

中国（三亚）跨境电子商务综合试验区 线上综合服务平台采购需求书

三亚市商务局

目录

A 包（系统开发与集成）	2
一、项目名称	2
二、建设工期	2
三、项目概况	2
1. 项目背景	2
2. 建设目标	3
3. 建设内容	4
四、功能需求	4
1 应用系统需求	4
2. 应用支撑子平台需求	9
五、非功能需求	16
1. 信息交换与共享需求	16
2. 数据资源需求	17
3. 系统部署需求	19
4. 系统集成需求	19
5. 网络安全服务采购需求	错误！未定义书签。
6. 运维服务需求	19
7. 性能需求	19
六、其他要求	20
1. 项目组织管理要求	20
2. 项目实施要求	20

3. 人员培训要求	21
4. 售后服务要求	21
B包（硬件设备与网络安全）	23
一、 项目概况	23
1.1 项目名称	23
1.2 项目预算	23
1.3 项目背景	23
二、 采购内容	24
三、 采购清单	25
四、 技术参数要求	28
4.1 服务器技术要求	28
4.2 网络设备技术要求	32
4.3 安全设备技术要求	34
4.4 网络安全服务技术要求	48
4.5 链路技术要求	50
五、 质保期	51
六、 付款方式	51
C包（项目监理）	52
一、 项目名称	52
二、 监理工作任务及目标	52
三、 监理工作范围	52
四、 项目监理总体要求	52
①项目前期监理要求	53

②项目中期监理要求	54
③项目后期监理要求	54
五、监理具体要求	54
①项目招标前期阶段监理工作内容.....	55
②项目招标阶段监理工作内容.....	55
③项目设计阶段监理工作内容.....	57
④项目实施阶段监理工作内容.....	59
⑤项目验收阶段监理的工作内容.....	61
六、交付成果要求	63
七、售后服务要求	63
八、监理团队要求	63
九、商务要求	64
D包（网络安全等级保护测评）	66
一. 项目名称.....	66
二. 项目预算	66
三. 项目目标	66
四. 项目内容	66
五. 项目工期	67
六. 项目需求	67
6.1 需求内容	67
6.2 服务清单	67
6.3 项目成果交付	68
6.4 测评方案	68

七. 服务要求.....	72
7.1 项目实施要求.....	72
7.2 项目验收要求.....	73
7.3 售后服务要求	73
E 包（商用密码安全性评估）.....	74
1. 项目名称	74
2. 项目预算	74
3. 项目目标	74
4. 项目内容	74
5. 项目工期	74
6. 项目需求	75
6.1 需求内容	75
6.2 服务清单	75
6.3 项目成果交付	75
6.4 测评方案	76
7. 服务要求	81
8. 服务保障	82

采购需求书

一、项目名称：中国（三亚）跨境电子商务综合试验区线上综合服务平台

二、项目预算：¥1029.8578 万元，其中 A 包系统开发与集成：833.0425 万元，B 包硬件设备与网络安全：161.5345 万元，C 包项目监理：15.2808 万元，D 包网络安全等级保护测评：8.0 万元，E 包商用密码安全性评估：12.0 万元。

三、项目地点：采购人指定地点。

四、资金来源：财政资金。

五、合同履行期限

A 包：从合同签订至项目验收的实施计划周期为 8 个月。

B 包：自合同生效之日起 50 天内交付。

C 包：从合同签订之日起到所监理的项目验收后止（本项目计划工期为施工合同签订后 8 月内完成），并在规定的项目质量保修期限内，负责检查项目质量状况，组织鉴定质量问题责任，督促责任单位。

D 包：达到测评实施条件后，自用户通知进场后 60 个工作日内。

E 包：下达测评通知书后 90 天内交付项目成果

A 包（系统开发与集成）

说明：未经采购人同意，供应商不得向与此项目无关的任何第三方透露采购需求技术内容部分。

注：加 ★ 号条款为必须满足条款，否则响应将被拒绝。

一、项目名称

中国（三亚）跨境电子商务综合试验区线上综合服务平台 A 包-系统开发与集成

二、建设工期

本项目从合同签订至项目验收的实施计划周期为 8 个月。

三、项目概况

1. 项目背景

2020 年 5 月 6 日发布《国务院关于同意在雄安新区等 46 个城市和地区设立跨境电子商务综合试验区的批复》（国函〔2020〕47 号），国务院同意三亚设立跨境电商综试区。2021 年 7 月 9 日，国务院办公厅发布了《国务院办公厅关于加快发展外贸新业态新模式的意见》（国办发〔2021〕24 号），意见指出，新业态新模式是我国外贸发展的有生力量，也是国际贸易发展的重要趋势。加快发展外贸新业态新模式，有利于推动贸易高质量发展，培育参与国际经济合作和竞争新优势，对于服务构建新发展格局具有重要作用。为深入贯彻党中央、国务院决策部署，促进外贸新业态新模式健康持续创新发展，经国务院同意，提出了相关意见。其中在扎实推进跨境电子商务综合试验区建设方面，要求扩大跨境电子商务综合试验区试点范围。积极开展先

行先试,进一步完善跨境电商线上综合服务和线下产业园区“两平台”及信息共享、金融服务、智能物流、电商诚信、统计监测、风险防控等监管和服务“六体系”,探索更多的好经验好做法。鼓励跨境电商平台、经营者、配套服务商等各类主体做大做强,加快自主品牌培育。建立综试区考核评估和退出机制,2021年组织开展考核评估。到2025年,综试区建设取得显著成效,建成一批要素集聚、主体多元、服务专业的跨境电商线下产业园区,形成各具特色的发展格局,成为引领跨境电商发展的创新集群。

根据《海南省人民政府办公厅关于印发中国（三亚）跨境电子商务综合试验区实施方案的通知》（琼府办函〔2020〕207号）文件精神,建设三亚电子商务线上综合服务平台,依托电子口岸,按照“一点接入”原则,建立跨境电子商务统一的数据标准和认证体系,为在三亚综试区开展业务的跨境电子商务交易企业、跨境电子商务平台企业、跨境支付企业、跨境物流企业等主体提供“关”“税”“汇”“商”“物”“融”一站式服务。对接海关、商务、交通、税务、外汇、市场监管、居民身份核验等部门的数据服务平台,实现监管部门间信息互换、监管互认、执法互助,完善信息共享、智能物流、金融服务等服务功能,探索开展跨境电子商务全程在线数字化服务。

2. 建设目标

充分借鉴“六体系”两平台的成功经验,通过中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开发建设,构建三亚跨境电商发展的基础框架,扎实推进跨境电子商务综合试验区建设。以“六体系两平台”的成功经验为参考进行探索,建成一批要素集聚、主体多元、服务专业的跨境电商产业载体资源库和线上服务产品,形成具有三亚特色的新发展格局,为下一步的跨境电商发展打下坚实的基础。最终输出“六体系、一通道、一门户、一实验室”的服务成果。

3. 建设内容

根据“六体系、一通道、一门户、一实验室”的建设目标，本项目主要建设跨境六体系、通关支持、企业服务、跨境大数据实验室四大业务子平台和应用支撑子平台。

（1）跨境六体系子平台：建设统计监测、信息共享、电商信用、风险防控、金融服务和智能物流六大子系统；

（2）通关支持子平台：集成省跨境电商公共服务平台跨境电商通关申报功能，间接地为企业提供通关便利化，实现通关服务支持；

（3）企业服务子平台：建设综试区门户、政策管理、线上展会和人才培育等企业服务子系统；

（4）跨境大数据实验室：包含数据归集、接口改造、数据处理、数据仓库和数据质量管理等内容；

（5）应用支撑子平台：包含统一安全认证、智能搜索、建模工具、可视化服务和日志审计等功能。

四、功能需求

1 应用系统需求

1.1 跨境六体系子平台需求

跨境六体系子平台是建立以信息为基础、以信用为核心、以技术为支撑的跨境电子商务新型监管服务模式，实现跨境电子商务自由化、便利化、规范化发展。通过构建信息共享子系统、金融服务子系统、智能物流子系统、电商信用子系统、统计监测子系统、风险防控子系统共六大子系统，实现跨境电子商务信息流、资金流、货物流“三流合一”，建立以真实交易为基础的电商信用评价体系，对企业或商品实施分类分级监管，简化优化监管流程，并依托大数据的数据分析服

务，为企业提供金融、物流等供应链综合服务。

（一）统计监测子系统★

功能主要包括外贸态势洞察、跨境产业云图、跨境产业监测等，并支持移动端访问。

1. 外贸态势洞察

利用大数据统计技术，对获取的通关数据、物流数据、金融支付数据、电商平台数据等外贸全流程的数据进行统计分析，从数据、业务分析方面建立规范、完整、系统、科学的统计监测体系，提供数据分析，为政府监管部门及外贸企业提供各类数据分析及决策依据。

2. 跨境产业云图

跨境产业云图包括产业链图谱、产业发展态势、产业链分析、产业地图、产业布局和园区产业分析五个功能模块。

3. 跨境产业监测

针对三亚重点企业群体及招商目标企业依托互联网和政务内部数据进行数据采集和综合分析。

（二）信息共享子系统

通过统一信息标准规范、信息管理服务，建立多位一体的跨境电商信息合作机制和共享平台，打通“关”、“税”、“汇”、“物”、“商”、“融”之间的信息壁垒，实现监管部门、地方政府、金融机构、电子商务企业、物流企业之间的信息整合，为跨境电子商务信息流、资金流、物流“三流合一”提供数据技术支撑。功能包括信息共享规范、数据交换共享与区、园区考核。

（三）电商信用子系统

电商信用主要是利用大数据技术对汇聚的各类信用数据进行分类和分析，制定统一的信用数据规则规范，设计出一套标准、通用、全面的数据字典，以此为基础，构建一套先进、成熟、权威的信用评价体系与模型，并对信用评价指标进行管理，主要功能包括信用评价、

信用管理、跨境用信等功能。

1. 信用评价★

利用大数据技术对汇集的各类信用数据进行分类和分析，制定统一的信用数据规则规范，设计标准、通用、全面的数据字典，建成电商信用基础数据库与信用模型，并对信用评价指标进行管理。

主要包括电商信用基础数据库，信用模型建设和信用评价指标管理。

（1）电商信用基础数据库

根据信用模型需求，梳理归集信用评价所需的数据，形成电商信用基础数据库。

（2）信用评价模型建设

三亚市跨境电商信用评级模型需充分借鉴国际权威的多维信用评价体系及经验，结合我国电子商务行业的实际情况，针对性的构建一套为科学的、合理的信用评价模型。

（3）信用评价指标管理

通过采集企业的业务数据，以及在各政府部门的政务数据和第三方社会服务机构平台所产生的数据。对企业各方面的信息进行全方位的收集并整理成相应的模型原始指标。功能包括评价指标维度管理、评价指标管理和评价指标计算。

（4）企业信用评价

信用评价分为评价任务设置和企业信用评价两部分功能。

2. 信用管理

实现对企业信用的管理，同时对信用的动态变化进行监控，对企业信用的负面清单进行预警。

包括信用信息管理、信用动态监控服务和企业信用负面清单服务等。

3. 跨境用信

贸易企业被评估后，信用的应用至关重要，意味着数据被调用的政府、事业单位、综合服务企业、贸易企业的认可与应用宽度。

（四）风险防控子系统

通过对国内外跨境最新资讯、WTO（世界贸易组织）/TBT（技术性贸易壁垒协定）通报和相关跨境舆情的分析，对跨境电商进行风险防控建设。主要功能包括多国资讯通报分析、跨境舆情监控与发布、企业画像与分类以及风险预警与消息订阅。

（五）金融服务子系统

以“破解企业融资难融资贵”为建设目标，推动提升金融服务实体经济质效；高效归集政务企业信息、金融机构产品供给、企业需求三类信息，开发核心金融服务平台应用，最终提供形成覆盖广泛、功能完备、产品丰富、过程监管的金融产品服务；对高信用评价的跨境电商企业在融资贷款、投保及结算等方面给予便利、优惠和扶持，通过整合优势资源及政策支持，促进跨境电子商务的持续健康发展。功能包括金融商城门户、外贸企业融资服务、金融机构信贷服务以及政府机构管理服务。

（六）智能物流子系统

系统对物流机构进行管理，物流机构登记跨境相关物流产品供跨境电商企业比选，跨境电商企业可对物流产品进行评价，为其他电商企业选择物流产品做参考，解决跨境电商物流成本高、效率低的问题。

1.2 通关支持子平台需求

为方便企业正常开展跨境电商业务，向企业提供包含基础管理、跨境电商进口、跨境电商出口等方面的通关服务支撑，支持跨境电商企业、跨境电商平台企业和物流企业、支付企业、报关代理企业、监管场所经营人等服务商通过该系统进行企业登记、订单、运单、支付单、清单、退货单、电子税单、收款单、出口清单等各类电子单据进

行全面管理和查询。

通关支持子平台通过系统集成方式实现用户集成、应用集成和数据集成。主要包括平台应用集成、基础数据集成以及通关数据集成等功能。

1.3 企业服务子平台需求

（一）综试区门户

综试区门户建设为用户提供综试区介绍、跨境电商政策解读、信息公示等资讯服务功能，集成政策兑现申报、综试区公共服务、跨境电商业务办理、在线客服、线上展会、人才培育等业务服务于一体，以提高三亚综试区的知名度，多种方式展示三亚跨境电商的特点与多元成长。同时为满足门户内容可调整要求，门户部分内容编排需实现可配置化

（二）政策管理

建设跨境政策的在线申报平台，实现三亚综试区的跨境相关政策的管理、发布以及企业自主申报等功能，及时对跨境企业进行政策补助和扶持。

（三）线上展会

为优质三亚企业及品牌产品提供对外中英文双语版宣传渠道，并迎合大促活动做整体推广营销。

（四）人才培育

通过线上调研、线下活动、云课堂等方式为本综试区培养跨境人才。

1.4 跨境大数据实验室需求

跨境大数据实验室子平台功能模块包括数据归集、接口改造、数据处理、数据仓库和数据质量管理等

（一）数据归集

主要对政务类数据、市场类数据、外贸类数据进行采集，政务类数据通过标准接口按有关流程进行归集，外贸类数据通过数据接口方式进行归集，市场类数据通过数据文件导入方式进行归集。

（二）数据处理

归集的数据需要进行数据处理，数据处理包括数据抽取、数据清洗、数据转换和加工等，能够支持全量和增量的数据抽取，支持基于规则和多种算法的数据清洗和转换，支持调度任务方式进行定期自动化数据处理，支持处理过程的日志记录，支持调度任务的监控等。

（三）数据仓库

数据仓库将根据实际需求进行分层设计，通过数据归集、数据治理、数据分析和主题库建设，实现数据组织、存储和管理，为平台层和应用层提供数据服务。

（四）数据质量管理

数据治理管控体系以行业数据标准与规范为依据，以数据管控组织与策略为支撑，以元数据管理系统、数据质量管理系统和数据审计管理系统为工具与手段，对数据资源从模型设计到共享服务全生命周期进行过程管控。

2. 应用支撑子平台需求

（一）应用站点管理

应用站点管理将中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开发的应用授权给各区、各园区，通过简单的向导式配置，快速完成新站点建立。

应用站点提供在统一门户的基础上，利用个性化页面实现应用站点千人千面，主要包括站点模板管理、站点管理、组件管理和站点门户维护。

（二）企业便利化备案

为了方便企业办理事前备案，设计企业便利化备案功能。主要包括企业备案与备案审核。

1. 备案申请

（1）企业备案申请

企业在平台中填写企业情况登记表，并提供佐证材料。

（2）备案材料检查

平台自动对企业提供的资料进行检查，对不符合要求或者缺失的佐证材料进行提醒。

2. 备案审核

企业填写备案申请后，由相关部门进行审核。

（三）统一安全认证

平台构建一套统一的安全认证体系，将中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开发的身份认证体系与海关侧以及省跨境电商公共服务平台等身份认证体系进行对接融合。

统一安全认证包含认证中心、用户中心、权限中心、身份集成、认证安全五个方面。

（四）智能搜索★

智能搜索平台对数据平台上的所有数据进行统一索引处理，提供类“百度化”的搜索功能，并按分类主题对数据进行详细展示，帮助用户高效便捷地访问数据平台中的所有数据。

智能搜索平台主要由首页门户、摘要页、详情页三个层级以及后台配置四部分组成。

1. 智能搜索门户

智能搜索门户是搜索的入口页面，在此页面完成首次搜索的输入功能。

（1）搜索主题

紧密贴合用户需求，按照业务域对所有搜索资源进行维度划分，所分维度显示于搜索框之上。每个维度又设计若干主题，用户在每个维度下，自定义配置主题，进而支持用户按主题进行数据检索。另外，搜索平台也会对各主题搜索频度进行统计排行，对搜索频度高的主题，通过“常用”模块呈现于搜索框之上。

（2）智能搜索框

支持用户选中主题后，自动计算出该主题下的搜索信息条数，方便用于及时获取信息总量；另外，搜索首页所呈现的维度和主题，均可根据用户需要进行灵活、可视化的自定义配置。

（3）全文搜索

智能搜索框所具备的搜索能力要求如下：

- 单个的中文字/词、英文字/词、阿拉伯数字及相关短语；
- 空格分隔的两个及以上的中文字/词、英文字/词、阿拉伯数字及相关短语。
- 逗号分隔的两个及以上的中文字/词、英文字/词、阿拉伯数字及相关短语。
- 单击精确可切换为模糊查询，默认为精确查询。

2. 摘要信息展示

摘要结果显示页展示搜索到的多条信息。每条信息涵盖标题部分和摘要部分，点击标题部分进入该信息的详情信息。同时支持所显示字段在后台系统中的自定义配置。

（1）分组统计

针对枚举类型的字段，支持按搜索结果条数进行分类统计。

（2）搜索结果排序

支持“按关联度排序”、“按时间顺序”、“按时间逆序”等多种搜索结果排列方式。所排序字段可在后台系统进行配置。

（3）取词搜索

支持用鼠标在搜索结果中选中若干个词，然后按所选词进行重新搜索。

（4）展示分页

当搜索结果数较多且无法在一页中显示全部信息时，对所搜索到的摘要信息进行分页显示。

（5）条件过滤

- 支持对搜索结果进行二次筛选，二次筛选支持如下操作：
- 按字段关系（与、或）进行多个字段过滤；
- 字段名称过滤；
- 按字段关系（等于、包含）进行多个字段过滤；
- 单过滤条件进行过滤；
- 多过滤条件进行过滤。

（6）导出

- 支持对所搜索的摘要结果保存为本地文件。
- 导出字段可在后台系统中默认配置；
- 导出字段可以在导出时再做选择；
- 导出文件格式支持 csv、txt、excel 等。

（7）关联搜索

支持在关联数据表中，对搜索关键字段展开关联搜索，并自动统计出所关联信息条数。

3. 详情信息展示

智能搜索详情页是搜索平台的核心内容，支持从多个维度、以多种可视化方式，展现被搜索对象的详情信息、统计结果、分析研判以及关联关系等。

详情页实现对所搜索对象的全方位信息展现。所显示模块由表单形式、表格形式和图形式构成。支持后台对显示方式、显示内容、显示格式的自定义配置，同时支持数据字段超链接配置。

（1）基本信息

搜索对象基本信息通常展现搜索对象的基本属性，维度对象的基本信息可根据实际情况，进行自定义配置。

（2）详情信息

详情信息是基本信息的补充和完善，由顶部标题、左侧页面导航、多个显示项目组成。详情页由后台系统进行配置，可为详情页配置多个显示项目，显示项目的显示方式主要分为表单形式、表格形式和图形式。可以配置每个显示字段的数据显示格式和超链接。

（3）关联关系分析

智能搜索系统会对搜索对象进行关联关系分析，并以八爪图的方式，直观显示多类相关信息，每条相关信息既可以信息统计的方式进行展现，也可进一步下钻为新的详情展示页面。

（4）信息钻取

智能搜索详情页支持信息的进一步钻取，钻取使信息的获取面更广、更深。钻取既可下钻至对象某属性的详细表格，也可下钻至其他主题对象。

（5）可视化展现

分为列表展示与图表展示两种方式，并支持数据联动分析展示。

4. 搜索后台配置

搜索系统后台管理的主要功能是把不同系统的数据汇总到搜索系统，提供统一的搜索和展示功能。

（1）数据注册

数据注册是搜索和展示的基础。数据注册的目的是把不同系统中的数据接入到搜索系统中，并按照搜索系统的要求完成对表结构的配置。

搜索系统支持 mysql、oracle、impala、ads、gbase 等关系型数据库系统数据的接入。

（2）主题分类配置

支持对一级主题、二级主题分类和名称的自定义配置。

（3）展示块配置

搜索系统中，每一个详情展示页称作看板，看板中的每一个展示部分称作展示块。支持对各展示块进行配置。

（4）看板配置

每一个详情页称为看板，看板由多个展示块拖拽布局而成，包括新建看板、添加展示块、导航配置、过滤条件配置、级联配置、八爪图配置、保存看板、详情页关联等功能。

（五）建模工具★

数据建模工具基于数据底盘库，支持数据建模分析、统计分析、挖掘分析、趋势分析等，实现基于业务分析的可视化建模。结合实际的业务场景，通过在画布中对相关组件进行拖拽和关联等。

建模工具主要分为组件区、工作区、属性区三部分，主要功能有：

- 支持选择需要分析的数据源（数据源的具体内容包括选择表、选择字段）。
- 支持选择数据处理工具对数据进行加工分析，如数据分组、数据过滤等。
- 支持选择数据可视化工具对模型运行结果进行展示，如列表，图形展示。

1. 模型管理

（1）模型维护

实现模型的说明维护以及模型逻辑设计等功能。

（2）复制模型

支持复制模型功能，选择需要复制的模型，支持从当前模型新建模型，弹出复制模型弹出框，复制后修改复制模型界面信息完成复制。

（3）运行模型

支持对模型的运行功能，对所建的模型进行运行和调试。

（4）运行节点

支持对模型的节点运行，节点运行可查看当前节点的字段内容。

（5）成为正式模型

创建的模型点击成为正式模型后，成为正式应用。可对正式模型进行权限设置，包括可二次开发及不可二次开发。

2. 支撑组件

（1）数据源组件

数据源组件支持系统数据和我的数据两种选择。

（2）数据处理组件

数据处理包括数据加工、数据滤重、数据过滤、数据分组、数据排序、数据查询界限定义等组件。

（3）机器学习

支持多种机器学习算法，包括 K 均值聚类、SVM 支持向量机、随机森林、决策树、关联规则等。

（4）统计分析

支持多种统计分析算法，包括正态检验、全表统计、直方图统计、方差、协方差、求和等算法。

（5）数据可视化

支持拖动列表、图形到模型可视化工作台区域，配置模型结果数据的输出，支持进入输出列表格式配置，勾选字段显示在结果列表中。

（六）可视化服务

可视化服务能够通过可视化配置，实现从数据源、建模到输出到可视化布局，是一整套面向用户的数据全景展示工具。平台提供丰富的可视化模板，多种图表组件，支撑多种数据类型的分析展示的数据展示大屏，通过零编程实现用户数据展示目标。包括多源数据接入、

多场景模板、多图标组件、拖拽式配置及应用在线分享等功能。

（七）日志审计

对于平台内部所有操作和运行情况记录日志信息，并提供日志的查询、下载和统计分析功能。日志类型包括调度日志、登录日志、操作日志等功能。

五、非功能需求

1. 信息交换与共享需求

通过集成省跨境电商公共服务平台，实现企业跨境电商单证申报服务协同。实现 1210、9610、9710、9810 这四种海关监管方式代码对应的申报功能。通过省数据共享平台实现与其他省级平台之间的信息交换，丰富数据采集来源。根据行业主管部门管理的要求，为企业提供其他申报入口。

1.1 总体需求

信息的交换与共享性：通过接口标准、数据链路及设定规则要求实现交换和共享。

信息的准确性：信息的数字化、加载、管理、查询、发布及统计分析结果应是准确可信的。

处理速度：要保证更新信息的及时获取、处理、入库与发布。

查询速度要求：由于系统的信息量大，并且信息的增长速度快，须有合理的数据存储结构和检索算法，以保证终端使用的响应速度。

1.2 信息交换需求

实现政务、企业数据接入，数据传输通道上支持通过省级平台实现与海关的跨境电商总署统一版进行数据交互。根据业务场景需求，

通过数据交换节点实现政务数据以及海关数据的交互。

（1）满足政务数据接入需求

实现政务部门的各类数据接入，为六体系建设及相关服务提供数据支撑。

（2）满足企业数据接入需求

需满足跨境电商行业各类市场主体按综试区管理要求接入数据的需求，以便能正常纳统和申领奖补等，同时也有利于三亚履行属地管理的职责。

（3）满足政务云和分中心独立业务专区之间的信息交换需求

需在政务云平台 and 分中心独立业务专区之间建立数据交换的通道。

（4）满足分中心独立业务专区与关务数据之间的信息交换需求

需在分中心独立业务专区建立数据交换节点，实现关务数据的信息交换。

1.3 信息共享需求

同跨境六体系服务的信息共享体系的需求描述，通过平台的长期建设，逐步实现监管部门、地方政府、金融机构、电子商务企业、物流企业等主体之间的信息互联互通，实现信息汇聚、加工处理、分析和应用。

2. 数据资源需求

2.1 数据应用需求

中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开发有三方面的数据应用需求，一是系统需采集跨境电商申报的电子单证、回执数据及企业对应的关务数据，如需实现与省跨境电商公共服

务平台、海关数据交换节点的对接；二是系统汇聚其他政府部门已有的企业信息和行政处罚等数据用于信用评估等应用；三是系统需采集外部第三方数据作为统计监测、信息评估等应用支撑，如省共享数据交换平台、省交通物流公共服务平台、省信用平台、省金融服务等平台进行对接。四是根据业务需求，由中标方适当采购其他第三方数据，丰富数据采集维度。

数据采集后，需进行过滤、清洗、转换、标准化等治理工作，形成数据仓库，为六体系和企业服务等应用提供基础数据支撑。

为支撑信用模型、统计监测等指标分析，全量数据或增量数据治理后，需根据指标计算周期进行各类指标预计算和预统计。

2.2 数据安全需求

为保障数据存储和应用安全，需实现：

（1）应制定数据风险管理策略，对风险进行分级管理，持续监督风险管理状况，及时预警，将风险控制在可接受水平；

（2）应建立健全各项管理与内控制度，从技术和管理等方面实施风险控制措施，监督、检查平台数据管理的各项规范、制度、标准和流程的执行情况以及风险管理状况；

（3）应建立健全数据管理工作的规章制度，确保数据可用、完整、安全、保密。

2.3 数据交换共享需求

中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开发需通过建立统一数据接口标准的方式，构建元数据资源库；同时为更好适应外部系统特点，制定个性化的数据采集策略与外部系统进行适配，具体的标准和方案可在确定系统承建方后，通过实地调研和收集其他部门需求后再做设计，目前暂无其他部门需求。需实现综试区

政务云端和省级平台之间的数据交换，需实现政务云端和海关端之间的数据交换，需实现海关端与数据分中心专网之间的数据交换。

2.4 大数据应用需求

系统采集企业主体的多维度数据，包括结构化与非结构化数据，经过加工处理和特征挖掘，为企业画像应用、统计监测等提供支撑。

3. 系统部署需求

本次项目部署分为海关端和政务云端，海关端部署跨境大数据实验室相关的应用和支撑数据库，政务云端部署六体系相关应用和支撑数据库。另外，在海关端与政务云端分别部署数据交换节点服务器实现两端数据互通。从而实现综试区政务云端和省级平台之间的数据交换，政务云端和海关端之间的数据交换以及海关端与数据分中心专网之间的数据交换。

注：海关端的服务器为国产自主可控品牌

4. 系统集成需求

系统需集成省跨境电商公共服务平台的用户体系、应用功能和数据体系，同时需与省共享数据交换平台、省交通物流公共服务平台、省信用平台、省金融服务等平台进行数据集成。

5. 运维服务需求

为保障系统的正常有效运行，需提供常态化的持续运维服务。在项目终验后提供2年售后服务、运维服务和产品升级服务。

6. 性能需求

中国（三亚）跨境电子商务综合试验区线上综合服务平台系统开

发软件需满足以下性能要求：

- （1）平台并发峰值为 2000，日常平均并发访问为 200 以下；
- （2）平台应可以满足日处理 50 万单的峰值要求；
- （3）页面响应速度，在合理网络和平台配置情况下，访问操作性界面的响应时间应小于 7 秒，静态页面响应时间应小于 2 秒，简单查询页面应小于 3 秒，复杂查询页面应小于 15 秒。

六、其他要求

1. 项目组织管理要求

响应人应充分考虑满足投标项目的建设要求，提出完整的项目管理、项目实施、项目验收、售后服务方案。

响应人应本着认真负责的态度组织项目团队，提供项目组主要成员名单。根据对项目的理解制定项目的人员配置管理计划，包括组织结构、项目负责人和技术负责人、组成人员及分工职责。拟担任项目团队技术负责人需具有系统分析师证书。

响应人需为本项目构建稳定的不少于 20 人的技术服务团队，提供近三个月社保证明。

2. 项目实施要求

本项目从合同签订至项目验收的实施计划周期为 8 个月。

本项目实施计划分 4 个阶段进行。请响应人根据阶段划分进一步细化成工作计划：

1. 设计阶段：要求中标单位自签订合同之日起 15 天内完成方案设计；
2. 开发阶段：要求中标单位自签订合同之日起，2 个月内完成六体系子平台及核心功能开发，并具备试运行条件；

3. 试运行及验收阶段：项目试运行 3 个月，试运行结束后 3 个月内，完成项目总结和最终验收；

4. 项目运维阶段：计划时长 24 个月，项目通过终验后开始，开展日常巡检、处理各类故障、修复软件 Bug 以及软件性能调优等工作，以保障项目安全稳定运行。

3. 人员培训要求

项目中标单位需要负责对相关技术人员进行全面的培训，通过对系统软件的性能、结构原理及维护管理技术和上网实际操作等培训内容，使之掌握用户系统配置、故障处理及日常维护，从而确保系统能正常安全的运行。

1. 培训对象：系统用户、系统管理员、运维人员等；
2. 培训内容：与本项目建设内容相关的全部内容；
3. 系统部分：按不同用户对象培训对应分配的功能操作；
4. 系统管理部分：系统授权、参数配置等相关内容；
5. 系统运维部分：培训系统部署、日常巡检、故障处理等相关内容。

4. 售后服务要求

据《计算机软件开发规范》(GB 8566-88)、《软件文档管理指南》(GB 8567-88)《计算机软件质量保证计划规范》(GB/T 12504-90)、《软件文档管理指南》(GB/T 16680-1996)和国家相关技术规范和质量标准及招标人需求进行验收。项目的工作内容及成果文档的提交至少应覆盖以下内容，电子文档是成果不可分割的部分。

项目技术档案包括但不限于：实施方案、需求规格说明书、概要设计说明书(包含系统体系结构图、业务流程图、数据流程图等)、详细设计说明书、数据字典、系统测试方案、项目实施报告、系统试运

行报告、培训计划、用户使用手册、管理员使用手册等内容。

B包（硬件设备与网络安全）

一、项目概况

1.1 项目名称

中国（三亚）跨境电子商务综合试验区线上综合服务平台 B包-硬件设备与网络安全

1.2 项目预算

项目预算：¥1615345.00 元

1.3 项目背景

三亚作为综试区建设的责任主体，将紧密围绕国务院、国家商务部及省政府对跨境电商综试区建设的工作要求，通过落实“六体系两平台”等成熟经验和做法，做好综试区的跨境电商发展基础框架搭建工作。同时按照国家对综试区考核评估的要求，以中国（三亚）跨境电子商务综合试验区线上综合服务平台为支撑，以数字化的贸易服务工具和方法为基础，以数据资产为核心，集聚全要素资源，同步开展三亚综试区在健全促进跨境电子商务发展的体制机制、推动配套支撑体系建设等方面取得新进展、新突破。

此次平台建设，是综试区建设关于信息化建地设的重要基础性和先导性工程，先解决从无到有的问题，不涉及各相关业务资源名称、主要内容、数量、类型、更新时间频率、覆盖范围等问题。发展跨境电商产业，首先需要完善基础设施，包含线下保税监管场所（非本项目建设内容）和线上综合服务平台；其次，需要培育市场主体，丰富服务商资源，完善产业生态环境，最后通过“六体系”建设，形成业务和数据的闭环，培植税源和业务，使三亚综试区的业务具备自生长

能力。

本项目包含海关端和政务云端，海关端计划部署在中国电子口岸数据中心海口分中心机房的独立业务专区，政务云端计划部署于省政务云机房。

二、采购内容

本项目计划采购 12 台服务器；分别用于部署数据库、大数据实验室、备份、存储等应用需求；6 台网络交换设备，用于满足应用的接入需求；9 套网络安全设备，分别用于网络安全，日志审计，动态感知等应用安全需求。

独立业务专区内部规划两个区域，分别是数据服务器区和安全管理局区，每个区域的有边界安全设备和网络交换机组成。

网络核心设备由两台核心交换机组成，提供高可靠的中枢网络系统，通过核心交换机的网络功能连接各个内外部区域，旁挂一台 SSL VPN 设备，提供互联网接入独立业务专区进行维护。

数据服务器区：数据服务器区承载本项目的核心业务（主要是数据库），连接到两台接入交换机，由交换机连接到区域边界的防火墙，防火墙配置了带 IPS 和 AV 功能许可，并部署安全终端管理软件，实现数据服务器区的安全保障。

安全管理区：由安全管理设备（堡垒机、数据库审计、日志审计、态势感知平台）、网络接入设备（一台连接安全管理设备的交换机）和区域边界安全设备（防火墙）组成，整个安全管理区为海关端独立业务专区平台提供集中的安全管理服务。

依据《海南省政务信息化项目建设管理实施细则（暂行）》新建项目网络安全设计包括安全管理制度建设、入网安全评估、等级保护测评（由 D 包实现）、渗透测试、安全加固、代码审计等安全内容；依据《网络安全法》要求，网络运营者应当制定网络安全事件应急预

案，定期演练。

2 条 100M 通信运营商数据链路专线和 1 条 10M 互联网宽带。

三、采购清单

此次项目的采购清单如下：

软硬件采购清单

序号	名称	单位	数量
1	服务器设备清单		
1.1	DB 服务器	台	6
1.2	数据备份服务器	台	1
1.3	数据存储服务器	台	1
1.4	数据共享服务器	台	2
1.5	大数据实验室服务器	台	2
	小计 1		12
2	网络设备清单		
2.1	核心交换机（核心交换区）	台	2
2.2	交换机（核心业务区）	台	2
2.3	交换机（安全管理区）	台	1
2.4	带外管理交换机	台	1
	小计 2		6
3	安全设备清单		
3.1	核心业务区防火墙	台	2
3.2	数据库审计	台	1
3.3	堡垒机	台	1
3.4	日志审计	台	1
3.5	态势感知平台（安全管	套	1

	理中心)		
3.6	安全管理区防火墙	台	1
3.7	终端安全管理系统	套	1
3.8	SSL VPN 网关	台	1
	小计 3		9
	合计		27

网络安全服务采购清单

序号	服务内容		
	名称	服务所针对的系统的个数（个）	服务期限
1	安全代码审计服务	1 个三级系统（综合服务平台 拟定第三级）	1 次
2	安全管理制度建设服务	单位整体网络安全工作	1 次
3	网络安全等级保护加固服务	1 个三级系统（综合服务平台 拟定第三级）	1 次
4	安全渗透测试评估服务	1 个三级系统（综合服务平台 拟定第三级）	1 次
5	入网安全评估服务	1 个三级系统（综合服务平台 拟定第三级）	1 次
6	应急演练服务	1 个三级系统（综合服务平台 拟定第三级）	1 次

通信运营商数据专线和互联网宽带采购清单

序号	名称	要求

1	通信运营商数据链路专线服务	共 2 条，每条 100M 带宽，满足本项目建设周期内的通信需求
2	互联网宽带服务	10M 互联网出口，满足本项目建设周期内的通信需求

四、技术参数要求

4.1 服务器技术要求

名称	技术指标要求	单位	数量
DB 服务器	<ol style="list-style-type: none"> 1. 国产自主可控品牌； 2. CPU: ≥ 2 个国产 x86 架构处理器, 单处理器基准主频≥ 2.5GHz 且≥ 16核, L3 缓存≥ 32MB, 最大支持双路 64 线程； 3. 内存: ≥ 256Gb DDR4 内存； 4. 硬盘: ≥ 4 块 1.2T SAS 硬盘； 5. RAID 卡: 支持 RAID 0/1/5/6/10/50/60； 6. 网卡: ≥ 2 个千兆 RJ45 以太网口, ≥ 1 个专用的管理端口； 7. 电源: 1+1 冗余电源； 8. 原厂服务: 要求设备厂商提供免费现场安装调试服务, 3 年原厂质保服务, 3 年硬盘免回收服务, 3 年免费上门服务。 9. 服务器需预装国产服务器操作系统; 操作系统支持文件管理、用户帐户管理、用户组管理、系统设备管理、系统日志管理、硬盘管理、资源管理, 应用程序和进程健康管理, 系统服务管理, 系统修复工具, 网络管理, 软件包管理等功能; 支持国密算法、可信计算; 支持在线升级服务, 操作系统含三年维保。 	台	6

<p>数据备份服务器</p>	<ol style="list-style-type: none"> 1. 国产自主可控品牌； 2. CPU: ≥ 1 个国产 x86 架构处理器, 单处理器基准主频$\geq 2.5\text{GHz}$ 且≥ 16 核, L3 缓存$\geq 32\text{MB}$, 最大支持双路 64 线程； 3. 内存: $\geq 64\text{Gb}$ DDR4 内存； 4. 硬盘: ≥ 2 块 600G SAS 硬盘, 4 块 4T STAT 硬盘； 5. RAID 卡: 支持 RAID 0/1/5/6/10/50/60； 6. 网卡: ≥ 2 个千兆 RJ45 以太网口, ≥ 1 个专用的管理端口； 7. 电源: 1+1 冗余电源； 8. 原厂服务: 要求设备厂商提供免费现场安装调试服务, 3 年原厂质保服务, 3 年硬盘免回收服务, 3 年免费上门服务。 9. 服务器需预装国产服务器操作系统; 操作系统支持文件管理、用户帐户管理、用户组管理、系统设备管理、系统日志管理、硬盘管理、资源管理, 应用程序和进程健康管理, 系统服务管理, 系统修复工具, 网络管理, 软件包管理等功能; 支持国密算法、可信计算; 支持在线升级服务, 操作系统含三年维保。 	<p>台</p>	<p>1</p>
----------------	---	----------	----------

<p>数据存储服务器</p>	<ol style="list-style-type: none"> 1. 国产自主可控品牌; 2. CPU: ≥ 2 个国产 x86 架构处理器, 单处理器基准主频$\geq 3.0\text{GHz}$ 且≥ 8 核, L3 缓存$\geq 16\text{MB}$, 最大支持双路 32 线程; 或≥ 1 个国产 x86 架构处理器, 单处理器基准主频$\geq 2.5\text{GHz}$ 且≥ 16 核, L3 缓存$\geq 32\text{MB}$, 最大支持双路 64 线程; 3. 内存: $\geq 64\text{Gb}$ DDR4 内存; 4. 硬盘: ≥ 2 块 600G SAS 硬盘, 4 块 4T STAT 硬盘; 5. RAID 卡: 支持 RAID 0/1/5/6/10/50/60; 6. 网卡: ≥ 2 个千兆 RJ45 以太网口, ≥ 1 个专用的管理端口; 7. 电源: 1+1 冗余电源; 8. 原厂服务: 要求设备厂商提供免费现场安装调试服务, 3 年原厂质保服务, 3 年硬盘免回收服务, 3 年免费上门服务。 9. 服务器需预装国产服务器操作系统; 操作系统支持文件管理、用户帐户管理、用户组管理、系统设备管理、系统日志管理、硬盘管理、资源管理, 应用程序和进程健康管理, 系统服务管理, 系统修复工具, 网络管理, 软件包管理等功能; 支持国密算法、可信计算; 支持在线升级服务, 操作系统含三年维保。 	<p>台</p>	<p>1</p>
----------------	---	----------	----------

<p>数据共享服务器</p>	<ol style="list-style-type: none"> 1. 国产自主可控品牌； 2. CPU：≥2 个国产 x86 架构处理器，单处理器基准主频≥2.5GHz 且≥16 核，L3 缓存≥32MB，最大支持双路 64 线程； 3. 内存：≥256Gb DDR4 内存； 4. 硬盘：≥4 块 1.2T SAS 硬盘； 5. RAID 卡：支持 RAID 0/1/5/6/10/50/60； 6. 网卡：≥2 个千兆 RJ45 以太网口，≥1 个专用的管理端口； 7. 电源：1+1 冗余电源； 8. 原厂服务：要求设备厂商提供免费现场安装调试服务，3 年原厂质保服务，3 年硬盘免回收服务，3 年免费上门服务。 9. 服务器需预装国产服务器操作系统；操作系统支持文件管理、用户帐户管理、用户组管理、系统设备管理、系统日志管理、硬盘管理、资源管理，应用程序和进程健康管理，系统服务管理，系统修复工具，网络管理，软件包管理等功能；支持国密算法、可信计算；支持在线升级服务，操作系统含三年维保。 	<p>台</p>	<p>2</p>
----------------	--	----------	----------

<p>大数据实验室服务器</p>	<ol style="list-style-type: none"> 1. 国产自主可控品牌； 2. CPU：≥2 个国产 x86 架构处理器，单处理器基准主频≥2.5GHz 且≥16 核，L3 缓存≥32MB，最大支持双路 64 线程； 3. 内存：≥256Gb DDR4 内存； 4. 硬盘：≥4 块 1.2T SAS 硬盘； 5. RAID 卡：支持 RAID 0/1/5/6/10/50/60； 6. 网卡：≥2 个千兆 RJ45 以太网口，≥1 个专用的管理端口； 7. 电源：1+1 冗余电源； 8. 原厂服务：要求设备厂商提供免费现场安装调试服务，3 年原厂质保服务，3 年硬盘免回收服务，3 年免费上门服务。 9. 服务器需预装国产服务器操作系统；操作系统支持文件管理、用户帐户管理、用户组管理、系统设备管理、系统日志管理、硬盘管理、资源管理，应用程序和进程健康管理，系统服务管理，系统修复工具，网络管理，软件包管理等功能；支持国密算法、可信计算；支持在线升级服务，操作系统含三年维保。 	<p>台</p>	<p>2</p>
------------------	--	----------	----------

4.2 网络设备技术要求

名称	技术指标要求	单位	数量
----	--------	----	----

核心交换机	<ol style="list-style-type: none"> 1. 配置≥ 20个 1000M 电口,≥ 4个 1G 光口,≥ 4个 10G 光口; 2. 配置交换容量≥ 750Gbps, 转发性能≥ 200MPPS; 3. 支持三层路由交换功能, 支持 VXLAN、支持 VRRP 等; 4. 每台配置≥ 4个 SFP+ 万兆模块 (850nm, 300m, LC); 5. 万兆光口可通过配置板卡, 扩容至 10 个; 6. 提供 3 年原厂质保服务。 	台	2
数据服务器区接入交换机	<ol style="list-style-type: none"> 1. 配置≥ 48个 1000M 电口,≥ 6个 10G 光口; 2. 配置交换容量≥ 500Gbps, 转发性能≥ 170MPPS; 3. 支持二层交换和叠堆等基本功能; 4. 配置≥ 2个 SFP+ 万兆模块 (850nm, 300m, LC); 5. 提供 3 年原厂质保服务。 	台	2
安全管理区接入交换机	<ol style="list-style-type: none"> 1. 配置≥ 24个 1000M 电口,≥ 4个 10G 光口; 2. 配置交换容量≥ 500Gbps, 转发性能≥ 100MPPS; 3. 支持二层交换和叠堆等基本功能; 4. 配置≥ 2个 SFP+ 万兆模块 (850nm, 300m, LC); 5. 提供 3 年原厂质保服务。 	台	1

带外管理交换机	1. 配置 ≥ 48 个100M电口， ≥ 4 个千兆光口，支持二层交换基本功能； 2. 提供3年原厂质保服务。	台	1
---------	---	---	---

4.3 安全设备技术要求

名称	技术指标要求	单位	数量
核心区防火墙	<p>1. 多核 CPU 硬件架构，网络层吞吐量$\geq 10\text{Gbps}$，IPsec 吞吐量$\geq 3.8\text{Gbps}$，防病毒吞吐量$\geq 2.5\text{Gbps}$，IPS 吞吐量$\geq 4\text{Gbps}$，最大并发连接数≥ 320万，每秒新建连接数≥ 9万，IPSec 隧道数≥ 1万个，最大 SSLVPN 用户数≥ 6000个；</p> <p>2. 1U 机架式，单电源，配置≥ 6个千兆电口（含一对 Bypass 接口），≥ 4个 SFP 光口（配置光模块），≥ 2个万兆 SFP+ 光口（配置光模块），≥ 1个 Console 口，≥ 1个 USB2.0 口，≥ 1个 HA 口，≥ 1个 MGT 口，≥ 1个 AUX 口，另支持≥ 2个通用接口扩展槽；</p> <p>3. 支持 NAT full cone 模式、NAT 的端口扩展技术，突破传统单个公网地址 64512 个端口的瓶颈。支持 NAT 地址可用性探测，支持 NAT 公网地址池中 IP 有效性检测，避免因 NAT 地址无法使用导致业务中断；</p> <p>4. 支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最</p>	台	2

近未命中天数等维度进行优化统计；支持基于国家地理位置、URL 等元素建立安全策略；

5. 具备对应用程序的识别和控制能力。应用程序特征库不少于 4000 种，并支持在线/手动更新；

6. 提供 8000 多种特征的攻击检测和防御，特征库支持网络实时更新，具备 4000 种以上 HTTP 特征库规则列表；

▲7. 支持与本项目态势感知平台的联动响应，可自动接收态势感知平台下发的拦截策略，并执行响应，可以快速自动阻断网络中的攻击威胁。（需提供产品功能界面截图，并加盖原厂公章）；

8. 配置 3 年病毒过滤、入侵防御、URL 分类库、流控 QoS 功能模块与特征库升级授权；提供 3 年硬件维保服务，应用识别库升级和软件升级维护服务；

▲9. 为保障产品自身安全性，产品须具有国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全测试证书》（要求提供资质证明文件，并加盖原厂公章）；

▲10. 为保障产品自身安全性，产品须具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》（要求提供资质证明

	<p>文件，并加盖原厂公章）；</p> <p>▲11. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（国家级）（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲12. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（APT 监测分析领域）（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲13. 为保障交付及运行效果，要求产品厂商具备软件服务商交付能力（四级）资质证书（要求提供资质证明文件，并加盖原厂公章）；</p> <p>14. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
<p>数据库 审计</p>	<p>1. 机架规格 1U，单电源，≥6 个千兆电口，≥1 个接口拓展插槽，≥2 个 USB 口，≥1 个 RJ-45 串口，可审计流量≥140M，入库速度≥6000 条/秒，日处理事件数≥8000 万条，硬盘容量≥2T，≥1 个监听口授权，≥3 个被审计 DB 服务数，3 年质保；</p> <p>2. 采用旁路方式部署，监听交换机镜像流量，对原有网络无影响，产品故障不影响被审计系统的正常运行；</p> <p>3. 支持 Oracle、SQL-Server、DB2、</p>	<p>台</p>	<p>1</p>

	<p>Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache 数据库审计；</p> <p>4. 支持国产数据库人大金仓、达梦、南大通用、神通、高斯数据库的审计；</p> <p>5. 支持支持双向审计，支持对 Select 操作返回行数和返回内容的审计；</p> <p>6. 支持对针对数据库的 XSS 攻击行为、SQL 注入攻击行为进行审计；</p> <p>7. 支持根据网络数据流自动建立数据库操作行为基线，对超出基线的操作可智能识别，并及时告警；</p> <p>8. 支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多 IP 登录、上下班操作量对比异常、操作响应时间分析。</p> <p>9. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
堡垒机	<p>1. 1U 机架式软硬一体设备，专用硬件平台和安全操作系统，≥6 个千兆电口，≥1 个 Console 管理口，存储容量≥1TB，单电源，带液晶面板，≥2 个扩展槽，≥800 路字符会话，≥200 路图形会话并发，≥100 点管理授权，含三年质保；</p> <p>2. 支持用户客户端 IP 和 MAC 限制，非法地址无法登录；</p> <p>3. 支持实现数据库命令级审计，支持的</p>	台	1

数据库类型包括：Oracle（支持 ORACLE RAC）、SQL Server、IBM DB2、Sybase、IBM Informix Dynamic Server、MySQL、PostgreSQL、teradata，不需采用数据镜像方式实现，以免增加部署的复杂性和网络负担；

4. 支持系统级账号三权分立，系统级账号包括：系统账号管理员，系统审计员，系统管理员；

5. RDP 协议支持 windows 服务端开启安全层 SSL 加密，加密级别符合 FIPS 标准，允许运行使用网络级别身份验证的远程桌面的计算机连接，以满足运维过程安全性的更高要求；

▲6. 支持扫描本地运维工具并进行配置保存，简化运维人员使用配置过程；（需提供产品功能界面截图，并加盖原厂公章）；

7. 支持 WEB 在线视频回放方式重现维护人员对服务器的所有操作过程；

8. 支持 web 页面防跳转功能，进行 http/https 访问过程中，运维人员仅允许访问授权地址；

▲9. 支持 C/S 客户端模式：提供 C/S 客户端功能，用于运维人员和管理员通过 C/S 客户端登录进行运维操作和管理操作，整个运维过程不依赖任何 Active 或

	<p>Java 控件；（需提供产品功能界面截图，并加盖原厂公章）；</p> <p>▲10. 产品具备 IPv6 Ready Logo 测试认证证书，（要求提供资质证明文件，并加盖原厂公章）；</p> <p>11. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
<p>日志审计</p>	<p>1. 1U 机架式千兆平台和安全操作系统，≥16G 内存，≥6 个千兆电口，双电源，存储容量≥2TB，授权≥110 个日志授权；</p> <p>2. 支持市面主流安全设备、网络设备、中间件、服务器、数据库、操作系统等设备对象的日志数据采集；</p> <p>3. Agent 至少支持采集日志监控、文件监控、包监控数据，支持控制采集时间、采集级别、采集范围、采集路径、采集名称、采集文件、多文件采集、采集编码格式、采集正则表达式、自定义采集等；</p> <p>4. 支持实时显示日志采集速度，无需人工统计；</p> <p>5. 支持关系图谱搜索、过滤，支持自定义关系节点图标、支持基于节点下钻查看日志信息、查看和拓展该点关系图等；</p> <p>6. 支持以世界地图和中国地图显示 IP 连接信息，显示 IP 地址地理位置，直观发</p>	<p>台</p>	<p>1</p>

现敏感外联日志；

7. 采用基于索引方式的日志存储和非关系型数据库的配置的存储架构，支持数据本地集中存储、本地离线备份存储、FTP 离线存储；

8. 支持日志数据冷热模式切换，即基于索引及时关闭和开启；

9. 提供 3 年设备原厂保修服务。

▲10. 为保障产品自身安全性，产品须具有国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全测试证书》（要求提供资质证明文件，并加盖原厂公章）；

▲11. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（国家级）（要求提供资质证明文件，并加盖原厂公章）；

▲12. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（APT 监测分析领域）（要求提供资质证明文件，并加盖原厂公章）；

▲13. 为保障交付及运行效果，要求产品厂商具备软件服务商交付能力（四级）资质证书（要求提供资质证明文件，并加盖原厂公章）；

14. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服

	务承诺函，并加盖原厂公章；		
态势感知平台 （安全管理中心）	<p>1. 一台态势感知一体机主机，一台全流量威胁检测探针，态势主机硬件配置： $\geq 2U$ 服务器、≥ 32 核、$\geq 256G$ 内存、$\geq 48T$ 存储、\geq 双千兆网卡、\geq 双万兆网卡、双电源，流量检测探针硬件配置：\geq 机架式 2U 服务器（含导轨）、≥ 8 核心 16 线程 CPU、$\geq 64GB$ 内存、\geq 双千兆管理电口、\geq 双千兆流量监听电口、\geq 双万兆流量监听光口、冗余电源、$\geq 600GB$ SAS 盘+2TB 企业级存储硬盘、≥ 4 个 USB 接口（至少 2 个 USB3.0 接口）；</p> <p>2. 支持 $\geq 1G$ 流量全流量威胁检测，$\geq 1000EPS$ 三方日志接入；</p> <p>3. 3 年态势感知一体机软硬件维保及规则更新服务，3 年威胁情报更新；</p> <p>4. 大数据处理：大数据处理模块，包含数据采集、数据解析、数据标准化、数据丰富化、数据存储、数据检索、数据计算、数据管理等功能；</p> <p>5. 基础检测分析：基础分析模块，包含情报分析、关联分析、威胁行为分析、ATT&CK 检测，XDR 关联分析；</p> <p>6. 基础安全运营：安全运营基础模块，包含安全态势、安全事件管理、ATT&CK 热力图、可视化 BI 分析、溯源取证、智能仪表盘、自动化报告、资产风险评估、</p>	套	1

安全信息库；

7. 全流量威胁检测：支持 1G 网络流量采集、协议识别、重组还原，内置威胁检测能力，可提供攻击检测、攻击成功检测、威胁情报检测等多种维度的威胁检测；

▲8. 支持基于不同数据源单独配置数据存储策略，提供数据存储冷、热分区，并可配置存储时间，提高数据查询性能，支持数据的自动备份，支持备份到 NFS、HDFS，支持使用数据压缩备份（要求提供产品功能界面截图，并加盖原厂公章）

▲9. 支持 Domain、IP、URL 等类型的威胁情报 IOC 关联检测，可根据情报 IOC 属性（威胁分值、可信度等）生成相关不同等级的告警（要求提供产品功能界面截图，并加盖原厂公章）

10. 支持双因子登录（Email 或短信），提高账号访问安全性

11 入围中央国家机关 2021 年安全软件协议供货。

▲12. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（国家级）（要求提供资质证明文件，并加盖原厂公章）；

▲13. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位

	<p>（APT 监测分析领域）（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲14. 为保障交付及运行效果，要求产品厂商具备软件服务商交付能力（四级）资质证书（要求提供资质证明文件，并加盖原厂公章）；</p> <p>15. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
<p>安全管理区防火墙</p>	<p>1. 多核 CPU 硬件架构，网络层吞吐量$\geq 4.5\text{Gbps}$，IPsec 吞吐量$\geq 1\text{Gbps}$，防病毒吞吐量$\geq 700\text{Mbps}$，IPS 吞吐量$\geq 1\text{Gbps}$，最大并发连接数≥ 100 万，每秒新建连接数≥ 2.6 万，IPSec 隧道数≥ 2000 个，最大 SSLVPN 用户数≥ 1000 个。</p> <p>2. 1U 机架式，单电源，标准配置≥ 5 个 10/100/1000M 自适应电口，≥ 4 个 GE/SFP 光电复用接口，≥ 1 个 Console 口，≥ 1 个 USB2.0 口；</p> <p>3. 支持 NAT full cone 模式、NAT 的端口扩展技术，突破传统单个公网地址 64512 个端口的瓶颈。支持 NAT 地址可用性探测，支持 NAT 公网地址池中 IP 有效性检测，避免因 NAT 地址无法使用导致业务中断；</p> <p>4. 支持策略命中分析，可基于命中数、首次命中时间、最近一次命中时间、最</p>	<p>台</p>	<p>1</p>

近未命中天数等维度进行优化统计；支持基于国家地理位置、URL 等元素建立安全策略；

5. 具备对应用程序的识别和控制能力。应用程序特征库不少于 4000 种，并支持在线/手动更新；

6. 提供 8000 多种特征的攻击检测和防御，特征库支持网络实时更新，具备 4000 种以上 HTTP 特征库规则列表；

▲7. 支持与本项目态势感知平台的联动响应，可自动接收态势感知平台下发的拦截策略，并执行响应，可以快速自动阻断网络中的攻击威胁。（需提供产品功能界面截图，并加盖原厂公章）；

8. 配置 3 年病毒过滤、入侵防御、URL 分类库、流控 QoS 功能模块与特征库升级授权；提供 3 年硬件维保服务，应用识别库升级和软件升级维护服务；

▲9. 为保障产品自身安全性，产品须具有国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全测试证书》（要求提供资质证明文件，并加盖原厂公章）；

▲10. 为保障产品自身安全性，产品须具有中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证证书》（要求提供资质证明

	<p>文件，并加盖原厂公章）；</p> <p>▲10. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（国家级）（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲11. 为保障产品厂商的安全服务能力，要求具备网络安全应急支撑服务单位（APT 监测分析领域）（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲12. 为保障交付及运行效果，要求产品厂商具备软件服务商交付能力（四级）资质证书（要求提供资质证明文件，并加盖原厂公章）；</p> <p>13. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
<p>终端安全管理 系统</p>	<p>1. 控制中心：终端安全管理系统软件基础组件，实现系统的集中管理、分组管理、消息推送、策略配置、报表查看等功能；</p> <p>2. 支持统计已停止更新服务操作系统的数量，并可查看操作系统终端详情，支持漏洞蓝屏修复功能，当安装系统补丁出现蓝屏时，可快速修复系统，支持系统核心进行加固，对内核攻击、子系统隔离、系统调用过滤、镜像攻击、内核隔离、内存检查保护、堆喷射、异常链</p>	<p>套</p>	<p>1</p>

	<p>进行防护，支持产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力；</p> <p>3. 提供三年维保升级服务；</p> <p>4. Linux 服务器客户端：30 点授权，针对 Linux 操作系统进行病毒查杀，支持 Linux 服务器病毒扫描及查杀，默认包含三年维保升级。</p> <p>5. 国产服务器客户端：30 点授权，针对国产操作系统进行病毒查杀，支持国产服务器病毒扫描及查杀，默认包含三年维保升级。</p> <p>▲6. 为保障交付及运行效果，要求产品厂商具备软件服务商交付能力（四级）资质证书（要求提供资质证明文件，并加盖原厂公章）；</p> <p>▲7. 具备公安部颁发的销售许可证，网络防病毒产品（要求提供资质证明文件，并加盖原厂公章）；</p> <p>8. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服务承诺函，并加盖原厂公章；</p>		
<p>SSL VPN 网关</p>	<p>1. 标准 1U 设备，双电源 400W-600W，2 核 2 线程 CPU X1，≥1T 硬盘，≥8G 内存；≥4 个千兆电口、≥2 个千兆光口，SSL 吞吐≥1.55G，≥3000 在线用户，≥5 个门户授权；</p>	<p>台</p>	<p>1</p>

2. 支持管理页面制作 RSA2048-SHA256、SM2-SM3 的 P10 请求；
3. 支持管理页面配置同一虚拟服务中同时使用 RSA2048 证书和 SM2 证书，根据 SSL Client Hello 数据包中自带的扩展项决定使用 RSA 或国密证书，保障 RSA 算法和国密算法切换不影响网络架构；
4. 支持 IPv4/IPv6 双协议栈；支持 IPv4/IPv6，IPv6/IPv4 协议转换；支持四、七层 SLB 及健康检查；支持 IPv6 动态路由；支持 IPv6 业务的高可用性及连接同步；
5. 支持证书快速解析功能 FAST CRL，提高 SSL 处理能力；
6. 支持通过 XML-RPC 接口实现与应用程序对接。支持通过 SOAP API 接口实现与应用程序对接。支持通过 REST FULL API 接口实现与应用程序对接；
7. 支持管理页面配置下载多个信任域 CRL，支持 ftp、http、ldap 方法下载 CRL，支持同一虚拟服务中配置多个信任域的 CRL；
8. 提供原厂商 3 年售后维保服务。
- ▲9. 产品具备商用密码产品证书，提供复印件并加盖厂家公章
10. 为保障产品质量和售后服务能力，需提供产品厂商产品授权函和三年售后服

	务承诺函，并加盖原厂公章；		
--	---------------	--	--

4.4 网络安全服务技术要求

序号	服务名称	服务内容	服务期限
1	安全代码审计服务	由精通安全漏洞原理、安全测试和软件开发等专业技术能力的资深安全专家，在项目建设单位授权范围内，使用专业自动化工具结合人工代码分析的方式对综试区平台应用程序代码进行检查，发现安全缺陷，并提供相应的补救建议的专业化服务。提供《安全代码审计报告》。	1次
2	安全管理制度建设服务	网络安全管理体系是一个系统化、程序化和文件化的管理体系，根据《中华人民共和国网络安全法》第二十一条国家实行网络安全等级保护制度。网络运营者应当按照网络等级保护制度的要求，履行下列安全保护义务，“制定内部安全管理制度和操作规程，确保网络安全负责人，落实网络安全保护责任”。安全管理制度建设服务应依据我国《网络安全等级保护基本要	1次

		求》（GB/T 22239-2019）标准规范，建立健全并落实符合相应等级要求的安全管理制度。提供《安全管理制度汇编》。	
3	网络安全等级保护加固服务	依据国家及行业信息安全等级保护的相关标准及法规的要求，从网络安全、主机安全、应用安全和数据安全的角度，结合多种技术手段为信息系统提供信息安全等级保护加固服务，逐步构建动态、完整、高效的信息安全技术体系，提高信息系统的整体技术防护能力，从整体上促进信息系统的安全稳定运行。提供《安全加固报告》。	1次
4	安全渗透测试评估服务	在项目建设单位授权范围内，参考 PTES (渗透测试执行标准) 对平台信息系统进行模拟攻击测试服务，用于帮助项目建设单位评估平台信息系统当前的安全性。提供测试包括外网渗透测试、内网渗透测试、黑盒测试、灰盒测试等，覆盖平台中包含的门户网站、服务器、数据库、中间件、网络设备、虚机等软硬件资产。提供《渗透测试报告》	1次
5	入网安全评估服	对平台进行入网安全检查和测	1次

	务	试，包括：网络安全架构检查、帐号安全检查、服务端口检查、防火墙策略检查、防病毒软件检查、系统日志安全检查、漏洞扫描检查、安全配置检查、弱口令检查。提供《入网安全评估服务报告》。	
6	应急演练服务	网络安全事件应急预案编制； 开展网络安全事件应急演练工作； 开展网络安全事件预防与应急技巧培训。提供《应用预案》和《应急演练报告》。	1次

4.5 链路技术要求

序号	名称	要求
1	通信运营商数据链路专线服务	共2条，每条100M带宽，满足本项目建设周期内的通信需求
2	互联网宽带服务	10M互联网出口，满足本项目建设周期内的通信需求

五、质保期

质保期：按照国家规定要求，具体条款采购合同自行拟定。

六、付款方式

合同生效后，采购人支付合同总额的 40%的预付款；设备到货签收后，采购人支付合同总额的 40%；项目初验后，采购人支付合同总额的 15%；项目终验后，采购人支付合同总额的 5% 。

C包（项目监理）

一、项目名称

中国（三亚）跨境电子商务综合试验区线上综合服务平台 C包-项目监理

二、监理工作任务及目标

受采购人委托，代表采购人的利益，了解用户业务目标和业务需求，依法对本项目的全过程进行监督管理。监理工作的目标是按照《国家政务信息化项目建设管理办法》、项目建设合同、国家和行业的信息技术标准、信息系统监理国标《信息技术服务监理 第一部分：总则》GB/T19668.1 以及相关分则开展监理工作。监理服务内容为对本次建设项目的设计、实施和验收阶段实施进行质量、进度、投资的控制，参与信息管理和合同管理，组织协调工作。

三、监理工作范围

● 硬件设备监理范围

监理必须对所有设备从采购、安装、调试、验收、试运行到竣工验收的全过程进行监督，并对设备验收和系统集成测试进行监督、审查。

● 软件系统监理范围

对系统软件及管理软件的到货验收、安装调试、验收全过程实施监理。

按照国家标准，对本项目的软件开发与集成进行监理，包括：审核软件开发方各阶段的开发文档，控制开发进度，验证开发内容与实际需求的一致性，控制开发方按标准进行开发。并协助采购人及软件项目中标人对应用软件进行阶段性测试。

四、项目监理总体要求

根据本项目及项目内各系统建设的特点，监理应全程开展以下工

作：

五控制：

质量控制—硬件设备采购进货、软件开发及测试和验收。

进度控制—采取总体项目进度管理方式，从整体协助业主进行项目推进管理；对每个分项进行甘特图管理，对每个分项之间交互界面进行控制衔接管理；及时对照进度计划进行进度分析，及时纠偏。

投资控制—硬件设备采购进货、软件开发投资及项目施工投资。

变更控制—施工过程中进行变更管理。

保密控制—建设过程中，全程人员、信息、系统的保密管理。

三管理：

合同管理—采购、施工、系统集成及软件开发等合同管理。

信息管理—投资控制管理、设备控制管理、施工管理及软件管理。

安全管理—项目的施工安全管理，系统的信息安全管理两部分。

一协调：

采用现场和会议方式进行协调，实施业主、承建方和监理的三方协调制度。

监理单位应按事前、事中和事后三过程开展监理工作。

①项目前期监理要求

协助业主和承建单位对项目需求和设计进行规范化的技术描述，为项目实施提供优化的设计方案；

协助并配合业主进行采购项目需求论证阶段工作的进行，使采购满足项目需求、符合相关的法律、法规和标准；

通过项目管理思路，建立整体项目计划，方案满足项目需求、符合相关的法律、法规和标准，并与项目建设合同相符，具有里程碑可验证性；

协助业主，审核承建方技术方案，满足项目整体需求，并与项目建设合同相符。

②项目中期监理要求

对项目实施方案进行详细审核，提出相关建议，确保其合法性、合理性、与设计方案的符合性；

对各子项目质量控制，确保项目中所使用的产品和服务、软件开发符合建设合同及国家相关法律、法规和标准；

监督项目实施过程，指定具有相关专业能力和资质的监理工程师驻场监理，确保满足建设合同的要求，并与项目设计方案、项目计划相符。

明确项目实施计划及进度，及时对计划进行调整，确保项目进度和整体进度相符合；

把握项目中投资、质量、进度的变更，规范项目变更流程；

对项目实施过程涉密部分，全程进行保密管理；

推动业主、各承建方之间的关系协调。

③项目后期监理要求

明确项目测试验收方案的符合性（验收目标、责任双方、验收提交清单、验收标准、验收方式、验收环境等）及可行性；

明确项目的最终功能和性能符合建设合同、法律、法规和标准的要求；协助业主进行各分项的验收工作；

保证承建单位提供的项目各阶段形成的技术、管理文档的内容和种类符合相关标准。

监理单位应针对质量控制、投资控制、进度控制、知识产权控制、信息安全控制、合同管理、文档管理和协调工作等方面提出详细监理规划并分别针对系统集成建设方面提出监理人员配备方案，并对项目相关的采购内容（软件等）进行监理。

五、监理具体要求

监理需要与总集和测评保持协调配合，并对以下监理需要负责的内容进行主导。监理工作包含但不限于以下内容：

①项目招标前期阶段监理工作内容

1. 方案控制

项目招标前期阶段的方案控制内容如下：

（1）监理单位应协助业主单位完成项目建设方案编制及建设方案的评审工作。

（2）监理单位应协助业主单位收集项目资料、整理归纳项目文档。

（3）监理单位应协助并配合业主进行采购项目需求论证阶段工作的进行，使采购满足项目需求、符合相关的法律、法规和标准；

②项目招标阶段监理工作内容

1. 质量控制

项目招标阶段的质量控制内容如下：

（1）监理单位应了解业主单位的业务需求，并将其作为监理工作的依据之一；

（2）监理单位应参与招标技术需求的编制；

（3）监理单位应对招标技术需求的下列内容提出监理意见（输出监理意见）：

a) 技术和质量的要求；

b) 项目所涉及的主要产品和服务的要求；

c) 投标单位资格的要求；

d) 验收方法、接受准则；

e) 时间进度的要求；

2. 进度控制

项目招标阶段的进度控制内容如下：

（1）监理单位参与业主单位招标前的准备工作，协助业主单位编制本项目的工作计划。工作计划应包含如下内容：

a) 项目建设内容；

- b) 组织管理；
- c) 项目建设的准备工作；
- d) 总包、分包方式；
- e) 项目建设的阶段划分及验收；
- f) 质量管理计划；

(2) 监理单位应分析项目的内容及过程，应对项目进度提出监理意见；

(3) 监理单位对招标书中项目进度安排及项目进度控制措施提出监理意见；

(4) 监理单位应对本阶段的工作进度提出监理意见；

(5) 监理单位应要求对项目合同中涉及的产品和服务的提供时间做出说明，并对业主单位的安排提出监理意见。

3. 投资控制

项目招标阶段的投资控制内容如下：

(1) 监理单位应协助业主单位对项目的目标、范围和功能进行界定，并确定项目的预算；

(2) 监理单位应协助业主单位根据项目预算，在招标技术需求中对项目的目标、范围、内容和产品及服务的技术要求做出明确说明。

4. 合同管理

项目招标阶段的合同管理内容如下：

(1) 监理单位应参与建设合同的签订过程，在建设合同中应明确要求承建单位接受监理机构的监理；

(2) 监理单位应建议业主单位在建设合同中明确规定项目所包含的功能、技术要求、测试标准、验收要求和质量责任；

(3) 监理单位应建议业主单位在建设合同中明确项目阶段划分及其质量和进度要求，并以此作为项目阶段性付款的依据。

5. 信息管理

项目招标阶段的信息管理内容如下：

（1）监理单位应与业主单位及相关单位建立信息沟通机制，保持各方对项目目标、范围和业务需求等理解的一致性；

（2）监理单位应向业主单位提供与项目建设有关的法律、法规和标准等信息；

（3）监理单位应妥善管理项目招标阶段所产生的与监理相关的文档资料，包括需求说明、招投标文件和监理文档等；

（4）监理单位应向业主单位和承建单位明确应提交的文档要求。

6. 项目招标阶段的协调

项目招标阶段的协调内容如下：

（1）监理单位应与业主单位确定相互间工作协调的机制；

（2）项目合同签订后，业主单位与承建单位有关项目的协调工作应通过监理单位进行。

③项目设计阶段监理工作内容

1. 质量控制

（1）监理单位应建议业主单位和承建单位充分考虑目标系统与现有系统的兼容性和互操作性；

（2）监理单位应审核设计文件与项目需求的符合性；项目关键技术的实现方法、流程及技术保障措施的合理性；项目实施的质量保证措施的可行性、合理性及其文档的完整性；

（3）监理单位应协助业主单位组织专业人员初审项目设计方案，审核后，签署监理审核意见。

2. 进度控制

（1）承建单位提交项目进度计划报审表后，应审核项目进度计划的可行性、合理性和各阶段工作成果的判定依据及其可操作性，审核后签署监理审核意见。

（2）监理单位应根据承建单位项目进度计划，确定阶段性进度监督、控制的措施及方法，作为监理细则的内容。

3. 投资控制

（1）监理单位应依据招投标文件、建设合同，审核项目计划、设计方案中所说明的建设目标、范围、内容、产品和服务，对可能的投资变化，向采购人提出监理意见；

（2）监理单位应控制设计变更，变更应由三方达成共识，并做备忘录。

4. 合同管理

（1）监理单位应及时处理采购人或承建单位合同变更的申请，协助保持合同、协议及其附件内容的实效性、一致性；

（2）监理单位应及时会同采购人和承建单位对合同的变更做备忘录。

5. 信息管理

（1）监理单位应与业主单位、承建单位建立信息沟通机制，并要求各方在项目工作中贯彻执行；

（2）监理单位应对设计阶段三方共同参与的过程和活动做项目备忘录并由三方签认；

（3）监理单位应要求业主单位和承建单位妥善保管有关的文档资料；

（4）监理单位应妥善保管项目设计阶段的文档，如项目计划、设计方案及监理文档，并监督检查项目文档的时效性和可用性；

（5）监理单位应对项目中各方提出保密要求的信息实施保密，尊重各方的知识产权。

6. 协调

（1）监理单位应与采购人、承建单位确定设计阶段的协调形式和方法，如监理例会和专题会议等，并在项目过程中执行；

（2）监理单位应协调采购人调动适当的资源，配合承建单位完成设计前期的调研工作；

（3）监理单位应对设计阶段出现的变更提出监理意见，协调采购人和承建单位达成一致；

（4）监理单位应对协调结果做备忘录。

④项目实施阶段监理工作内容

1. 质量控制

（1）监理单位应审核承建单位提交的质量管理计划申报表并签署意见；

（2）监理单位应组织采购人、承建单位召开项目实施准备会议，做出会议纪要，并经三方签认；

（3）监理单位应组织审核承建单位提交的实施方案从实施方案与法律、法规和标准的符合性；实施方案的合理性和可行性；实施方案与合同、设计方案和实施计划的符合性；项目实施的组织机构和人员配置是否满足项目建设需求等方面把关出具监理审核意见；

（4）监理单位对承建单位提供的产品及服务进行验收，对验收结果作出记录，并经三方签认；

（5）监理单位应检查承建单位项目实施状况、人员与实施方案的一致性；

（6）监理单位应执行阶段性质量监督和控制，并做监理日志；

（7）监理单位应及时处理承建单位提交的关键环节的 implementation 申请，审核其合理性后签认并报采购人批准；

（8）监理单位应审核项目变更申请，保证项目总体不受影响；

（9）监理单位应处理实施项目出现的各种质量事故；

（10）监理单位应在实施过程中，如发现存在重大质量隐患，应及时向承建单位签发停工令，并报采购人。

2. 进度控制

（1）监理单位应审核承建单位提交的项目实施计划的合理性及实施计划报审表，并签署审核意见；

（2）监理单位应审核承建单位提交的开工申请，并检查项目准备情况，签发开工令报采购人签认，通知承建单位开始实施项目；

（3）监理单位应审核承建单位提交的阶段性进度计划报审表；

（4）监理单位应定期检查项目的实施进度情况，确保实际进度与计划的一致性，并及时处理项目延期申请；

（5）监理单位应审查进度纠偏措施的合理性、可行性，签发监理通知单，报采购人，并要求承建单位按计划进行修改。

3. 投资控制

（1）监理单位应审核承建单位提交的项目阶段性报告和付款申请，签发项目款支付意见，报采购人签认；

（2）监理单位应审查项目的质量、进度和投资等方面的变更，并做项目备忘录；

（3）监理单位应及时处理各种索赔申请。

4. 合同管理

（1）监理单位应监督合同执行情况，定期向承建单位、采购人提交监理报告；

（2）监理单位应根据实际情况，参考变更文件及其他有关资料，按照建设合同的有关条款，对项目变更范围、内容、实施难度以及变更的投资和工期做出评估，处理项目实施中的各种变更并报采购人批准；

（3）监理单位应及时协调合同纠纷，公正地调查分析，提出监理意见。

5. 信息管理

（1）监理单位应妥善管理实施阶段中所产生的开工令、停工令、

监理通知、监理日志和项目备忘录等资料；

（2）监理单位应对项目实施阶段三方共同参与的过程和活动做项目备忘录，并由三方确认；

（3）监理单位应监督采购人和承建单位按照既定的要求编制和管理项目文档。

6. 协调

（1）监理单位应与采购人和承建单位共同建立实施阶段协调的机制；

（2）监理单位应及时组织专题会议，解决专项问题，做出会议纪要，并提交采购人和承建单位；

（3）监理单位应协调采购人和承建单位对项目变更的范围和内容等达成一致；

（4）监理单位应协调采购人和承建单位对索赔意见达成一致；

（5）监理单位应协调采购人配合承建单位的项目实施。

⑤项目验收阶段监理的工作内容

1. 质量控制

（1）监理单位应及时处理承建单位提交的初验申请，审核初验的必备条件，签认后报采购人签认；

（2）监理单位应协助采购人审核承建单位验收计划及方案，明确验收目标、各方责任、验收内容、验收标准、验收方式和验收结果等内容，审核后签署意见；

（3）监理单位应协助采购人对初验中发现的质量问题进行评估，并确定整改要求和验收方式；以监理通知单告知承建单位。必要时组织重验；

（4）监理单位应敦促承建单位根据整改要求提出整改方案，并监督整改过程；

（5）监理单位应与采购人和承建单位共同对初验结果进行确认，

并共同签署初验合格报告；

（6）监理单位应监督系统的试运行；敦促承建单位解决试运行出现的各种质量问题；

（7）监理单位应协助采购人组织项目验收；

（8）监理单位应对项目中的关键性技术指标，要求出承建单位出具第三方测试机构的测试报告，第三方测试机构应由采购人和监理单位同意；

（9）监理单位应参与本项目涉及软件的测试过程，与业主单位共同审核《测试方案》，要求开发人员不能参与测试自己开发的模块。要求承建单位实施单元测试、集成测试、确认测试和系统测试的完整过程，审核《测试报告》，抽查并验证部分测试结果，直到符合缺陷管理规定。

（10）监理单位应督促承建单位完成项目实施方案中确定的培训，并对培训进行评估。

2. 进度控制

（1）监理单位应对验收阶段进度安排提出监理意见；

（2）监理单位应审核承建单位初验、终验和项目整改计划的可行性，并以通知单的形式告知采购人和承建单位；

（3）监理单位应要求采购人和承建单位以初验合格报告作为启动试运行的依据，以终验报告作为项目验收结束的依据。

3. 投资控制

（1）监理单位应审核承建单位提交的阶段性付款申请，并根据合同规定签发项目支付意见；

（2）监理单位应协助采购人进行项目结算。

4. 合同管理

（1）监理单位应及时向采购人、承建单位通报建设合同、协议及相关变更所规定项目内容的执行情况，提出监理意见；

(2) 监理单位应协助采购人和承建单位签署其他补充协议。

5. 信息管理

(1) 监理单位应管理项目验收阶段文档；

(2) 监理单位应敦促采购人、承建单位按照事先约定，编制、签署和妥善保存验收阶段的项目文档；

(3) 监理单位应督促采购人、承建单位及时整理项目文档；

(4) 监理单位应整理与项目有关的全部监理文档，并提交采购人。

6. 协调

(1) 监理单位应协调采购人和承建单位在验收计划、验收目标、验收范围、验收内容、验收方法和验收标准等方面的一致性，填报项目备忘录，并经三方签认；

(2) 监理单位应协调采购人配合验收阶段的工作；

(3) 监理单位应及时填报验收阶段的项目备忘录，并经三方签认；

(4) 监理单位应协助采购人和承建单位完成项目移交工作。

六、交付成果要求

主要产出成果物：开工令、复工令、停工令、项目款支付证书、监理周报、各类会议纪要、监理月报、实施文档类监理审核意见、监理工作联系函、监理通知单、项目备忘录、监理记录、专项监理报告、阶段性项目总结、项目监理工作总结报告等。

七、售后服务要求

在规定的工程质量保修期限内，负责检查项目质量状况，组织鉴定质量问题责任，督促责任单位维修。

八、监理团队要求

要求监理单位具有较强的实力，并能统揽全局，能有效地组织、协调、监管项目实施过程中各方面的工作，使本项目质量达到一流水

平，工期得到保证，成本得到控制。

(1) 项目监理部须编制监理规划，应包含目标规划、动态控制措施、监理纪律守则和人员的定岗、职责等；根据建设方确定的项目分组情况，配置固定专门的监理人员。

(2) 参加项目的总监必须具备五年以上监理工作经验，并具有高级项目管理执业资格。

(3) 项目监理部及其人员需自行配备交通、通信、生活、办公、检测等设备、设施或仪表，以确保监理方案的顺利实施。

(4) 项目监理部须协助业主收集、整理、归纳项目资料，并且形成电子文档。

(5) 从事项目监理活动能遵循“守法、诚信、公正、科学”的准则。

(6) 监理单位应根据项目情况，制定适宜的表格来加强对设计、实施、验收的控制力度，包括但不限于如下方面：

- a) 针对关键环节，制定项目进度计划详表，在监理规划中报送；
- b) 监理周报、月报；
- c) 主要工作量记录表，在监理月报中报送；
- d) 安全情况记录表，在监理周报中报送；
- e) 其它现场验收表格。

九、商务要求

序号	内容	招标采购要求
1	服务期限	从合同签订之日起到所监理的项目验收后止(本项目计划工期为施工合同签订后 8 月内完成)，并在规定的项目质量保修期限内，负责检查项目质量状况，组织鉴定质量问题责任，督促责任单位。

2	履约、验收要求与标准	参照《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）的要求进行验收。
3	款项支付方式、进度	<ol style="list-style-type: none"> 1. 合同签订后 15 日内支付 50% 2. 所监理的项目初验合格后 15 日内支付 30% 3. 所监理的项目终验合格后 15 日内支付 20%

D包（网络安全等级保护测评）

一. 项目名称

中国（三亚）跨境电子商务综合试验区线上综合服务平台 D包-网络安全等级保护测评

二. 项目预算

项目预算：¥80000.00 元

三. 项目目标

通过委托专业的网络安全等级保护测评服务机构，对招标方的信息系统安全保护等级进行需求分析，并协助招标方完成等保备案相关事宜。依据《信息安全技术网络安全等级保护基本要求》

(GB/T22239-2019)、《信息安全技术网络安全等级保护测评要求》

(GB/T28448-2019)，对信息系统的物理机房、网络结构、应用系统、主机、网络及安全设备等进行合规性检查，分析信息系统与等级保护要求之间的差距，出具《网络安全等级保护测评报告》及相应的整改建议，提升信息系统的安全性。

四. 项目内容

1、对用户的信息系统进行摸底、分析和梳理，提出详细的测评方案及完成系统备案工作。

2、逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

(1) 安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心五个方面的安全测评；

(2) 安全管理测评：包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。

3、完成测评工作后，出具符合等保要求的网络安全保护等级测评报告，提出整改意见。

五. 项目工期

项目工期：达到测评实施条件后，自用户通知进场后 60 个工作日内。

六. 项目需求

6.1 需求内容

对信息系统的整体保护状况和信息系统组件，逐一进行安全等级保护测评，测评的内容包括但不限于以下内容：（1）安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评；（2）安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理、安全运维管理等五个方面的安全测评。

在完成信息系统安全等级保护测评后，针对等级测评过程发现的问题，依据信息系统安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）的规定，出具相应的网络安全整改建议书。

6.2 服务清单

序号	评估对象	系统等级	系统描述
1	中国（三亚）跨境电子商务综合试验区线上综合服务平台	三级	跨境六体系子平台是建立以信息为基础、以信用为核心、以技术为支撑的跨境电子商务新型监管服务模式，实现跨境电子商务自由化、便利化、规

序号	评估对象	系统等级	系统描述
	台		范化发展。

6.3 项目成果交付

中国（三亚）跨境电子商务综合试验区线上综合服务平台测评报告

6.4 测评方案

6.4.1 测评服务步骤

网络等级保护测评过程需按照《信息安全技术网络安全等级保护测评过程指南》（GB/T28449-2018）开展工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

6.4.2 测评准备活动

测评准备工作包括编制项目启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向用户提交《项目计划书》《提供资料清单》
	2. 编制《项目计划书》	
	3. 确定测评委托单位应提供的资料	

信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1. 整理调查表单	
	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
5. 分析调查		
工具和表单准备	1. 调试测评工具	确定测评工具（测评工具清单）《现场测评授权书》《测评结果记录表》《文档交接单》
	2. 模拟被测系统搭建测评环境	
	3. 模拟测评	
	4. 准备打印表单	

6.4.3 方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出成果
一、测评对象确认	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用	《测评方案》的测评对象部分

	确定测评对象	
二、测评指标确定	识别被测系统业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	选择对应等级的安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	确定工具测试的测评对象 选择测试路径 确定测试工具的接入点	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

6.4.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调，为现场测评的顺利开展打下良好基础，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、现场测评和结果记录、结果确认和资料归还三项主要任务。

详细要求见下表：

工作内容	工作详细任务	输出
1. 现场测评准备	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
2. 现场测评和结构记录	测评方案、结构记录表格等资料更新	访谈结果：技术安全和管理安全测评的测评结果记录或录音文档审查结果：管理安全测评的测评结果记录配置检查结果：技术安全测评的网络、主机、应用测评结果记录表格工具测试结果：技术安
	依据测评指导书实施测评	
	记录测评获取的证据、资料等信息	
3. 结果确认和资料归还	汇总测评记录，如果需要，实施补充测评	技术安全测评的网络、主机、应用测评结果记录表格工具测试结果：技术安
	召开现场测评结束会	
	测评委托单位确认测评	

	过程中获取的证据和资料的正确性，并签字认可	全测评的网络、主机、应用测评结果记录，工具测试完成后的电子输出记录，备份的测试结果文件 实地察看结果：技术安全测评的物理安全和管理安全测评结果记录 测评结果确认：现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件
	测评人员归还借阅的各种资料	

6.4.4 报告分析及编制活动

在现场测评工作结束后，应对现场测评获得的测评结果（或称测评证据）进行汇总分析，形成等级测评结论，并编制测评报告。

测评人员在初步判定单元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。

七. 服务要求

7.1 项目实施要求

项目实施过程中，投标人应遵循国家标准、行业标准。在项目实施中投标人须做到：

- (1) 本项目的项目经理必须具有 1 年以上的等保测评服务项目管理经验；其中，本项目成员中至少有 2 人具备信息安全等级保护中级测评师资格；

- (2) 提供完整的系统实施方案和项目实施管理办法；
- (3) 提供详细的项目实施方案和计划进度说明书；
- (4) 项目实施完成后提供可靠的后期技术服务工作；
- (5) 严格按照双方确定的计划进度保质保量完成工作；
- (6) 规范项目实施过程中的文档管理。

7.2 项目验收要求

中标人必须提供给业主详细的项目验收方案。

7.2.1 验收组织

成立由业主、中标人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

7.2.2 验收标准

- (1) 标准化：项目验收最关键的指标，应确保测评过程符合国家标准规范；
- (2) 系统稳定性：在测评过程中应确保软硬件环境的稳定性、运行正常；
- (3) 系统文档：验收文档是否齐全、规范、准确、详细；
- (4) 系统可操作性：交付成果清晰、通俗易懂。

7.3 售后服务要求

对于评估中发现的应用系统、主机和网络设备漏洞，投标方应提供项目验收后一年内的跟踪服务，对本次评估范围内的问题提供远程或现场技术咨询，对于漏洞的修补、问题的排除给出建议和指导。

E 包（商用密码安全性评估）

1. 项目名称

中国（三亚）跨境电子商务综合试验区线上综合服务平台 E 包-商用密码安全性评估

2. 项目预算

项目预算：¥120000.00 元

3. 项目目标

项目的总体目标是：依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，对中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统开展密评工作，通过密评工作深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为提升信息系统安全水平奠定基础，推动国产密码应用工作的进一步落实，保障和促进三亚市商务局信息化安全体系建设健康发展。同时，也指导三亚市商务局的信息安全保障体系建设，增强密码安全管理意识，促进安全管理水平的提高。

4. 项目内容

GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等方面对信息系统开展密码应用安全性评估工作，分析信息系统与基本要求之间的差距，出具《中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统密码应用安全性评估报告》，提出具有针对性的整改意见，并根据信息系统及安全防护措施的现状，提供其他安全服务，确保信息系统的安全运行。

5. 项目工期

项目工期：下达测评通知书后 90 天内交付项目成果

6. 项目需求

6.1 需求内容

1. 对中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统进行摸底、分析和梳理，提出详细的测评方案。

2. 针对中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统进行密码应用安全性评估，内容包括：物理和环境、网络和通信、设备和计算、应用和数据、安全管理等。

3. 完成密码应用安全性评估工作后，针对评估发现的问题，向三亚市商务局提交改进建议；三亚市商务局根据整改建议，对信息系统进行密码应用安全性整改，解决存在的问题。最后，根据系统中实际情况，出具测评报告。

4. 服务保障工作：评估报告提交 1 年内，围绕评估发现的问题和针对性改进建议，测评服务机构应向三亚市商务局免费提供咨询服务。

6.2 服务清单

序号	评估对象	系统等级	系统描述
1	中国（三亚） 跨境电子商务 综合试验区线 上综合服务平 台	三级	跨境六体系子平台是建立以信息为基础、以信用为核心、以技术为支撑的跨境电子商务新型监管服务模式，实现跨境电子商务自由化、便利化、规范化发展。

6.3 项目成果交付

1. 《中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统密码应用安全性评估测评方案》

2. 《中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统密码应用安全性评估报告》；

3. 《中国（三亚）跨境电子商务综合试验区线上综合服务平台项目信息系统密码应用安全性评估整改建议》；

4. 《中国（三亚）跨境电子商务综合试验区线上综合服务平台项目整体性的汇总报告》；

6.4 测评方案

按照商用密码应用安全性分类分级评估的要求，依据《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）要求及信息系统等级保护定级情况，进行评估，包括但不限于以下内容：

测评单元		测评指标	
技术要求	物理和环境安全	身份鉴别	a) 宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；
		电子门禁记录数据存储完整性	b) 宜采用密码技术保证电子门禁系统进出记录数据的存储完整性；
		视频监控记录数据存储完整性	c) 宜采用密码技术保证视频监控音像记录数据的存储完整性。
	网络和通信安全	身份鉴别	a) 应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；
		通信数据完整性	b) 宜采用密码技术保证通信过程中数据的完整性；
		通信过程中重要数据的机密性	c) 应采用密码技术保证通信过程中重要数据的机密性；

	网络边界访问控制信息的完整性	d) 宜采用密码技术保证网络边界访问控制信息的完整性；
	安全接入认证	e) 可采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。
设备和计算安全	身份鉴别	a) 应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；
	远程管理通道安全	b) 远程管理设备时，应采用密码技术建立安全的信息传输通道；
	系统资源访问控制信息完整性	c) 宜采用密码技术保证系统资源访问控制信息的完整性；
	重要信息资源安全标记完整性	d) 宜采用密码技术保证设备中的重要信息资源安全标记的完整性；
	日志记录完整性	e) 宜采用密码技术保证日志记录的完整性；
	重要可执行程序完整性、重要可执行程序来源真实性	f) 宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。
应用和数	身份鉴别	a) 应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的

	据安全		真实性；
		访问控制信息完整性	b) 宜采用密码技术保证信息系统应用的访问控制信息的完整性；
		重要信息资源安全标记完整性	c) 宜采用密码技术保证信息系统应用的重要信息资源安全标记的完整性；
		重要数据传输机密性	d) 应采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；
		重要数据存储机密性	e) 应采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；
		重要数据传输完整性	f) 宜采用密码技术保证信息系统应用的重要数据在传输过程中的完整性；
		重要数据存储完整性	g) 宜采用密码技术保证信息系统应用的重要数据在存储过程中的完整性；
		不可否认性	h) 在可能涉及法律责任认定的应用中，宜采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。
管理要求	管理制度	具备密码应用安全管理制度	a) 应具备密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；

	密钥管理规则	b) 应根据密码应用方案建立相应密钥管理规则；
	建立操作规程	c) 应对管理人员或操作人员执行的日常管理操作建立操作规程；
	定期修订安全管理制度	d) 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订；
	明确管理制度发布流程	e) 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；
	制度执行过程记录留存	f) 应具有密码应用操作规程的相关执行记录并妥善保存。
人员管理	了解并遵守密码相关法律法规和密码管理制度	a) 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度；
	建立密码应用岗位责任制度	b) 应建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限： 1) 根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位； 2) 对关键岗位建立多人共管机制； 3) 密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中

			<p>密钥管理员岗位不可与密码审计员、密码操作员等关键安全岗位兼任；</p> <p>4) 相关设备与系统的管理和使用账号不得多人共用。</p>
		建立上岗人员培训制度	c) 应建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能；
		定期进行安全岗位人员考核	d) 应定期对密码应用安全岗位人员进行考核；
		建立关键岗位人员保密制度和调离制度	e) 应建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。
建设运行		制定密码应用方案	a) 应依据密码相关标准和密码应用需求，制定密码应用方案；
		制定密钥安全管理策略	b) 应根据密码应用方案，确定系统涉及的密钥种类、体系及其生命周期环节，各环节安全管理要求参照《信息安全技术信息系统密码应用基本要求》附录 A；
		制定实施方案	c) 应按照应用方案实施建设；
		投入运行前进行密码应用安全性评估	d) 投入运行前应进行密码应用安全性评估，评估通过后系统方可正式运行；

		定期开展密码应用安全性评估及攻防对抗演习	e) 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。
应急处置		应急策略	a) 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置；
		事件处置	b) 事件发生后，应及时向信息系统主管部门进行报告；
		向有关主管部门上报处置情况	c) 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况。

7. 服务要求

评估项目实施过程中，投标人应遵循国家标准、行业标准。

1. 项目实施要求

在项目实施中投标方必须做到：

- (1) 提供项目实施组织架构；
- (2) 提供详细的项目实施方案和计划进度说明书；
- (3) 严格按照双方确定的计划进度保质保量完成工作；
- (4) 规范项目实施过程中的文档管理；
- (5) 项目实施中要引入风险管理、质量管理、成本管理；
- (6) 签署《保密协议》。

2. 评估实施团队要求

(1) 投标人须在投标文件中提供完整的评估实施团队名单及职责分工，所有实施人员必须属于投标人在册员工(提供 2021 年 1 月至今连续 3 个月社保缴纳证明为认定依据)，而且必须具备国家商用密

码应用安全性评估人员测评能力考核小组颁发的商用密码应用安全性评估服务人员测评能力考核证书，在项目实施期间持证上岗并接受查验，实施团队名单中所列人员的社保缴纳证明和商用密码应用安全性评估服务人员测评能力考核证书，复印件需在投标文件中提供，并加盖公章。

（2）按照国家密码管理局对商用密码应用安全性评估服务机构管理的规定和要求，评估项目现场实施的人员必须是本机构的商用密码应用安全性评估服务人员测评能力考核证书，而且测评项目不允许分包或转包，中标人一旦出现上述违规情况采购人有权解除合同并追究其法律责任。

3. 项目验收

投标人必须书面通知参加联合采购的采购人所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经参加联合采购的采购人认定后方可执行。

4. 验收组织

成立由参加联合采购的采购人以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

8. 服务保障

1. 供应商必须确保能建立一支具有一定服务能力的管理团队，并合理调配各岗位人员，保障服务工作相关岗位人员需要。
2. 中标单位从中国（三亚）跨境电子商务综合试验区线上综合服务平台项目进场之日起 5 个工作日内 要完成评估系统确定和测评方案编制。
3. 中标单位需在中国（三亚）跨境电子商务综合试验区线上综合服务平台项目验收之前完成并提交密码应用安全性评估报告。

4. 服务期间提供 7×24 服务响应，需要进行现场服务的，对设区城市主城区，技术人员能够在 2 小时之内到达现场处理；对县（城区），技术人员能够在 4 小时之内到达现场处理。
5. 服务期间提供应急保障工作，针对应急、攻坚克难等事宜提供保障方案，包括高层支撑和响应时间等。
6. 严守工作秘密。中标服务商必须与采购人签署保密协议，工作人员须与单位签署《保密承诺书》，对知悉的事项及信息予以保密，所有资料、技术文档妥善保管，不得遗失、转借、复印，不得以任何形式向第三方透露；所有密码应用解决方案和采集汇总后的数据严禁通过互联网等公共信息网络、普通邮政进行传递，严禁在连接互联网计算机上存储、处理。
7. 严格遵循操作规程，承担服务工作质量责任。

