	**正偏离**
70	3.3.4 政务大数据安全制度规范体系建设	在海南省大数据安全体系规划架构之下，结合政府数据安全管理的实际情况，设计海南省政务大数据安全制度规范体系。建立大数据安全制度规范体系，为大数据安全防护运营提供依据，数据安全管理策略的完善，为大数据安全防护、审计、运营提供了依据，使政务数据安全管控有据可依。 政务大数据安全制度规范，需在工期内完成编制并由海南省大数据管理局印发 制度清单包括： 1.一级管理制度 《政务数据安全管理办法》 《政务数据安全问责办法》	满足招标文件要求。**增加了三级工作流程、细则内容的编制。共增加三个三级工作流程，《业务系统上线前安全检测流程》、《安全漏洞管理细则》、《系统下线流程》。**	**正偏离**

海南省大数据安全体系建设项目—2021-09-4 00:35:10.884—bb32fe06f6da453f6b15d5dae—7.6.1005.271

		2.二级管理规范和技术标准 《政务数据安全管理规范》 《政务数据安全管理规范》 《政务数据安全分级规范》 《数据资产安全管理规范》 《政务数据安全技术防护标准》 《政务数据脱敏规范》 《数据权限管理规范》 《数据审核合规规范》 《数据日志留存指南》 《日志安全审计规范》 《数据安全评估规范》 《政务数据安全监管规范》 《政务数据安全监测与预警规范》 《数据安全事件与应急规范》 《数据销毁安全规范》 《数据申请流程》 《数据安全应急预案》 《大数据平台安全基线配置标准》 《基线配置要求及检测要求-网络设备》 《基线配置要求及检测要求-操作系统 《基线配置要求及检测要求-数据库》 《基线配置要求及检测要求-中间件》 《基线配置要求及检测要求-web 应用系统》 《网络分区分域安全防护标准》 《政务云安全体系规范》 《海南省电子政务外网管理规范》 《政务外网网络安全建设指南》	详见投标技术方案 18.3.2.4政 务大数据安全制度规范技术方案	

海南省大数据安全体系建设项目—2021-09-24 00:32:10 8f4bb22fe9676d2453f864b0456d55daaee—7.6.

71	3.3.5 政务大数据安全运营监管服务 3.3.5.1 政务大数据安全运营监管服务清单	政务大数据安全运营监管服务清单 包括全面资产管理、数据分级、系统安全检测、数据权限安全监管、数据输出安全监管、数据安全风险监测、安全应急及重保服务、大数据安全风险评估、安全检查与审计、大数据安全监管报告、大数据安全监管报告	满足招标文件要求。详见投标技术方案 18.3.2.5政务大数据安全运营监管服务技术方案 18.3.2.5.3 政务大数据安全运营监管服务清单	完全响应
72	3.3.5.3 政务大数据安全监管人员要求	安全运营监管团队人员数量要求不低于 15 人，一线人员 8 人，其中，不少于 1 名项目经理、7 名项目团队人员，其中项目经理需具备数据安全相关高级资格证书，项目团队中至少 3 人需具备数据安全相关中级资格证书，其余项目组成员至少 3 年以上的数据安全相关方面工作经验。二线人员 4 人，需具备数据安全相关中级资格证书，并具备 3 年以上数据安全相关方面工作经验。专家 3 人，需具备数据安全相关高级资格证书，并具备 5 年以上数据安全相关方面工作经验。供应商须在响应文件中提供完整的实施团队名单及职责分工，所有人员必须属于供应商在册员工（提供 2021 年近三个月社保缴纳证明为认定依据），并提供相应人员相关信息（包含所学专业、学历及相关资质证明与安全相关的资质证书证明材料），相关证明须加盖投标人公章。如中标后提供的项目团队与投标提供的团队名单材料不符，将追究法律责任。	**除满足招标文件要求外，增加1名一线驻场人员，总共为9人**。详见投标技术方案 18.4.6.2项 目人员清单 18.4.6.3项 目组成员详细信息 18.7 大数据安全运营监管服务承诺函	**正偏离**
73	3.3.5.3.1 资产管理	1.服务内容 1）IT 资产管理 梳理省大数据中心重要业务系统的存量 IT 资产，包括公共服务平台、共享交换平台、码上办事平台和政务一体化服务平	满足招标文件要求。详见投标技术方案 18.3.2.5.4.1 资产管理	完全响应

海南省大数据安全体系建设项目—2021-09-24 06:34:10 844-b32ee3e67d2153f8f4b0436d5dac—7.6

		台，形成具备资产属性、IP、版本、资产责任人等的资产台账。建立新增 IT 资产的管理模式，确保所有资产纳入管理。 3）数据资产管理 梳理公共服务平台、码上办事平台和政务一体化服务平台等系统的数据资产，形成数据资产清单，明确管理对象，严控政务数据安全风险，杜绝数据泄漏、误用与滥用。 2.服务成果 全面资产管理，按月交付包括不限于以下服务成果： 1）《IT 资产清单》 2）《数据资产清单》		
74	3.3.5.3.2 数据分级	1.服务内容 按照数据分级标准，借助省大数据局的分类分级平台，对公共服务平台、码上办事平台、政务一体化服务平台等的数据进行安全分级，数据分级的粒度到数据字段级别。数据分级完成后，定期对数据级别进行核查，如发生变化，应对相关数据的安全级别进行变更。 2.服务成果 （1）在数据分级平台中完成元数据的安全级别的标识，并通过接口供各平台获取调用数据级别结果。 （2）对大数据公共服务平台分级分类工作进行监管。	满足招标文件要求。详见投标技术方案 18.3.2.5.4.2 数据分级	完全响应
75	3.3.5.3.3 系统安全检测	3.3.5.3.3 系统安全检测 1.服务内容 系统安全检测包括日常系统安全检测、系统/接口上线前安全检测、重要时期系统安全检测。 系统安全检测方法包括不限于安全基线检测、漏洞扫描、渗透测试、代码审计等方法。 1）日常系统安全检测内容包括不限于：	满足招标文件要求。详见投标技术方案 18.3.2.5.4.3 系统安全检测	完全响应

海南省大数据安全体系建设项目—2021-09-4 10:33:10.884—bb22e9.976d2453f864b0456d55daaee—7.6.1005.21

		对政务云部署系统进行日常安全检测： i. 对大数据管理局自有业务系统进行安全检测，通过排查系统的安全风险，发现安全短板，并及时对系统加固，每月至少覆盖所有系统。 ii. 对政务云部署的其他单位系统进行安全检测，排查系统的安全风险，并反馈系统责任方进行系统加固，每月覆盖所有系统。 iii. 对开发、运维人员将与省大数据局相关的研发代码、配置参数、技术文档等数据和信息发布到互联网共享平台的行为进行常态化检测。 2）系统/接口上线前安全检测 政务云部署的系统或接口新上线或有重大变更前，进行安全检测。 i. 系统安全检测。准备上线业务系统的相关资产进行安全检测，包括主机资产、数据库资产、中间件、应用等。 ii. 接口安全检测。针对需要上线的接口安全检测的内容包括接口身份验证方式、传输加密、请求参数、数据传输逻辑、输出数据内容、接口封装等。 3）重要时期系统安全检测 在国家或省里有重大活动前（如国庆、春节、护网期间或其他重大纪念活动、会议等），针对政务云部署的重要的政务业务系统开展系统安全检测工作，确保重保前系统安全无重大安全隐患。 4）安全问题协助加固整改，实现闭环。 2.服务成果 系统安全检测工作，按月交付包括不限于以下服务报告： 1）《系统上线前安全检测报告》 3）《日常系统安全检测报告》 3）《重保前系统安全检测报告》		

海南省大数据安全体系建设项目—2021-09-24 00:33:16-84-bb2e1e9e976d2253f864b0456d55daaee—7.6.

76	3.3.5.3.4 数据权限安全监管	1.服务内容 梳理省电子政务云业务系统现有的主机和数据库的账号和权限，设计权限管理方案，实现数据操作访问权限的统一管理。开展日常账号权限审批工作，对申请的账号以及权限进行确认，进行权限的配置。每月对账号权限清查和变更管理 2.服务成果 数据权限管理，按月交付包括不限于以下服务报告： 1）《账号与权限管理清单》 2）《账号与权限清查报告》	满足招标文件要求。详见投标技术方案 18.3.2.5.4.4 数据权限安全监管	完全响应
77	3.3.5.3.5 数据输出安全管控	1.服务内容 省电子政务外网需要借助大数据安全保障平台进行数据输出的安全管控，包括进行数据输出的审批，对输出的数据视需求进行脱敏或增加数字水印，对输出内容进行安全检测等，定期进行数据输出内容的安全审计。 按照《数据销毁安全规范》指导数据销毁工作，确保数据销毁全过程的记录、监管及结果验证。 2.服务成果 数据出口监管服务，按月交付包括不限于以下服务报告： 1）《数据输出安全统计分析报告》 2）《数据输出安全监管报告》	满足招标文件要求。详见投标技术方案 18.3.2.5.4.5 数据输出安全管控	完全响应
78	3.3.5.3.6 数据安全风险监测与审计	1.服务内容 1） 数据接口监测与审计 省电子政务外网重要系统的接口的合规性进行监测和审计，处置未纳入监管的数据 API 接口。 2） 数据操作行为监测 对拥有省电子政务外网账号和权限的人员的操作行为进行监测和预警 3） 数据安全风险闭环管理	满足招标文件要求。详见投标技术方案 18.3.2.5.4.6 数据安全风险监测与审计	完全响应

海南省大数据安全体系建设项目—2021-09-4-20035108-4—bb22e9970d2f53f864b0456d55daae—7.6.1005.21

		对通过监测发现风险，进行处置和跟踪，确保风险实现闭环。 2.服务成果 数据安全风险监测与审计，按月交付包括不限于以下服务报告： 1）《数据安全监测与审计报告》		
79	3.3.5.3.7 大数据安全应急响应管理与重保服务	1.服务内容 按照《数据安全事件与应急规范》、《数据安全应急预案》的要求，开展安全应急和重保工作，按照应急预案的机制和流程定期开展应急演练工作，并持续优化应急管理机制。发生安全事件后，开展应急处置工作。 在国家或省里有重大活动前（如国庆、春节、护网期间或其他重大纪念活动、会议等），派驻专家，提供重保服务，为重要时期提供安全保障。 2.服务成果 大数据安全应急管理与重保服务，交付包括不限于以下服务报告： 1）《应急演练方案》 2）《应急演练报告》 3）《应急处置、整改报告》 4）《重保期间服务报告》	满足招标文件要求。详见投标技术方案18.3.2.5.4.7 大数据安全应急与重保服务	完全响应
80	3.3.5.3.8 大数据安全风险评估	1.服务内容 对照“政务大数据安全管理制度体系”的要求，通过技术测试、管理检查、数据分析等多维度手段，开展大数据安全风险评估服务。评估范围覆盖政务大数据中心网络、系统、数据、业务流程以及相关人员，包括不限于,对承载数据的机房、网络、主机、平台、数据库、应用进行全面安全风险评估；对数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁等全过程以及和数据生命周期相关的管理、运营工作的执行情况进行安全评估；对承担省政务大数据中心系统开发、建设	满足招标文件要求。详见投标技术方案18.3.2.5.4.8 大数据安全风险评估	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.84—bb32fe976e2f53f80fb0456d55daaee—7.6.—1.03.271

		和运维人员进行安全检查。通过风险评估，全面了发现大数据安全风险。针对大数据安全风险评估发现的问题，大数据安全运营监管中心需指导和监督整改工作，确保风险整改，实现管理闭环。 2.服务成果 大数据安全风险评估服务，交付包括不限于以下服务报告： 1.《大数据安全风险评估报告》		
81	3.3.5.4 安全检查和审计	1.服务内容 大数据安全运营监管中心将针对政务云平台用户、重要的数据相关方，如第三方开发建设厂商、服务提供商，政务部门接触使用数据的人员、政务云服务商分级分域方案实施执行情况等进行安全检查与审计，进一步防控数据安全风险，内容不限于对于基本情况的检查与审计；3）对于数据安全管理相关情况的检查与审计；对承担关键工作的员工的检查和审计：网络访问行为、系统操作行为、数据访问行为、终端留存的数据；针对政务云服务商分级分域的实施情况的检查与和审计；协助监测各类设备状态，发现故障后及时进行通报和处置。 2.服务成果 安全检查与审计服务，交付包括不限于以下服务报告： 1)《安全检查与审计报告》	满足招标文件要求。详见投标技术方案18.3.2.5.4.9 安全检查和审计	完全响应
82	3.3.5.5 大数据安全运营监管报告	1.服务内容 按月将大数据安全运营监管情况形成报告并向大数据管理局汇报，报告包括不限于：敏感数据安全态势情况、重点工作开展情况、安全事件通报情况等。 2.服务成果 安全检查与审计服务，交付以下服务报告： 1)《大数据安全运营监管报告》	满足招标文件要求。详见投标技术方案18.3.2.5.4.11 大数据安全运营监管报告	完全响应

海南省大数据安全体系建设项目—2021-09-14 20:35:10.884—bb22e976d25538d4b0456d55daaee—7.6.

83	3.3.6 其他要求 3.3.6.1 政务大数据安全运营监管服务周期要求	政务大数据安全运营监管服务周期为 1 年。大数据安全保障平台和云监管平台系统部署上线并完成项目初验后，经甲方确认后，正式进入服务期。	满足招标文件要求。详见投标技术方案 18.3.2.5.5.4 服务周期	完全响应
84	3.3.6.3 实施要求 3.3.6.3.1 总体要求	供应商应结合自身的项目管理制度和经验，根据本项目的实际情况，在整个项目实施过程中各个控制阶段提出针对性的管理方法。以下内容主要是对项目实施过程的一些通用要求。 1、供应商应在采购人要求的工期内完成所有规定的系统建设任务。 2、采购人及采购人所委托的监理单位，有权对整个项目实施的全过程进行监督检查。供应商必须给予积极支持和配合，不得以任何理由回避采购人或监理单位的监督检查。 3、供应商必须建立完善的项目管理机制，以保证项目建设能按期进行。	满足招标文件要求。详见投标技术方案 18.4 项目实施方案 18.4.1 概述	完全响应
85	3.3.6.3.3 工期要求	供应商应在签订合同后 15 个工作日内提交详细的《项目实施计划》，合同签订后 12 个月内完成项目建设；	满足招标文件要求。详见投标技术方案 18.4 项目实施方案 18.4.3 实施进度计划	完全响应
86	3.3.6.3.3 服务要求	大数据安全监管服务的考核指标包括： 1.提供大数据安全监管服务团队人员数量。 安全运营监管团队人员数量要求不低于 15 人，不同能力等级人员的配备要求如下： 1）一线人员：7*34 小时值班，8 个人，负责大数据安全日常运营监管服务工作，在大数据管理局驻场服务，须具备相应的安全技术能力。	除满足招标文件要求外，**增加 1 名一线驻场人员，总共为 9 人**。详见投标技术方案 18.3.2.5.5 政务大数据安全运营监管服务指标	**正偏离**

海南省大数据安全体系建设项目—2021-09-4 20:25:10.884—bb22fe97b2253386b15d55daaee—7.6.1105.271

		3）二线人员：5*8 小时值班，4 个人，远程技术支持，必要时需现场支持，出现问题时 1 小时内能响应，具有较高的技术能力。 3）专家：远程技术支持，5*8 小时，3 人，具备高级技术能力。 3.大数据安全监管服务范围。 大数据安全监管服务范围应为大数据管理局所属系统检测覆盖率 100%，数据监管覆盖率 100%。 3. 大数据安全运营监管服务响应时间 1）驻场团队应小于 0.5 小时响应时间； 3）远程专家支撑团队应小于 1 小时响应时间。 4. 大数据安全运营监管服务时间 1）提供 5*8 小时现场服务 3）重要时期提供 7*24 小时现场服务 5. 重大数据安全事件数量 在提供大数据安全监管服务期间，省大数据管理局重大数据安全事件数量为 0。	18.4.6.2项 目人员清单 18.4.6.3项 目组成员详细信息 18.7 大数据安全运营监管服务承诺函	
87	3.3.6.3.4 项目组织管理要求	供应商应根据本项目的建设内容和项目特点确定本项目实施的组织结构和项目协调管理机制。	满足招标文件要求。详见投标技术方案 18.4.4 项 目组织管理 18.4.5 项 目管理方案	完全响应
88	3.3.6.3 系统安装、测试、试运行要求 3.3.6.3.1 安装检验	软件系统应通过光盘安装，系统的配置应简单、方便。供应商应提供现场专业技术咨询、安装、调试、初验、竣工验收和试运行保障服务（提供安装、测试所用的测试设备、工具等），并按照采购人要求进行产品客户化。在投标文件中应提交安装、调试、验收实施计划书，在安装调试验收无误后，提交安装实施、调试、检测报告、验收报告、技术资料、系统技术说明书、使用说明书、维护手册等。	满足招标文件要求。详见投标技术方案 18.4.6.1安 装检验	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:35:10.884-bb21e9576d2453f8b0456d55daaee—7.6.1005.271

		（1）安装调试人员应参照说明书或咨询供应商，了解设备的正确安装方法和使用的注意事项后，再拿到现场去安装调试，安装调试过的设备应能正常使用。 （3）安装调试人员应根据用户需求调试安装设备，设备调试的最终参数做成文档形式，交由用户存档。如：交换机的设置参数、使用端口等。 （3）对设备在安装时发现有异常，如：与合同不符没有联络函、设备有破损或配件不全等，应先停止安装，明确没问题后再安装调试。 （4）设备的调试过程中，发现有设备运行不稳定的，应及时联系供应商将问题解决或退换设备，避免将隐患留下。 （5）设备的调试应让设备发挥最大的效果，且设备不在满负荷下运行。 （6）设备的调试要作长远的规划，考虑将来的变更可能使用到的资源，包括硬件和参数资源，以应对在近期进行小的改动不至于增加工作量。 （7）设备调试完毕后，除记录相关参数存档外，调试所用的资源、资料，应在本地作一次系统备份和资源、资料备份，以备以后维护使用。 （8）设备调试后，应对设备的功能作一次基本的测试以验证设备的可用性。		
89	3.3.6.3.3 系统测试	供应商须制定系统整体测试方案，经采购人审查通过后，根据双方确认的测试方案对系统进行全面的检查与测试。 软件系统的测试 软件系统的测试工作包括以下几个方面： （1）测试方案的设计——测试方案的设计在系统方案设计阶段制定，必须得到双方的认可，经过专家审核后有效，并作为验收文件之一。 （3）系统测试——双方在项目测试阶段，严格按照测试方案进行测试工作。	满足招标文件要求。详见投标技术方案18.4.6.2系 统测试方案	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:32:10 884 b82ee9576d245a38fb0456d55daaee—7.6.

		（3）提交测试报告——项目测试完成后，编制项目测试报告，提交采购人或采购人委托的监理签署。 （4）软件测试方案需要包括软件集成测试和上线测试，测试内容要不少于：稳固性检查、系统可靠性测试、系统稳定测试、性能调整调试、各模块功能测试和完整性测试等。 硬件系统的测试 硬件系统安装完成后，按照系统要求的基本功能逐一测试。 （1）单项测试：单项产品安装完成后，由供应商进行产品自身性能的测试。 （3）网络联机测试：网络系统安装完成后，由供应商和系统使用单位对所有采购的产品进行联网运行，并进行相应的联机测试。 （3）系统运行正常，联机测试通过。 如系统测试中发现功能上不符合标书和合同时，将被看作性能不合格，系统使用单位有权拒收并要求赔偿。 供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术方案、资料、及安装、验收报告等文档交付系统使用单位。		
90	3.3.6.4 技术培训要求	有针对性的拟定培训计划，包含培训目的、培训内容、培训时间要求、考核办法等内容，确保使每个参加培训的人员能掌握系统的使用方法，培训计划应包含但不限于以下内容： （1） 能够免费为系统操作人员和系统管理员进行有关维护、操作等方面的技术培训，直至能熟练独立操作，并提供详细的培训天数、培训计划和培训内容并在合同签订后实施。 （3） 投标方应根据不同培训对象提供不同的培训内容，如系统操作、权限管理、日常运维等内容。确保培训人员对系统基	满足招标文件要求。详见投标技术方案 18.5 项目培训及售后方案 18.5.1 项目培训方案	完全响应

海南省大数据安全体系建设项目—2021-09-24-00:32:10-814-b822e9e9676d25f3864b0456d55daaee—7.6.

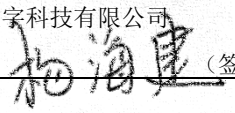
		本原理、技术特性、操作规范、管理维护等方面获得全面了解和掌握。 （3） 培训方式、培训人数、培训时间：采用现场培训、远程培训培训方式，培训人数、具体培训时间等在中标后双方再行确定。中标方在培训开始前 30 天内提交培训计划和教材。		
91	3.3.6.5 测试和验收要求	本项目验收应包括初步验收、竣工验收二个阶段，在项目终验完成时，应提供但不限于下列文档： （1） 初步验收申请表(承建单位向建设单位申请)； （3） 立项材料(经批复的项目立项文件、项目建议书或可行性研究报告)； （3） 项目采购文件(招投标文件)； （4） 采购结果通知书； （5） 项目合同书； （6） 项目设计文档(初步设计、详细设计)； （7） 项目实施方案； （8） 项目测试报告(系统测试、强弱电气检测、防雷、消防等,根据实际情况确定) （9） 项目经费结算表； （10） 项目建设内容完成报告； （11） 项目监理文档(大纲、规划、细则、报告和行业规范要求的文档)； （13） 其他材料(项目变更批复、设备清单、合同设备清单差异比对表、设备质量证明文件、设备验收单、变更单、第三方软件授权证明、培训手册、培训记录、设备配置。 （13） 含有软件开发的项目还需提供以下资料:1)软件需求规格说明书;3)概要设计说明书;3)数据及数据库设计说明书:4)详细设计说明书;5)操作手册;6)用户手册。 （14） 信息系统安全方面的材料:1)非涉密信息系统安全保护等级备案证明;3)涉密信息系统保密审查批复见;3)第三方机构软	满足招标文件要求。详见投标技术方案 3.4.7 项目验收方案	完全响应

海南省大数据安全体系建设项目—2021-09-24 00:35:10.841—bb22fe9670245388b4b0456d55daa6e—7.6.

		件测评报告:4)第三方机构出具的系统等级保护测评报告、整改意见及整改方案(非涉密系统)第三方机构出具系统分级保护测评报告、整改意见及整改方案(涉密系统)。		
92	3.3.6.6 知识产权要求	（1） 乙方为甲方开发的云监管平台和政务大数据安全保障平台权归甲方所有，乙方为实施项目而提供的资料及全部项目工作成果（包括项目计划、需求规格说明书、概要设计说明书、详细设计说明书、测试报告、安装部署手册、操作手册、培训方案、试运行报告、前台页面及软件源代码、项目验收文档等资料）的知识产权权利归甲方所有，乙方提供的具备知识产权的产品或采购具备知识产权的成熟产品（包括硬件产品和软件产品），知识产权仍归产品提供方所有；基于成熟产品进行二次开发的系统及成果的知识产权归甲方所有。 （3） 乙方保证对其销售的产品/服务拥有完全的所有权/处置权或已取得相关授权，不侵犯任何第三方的专利、商标、著作权和其他合法权利，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由乙方承担所有相关责任的同时不得耽误本项目进度。 （3） 乙方保证其提供的软件及服务不含有任何旨在破坏最终用户计算机信息系统和/或获取最终用户隐私信息的恶意代码。 （4） 乙方应在项目完成时，将本项目所有文档汇集成册交付甲方。技术文档（光盘与纸质）及为本项目开发的软件系统（光盘形式，包括注释清晰明了的源代码）各两份。	满足招标文件要求。详见投标技术方案 18.6 知识产权承诺函	完全响应
		未列入本表的条款	全部接受	完全响应

海南省大数据安全体系建设项目—2021-09-4 20:35:10 8f1-bb32e 9702f25 38d4b0456d55daaee—7.6.

投标单位全称（公章）：联通数字科技有限公司

法定代表人（或授权代理人）：  （签字或盖章）

注： 1、此表为样表，行数可自行添加，但格式不变。

2、根据投标文件响应情况，分别注明“正偏离”、“完全响应”、“负偏离”

3、对招标文件无偏离，视为对未列入本表的条款全部接受，注明“完全响应”。

海南省大数据安全体系建设项目—2021-09-24 00:35:10.884—bb32fe9676d2453f864b0456d55daaee—7.1005.271