采购需求

一、项目基本信息:

1、项目名称：省政务云数据安全及态势感知项目（项目编号：HNYH2020-20-0108）；

2、采购单位：海南省大数据管理局；

3、采购预算：¥1029.338 万元（大写：人民币壹仟零贰拾玖万叁仟叁佰捌拾元整）；

4、项目概况：本项目共分为 3 个标包，本次招标为 A、B、C 包，分包情况如下：

标包名称	标号编码	采购预算（万元）
A 包海南省电子政务外网网络及数据安全态势感知平台建设项目	HNYH2020-20-0108（A）	786.4
B 包海南省电子政务外网政务云密码服务平台建设项目	HNYH2020-20-0108（B）	218.8
C 包监理	HNYH2020-20-0108（C）	24.138

二、采购需求:

A 包采购需求：

（一）项目名称：A 包海南省电子政务外网网络及数据安全态势感知平台建设项目

（二）项目概述

2.1 概述

海南省大数据管理局负责统筹电子政务基础设施的建设和管理，同时承担大数据建设、管理和服务等职责，包括推进政府数据资源共享交换，推动公共服务大数据应用创新，完善大数据安全保障体系，建立大数据安全评估体系等。因此，海南大数据管理局需推动电子政务外网数据安全及态势感知项目的建设，来保证政务外网网络安全、政务云平台运行安全、政务数据安全使用。

2.2 项目建设目标

构建政务数据安全开放平台，对数据资产情况、数据流转、数据访问、数据态势进行全面的监管和控制，并进行可视化呈现；构建网络安全态势感知与安全运营平台、政务数据监管与安全开放平台，提升网络安全风险管控及态势感知能

力、安全事件响应及应急处置能力、用户网络与信息安全管理和分析水平，实现政务外网网络安全的整体感知和预警。通过面向业务的安全服务、面向数据的安全管控以及面向网络的态势感知，形成多层次、多维度相融合的电子政务外网平台安全防护、监管和感知能力，实现海南电子政务外网平台全时、全域、全维的网络安全保障能力，为海南电子政务外网平台的长远发展提供安全保障。

2.3 项目建设内容

项目建设主要通过构建网络安全态势感知与安全运营平台、政务数据监测监管与安全开放平台，为电子政务外网提供网络安全监管服务与数据安全使用服务，保证电子政务外网上业务安全、数据安全。

1. 构建网络安全态势感知和安全运营平台。通过汇聚海南省政务外网相关安全数据，如安全设备数据、日志数据、流量数据等，进行统一关联分析、交叉验证等态势研判，通过安全可视化技术进行综合态势、资产态势、威胁态势等多维度的态势呈现。

2. 构建政务数据监测监管平台。秉承“数据不动程序动”、“数据可用不可见”的安全理念，支持多种数据源，支持对数据访问权限严格控制，支持对所有数据操作留痕审计，支持行为风险分析和识别，具备数据访问申请与授权体系和输出结果申报与审核机制，实现数据所有权和使用权分离，确保数据安全可控。

2.4 采购需求清单

本次项目主要对海南省电子政务外网网络及数据安全态势感知平台建设相关软硬件产品、等保测评、培训服务和相关管理制度进行采购，具体清单如下：

序号	项目内容		
一	网络安全态势感知平台		数量（套）
1	数据采集系统-日志采集处理引擎	1、购买 2 套日志采集处理系统，覆盖电子政务外网区、互联网对外发布区； 2、支持日志获取、配置管理、日志泛化、插件管理、性能监控等功能，实现省级政务云日志采集与审计。	2
2	数据采集系统-流量采集分析引擎	1、购买 3 套流量采集分析系统，覆盖电子政务外网区、互联网对外发布区和办公用户互联网区。为满足对各委办厅局、地级市政府和政务云的流量采集，应配置不少于 19 台探针设备。 2、支持对流量进行深度解析识别，进而对各种应用协议进行深度内容还原。	3

3	数据采集系统-资产及漏洞探测引擎	支持网络扫描，自动发现在线网络资产，并自动对其操作系统、软件、服务等指纹信息进行识别；	1
4	大数据存储系统	用统一的分布式数据计算、存储、分析支撑，实现网络安全数据融合共享。实现对海量多源异构数据的统一处理及存储能力，实现按需进行计算资源扩展。	1
5	研判分析系统	支持对各类网络攻击、恶意代码、异常及违规行为等的综合研判分析，为安全管理决策提供数据支撑，从海量的日志和告警中甄别出真正的安全事件。	1
7	业务管理系统-态势感知管理功能	网络安全态势感知管理平台，提供资产管理、漏洞管理、风险管理、告警管理、威胁情报管理、应急管理、报表管理、系统管理等各类应用管理。	1
8	态势呈现系统	将平台综合研判分析的结果通过丰富的可视化方式进行呈现，提供多维度、多视图、多视角的安全态势展示、检索、查询和统计分析。	1
二	**政务数据监测监管平台**		
1	数据资产自动发现	支持敏感数据发现能力、数据资产自动化梳理能力、数据资产扫描能力、数据资产动态梳理能力、数据资产目录管理能力。	1
2	数据资产分级分类	支持数据分类分级管理功能、数据分类分级模型管理功能、数据分类发布功能、分类分级规则管理功能。	1
3	访问行为分析与鉴权	支持数据资产权限动态梳理功能、数据资产访问鉴权管理功能、智能化敏感数据监控功能、数据访问行为分析功能。	1
4	数据安全标签	支持数据安全标签管理，敏感数据全局唯一标识配置管理。	1
5	预警与响应	支持预警通报和响应处置。	1
6	数据安全态势感知	支持展示数据分布态势、数据流转态势、数据合规态势、数据访问权限态势。	1
三	**安全测评**		
1	安全测评	提供项目 2 年质保期内等保三级测评服务	1
四	**安全服务**		
1	电子政务	1.项目质保期内，提供驻场的电子政务外网网络安全监测和	1

	外网网络安全监测运营和平台安全服务	运营服务，包含 1 名项目运营经理，2 名威胁分析工程师，1 名漏洞验证工程师，1 名事件处置工程师；	
		2.项目质保期内，对平台提供配套的安全服务，包含全流量威胁分析服务、攻击者分析服务、攻防演练防守监测服务、渗透测试、安全加固、基线扫描等，协助将网络安全态势平台与政务数据监管平台运营，完善安全事件的处置闭环。	
		3.按需对网络安全态势感知平台和政务数据监测监管与态势感知平台提供渗透测试服务、安全加固服务、基线扫描服务。	
		4.对由海南省大数据管理局建设运营的基础性、公共性电子政务信息系统，提供 1 年的渗透测试服务、漏洞扫描、基线扫描等安全管控服务。	
		5. 对由海南省大数据管理局建设运营的基础性、公共性电子政务信息系统（包括：省一体化在线政务服务平台、省大数据公共服务平台、省数据共享交换平台、省互联网+监管系统、省工程建设项目审批管理系统、省业务中台等），按照采购人要求提供不少于 2 次的代码审计服务并提供审计报告。	
2	相关标准规范体系	提供电子政务外网安全管理规范编制服务	1
3	系统使用培训	为海南省、地级市和市县各级领导、业务管理人员、业务人员、维护人员提供所需要的业务管理类、技术类、操作类的培训。	1
4	质保服务	项目完成终验后，提供 2 年的质保服务	1

（三）项目要求

3.1技术参数要求

3.1.1部署要求

系统应结合实际业务需求和海南省电子政务外网现状进行部署。

1.在政务外网安全管理区部署安全态势感知管理端，在政务外网出口、互联网发布区和办公用户互联网区等处部署流量探针。

2.在电子政务外网区、互联网对外发布区部署网络安全态势感知系统日志采集处理系统对日志信息进行采集分析和处理。

3.在关键业务应用及数据库出部署数据治理插件。

3.1.2网络安全态势感知平台技术要求

1.平台总体上应满足《政务网络安全监测平台总体技术要求》（T/CIIA

005-2019），《政务网络安全监测平台数据总线结构规范》、政务网强安全监测业务服务规范等相关制度要求。

2.应支持按照《政务网络安全监测平台总体技术要求》（T/CIIA 005-2019）和中央级政务安全监测平台、以及地市级、政务云安全监测平台进行数据的级联对接，实现总体态势、告警日志、威胁情报、认证、报表等数据的级联对接。

3.1.2.1 部署范围要求（本项技术参数为实质性要求，投标人不满足视为无效投标）

网络安全态势感知平台应支持部署在电子政务外网安全管理域中，支持旁路部署，覆盖海南省政务外网、政务云及其上的政务应用，其中：

● 流量采集分析系统需覆盖级电子政务外网区、互联网对外发布区、办公用户互联网访问区的流量镜像数据，各区域情况说明及探针部署需求详见下表：

部署区域	节点名称	节点说明		预估流量	探针数（台）
办公用户互联网访问区	核心交换区	办公用户互联网访问区核心交换节点，下挂省委办公区、省政府办公区和海府办公区等办公园区		4Gbps	1
电子政务外网区	核心交换区	电子政务外网区核心交换节点		10Gbps	1
	云平台	云内部已经部署态势感知设备，本次需实现和云平台态势感知或安全监测系统的对接。	政务云 1	-	-
			政务云 2	-	-
			政务云 3	-	-
	地级市政府接入	共涉及海口市人民政府办公区、三亚市人民政府办公区、儋州市人民政府办公区 3 个节点和南海云、南海云都 2 个下级政务云节点，均作了 NAT，需在各市县 NAT 之前部署探针。	海口市政府	2Gbps	1
			儋州市政府	2Gbps	1
			三亚市政府	2Gbps	1
			儋州南海云都	2Gbps	1
			南海云	2Gbps	1
	省直单位接入接入	共涉及 11 个厅局节点，均作了 NAT，需在各厅局 NAT 之前部署探针。	民政厅	2Gbps	1
			财政厅	2Gbps	1
			交通厅	2Gbps	1
			省地税局	2Gbps	1
			水务厅	2Gbps	1
			人社厅	2Gbps	1

			省工商	2Gbps	1
			电教馆	2Gbps	1
			科技厅	2Gbps	1
			药监局	2Gbps	1
			国土环保厅	2Gbps	1
互联网对外发布区	核心交换区	互联网对外发布区核心交换节点		5Gbps	1
	云平台	云内部已经部署态势感知设备，本次需实现和云平台态势感知或安全监测系统的对接。	政务云 1	-	-
			政务云 2	-	-
			政务云 3	-	-
合计					19

● 日志采集处理系统需覆盖省级电子政务外网区、互联网对外发布区网络及安全设备的告警日志信息、应用系统的运行日志信息等；

● 资产信息采集系统需覆盖省级电子政务外网区、互联网对外发布区、办公用户互联网访问区网络及安全设备、应用系统服务器等信息资产。

3.1.2.2 部署硬件性能要求

3.1.2.2.1 流量采集分析系统性能要求

流量采集分析系统标准配置 1 个 10/100/1000M 专用管理接口，1 个 Console 口，4 个万兆光口，4 个 10/100/1000M 自适应电口，冗余电源，2 年全功能特征库升级服务，3 年维保。同时开启网络流量采集、威胁数据采集和日志上报功能情况下混合流吞吐量 10Gbps;HTTP 并发连接数 800 万;HTTP 新建连接速率 30 万/秒。

3.1.2.2.2 日志采集处理系统硬件要求

日志采集处理系统标准配置 4 个千兆电口，1 块 RAID 卡，32G 内存，冗余电源，8TB*3 块硬盘使用 RIAD5。日志源 IP 授权节点≥100 个，事件处理性能不低于 10000EPS，包含 3 年维保。

3.2.2.2.3 资产及漏洞探测引擎硬件要求

资产及漏洞探测引擎配置硬盘 1T 以及上，标准配置 6 个 10/100/1000M 自适应电口，2 个 SFP 插槽,2 个扩展插槽，冗余电源。Web 扫描任务并发数为≥25 个域名。系统扫描 IP 地址无限制，支持扫描 A 类、B 类、C 类地址，系统扫描支持≥150 个 IP 地址并行扫描。包含 2 年漏洞特征库升级，3 年维保。

3.1.2.3 数据采集系统

3.1.2.3.1 日志采集处理

日志采集方式。支持通过 Syslog、SNMP、OPSECLEA、NETFLOW、ODBC/JDBC、API、Agent、FTP、HTTP 等协议方式完成各种日志的收集功能；

支持插件代理主动采集日志。

日志支持类型。支持采集安全设备日志、网络设备日志、操作系统日志、数据库日志、中间件日志、应用系统日志和终端日志等；日志信息应支持告警信息、系统事件信息、原始日志、访问信息、状态信息、错误信息等。

日志归一化处理。支持对日志进行归一化处理为统一格式的指定类型数据输出，同时保留原始日志；支持通过可视化配置相关解析规则、过滤规则、富化规则、日志类型，实现过滤、丰富、分类日志信息；

日志分析处理。支持自定义预处理解析规则文件，可根据应用场景，通过配置选择插件、正则表达式、分隔符、Key-Value、JSON 等方法定义解析规则；支持各种主流安全事件的采集、解析，数据过滤和预处理，事件类型包括：访问控制、身份管理、身份认证、侦查、入侵攻击、拒绝服务攻击、恶意代码、恶意邮件、可疑行为、漏洞利用、系统、网络、设备、合规性等，能够有效支撑日志审计工作。

3.1.2.3.2 流量采集处理

支持利用深度包识别 DPI 和深度流识别 DFI 技术，对网络流量高速采集和解析，支持应用协议的全字段解析，包括 HTTP/SMTP/POP3/IMAP/FTP/TELNET/DNS/SSL/ SSH/RDP/Samba/ARP/SNMP 等协议；

支持对网络流量进行还原解析生成流量日志并进行采集；支持对网络传输文件的还原，支持按照文件类型、文件大小、应用协议等查询；

支持对原始 Pcap 数据包的全留存，支持按照应用协议下载，进行取证分析；

支持对入侵攻击、恶意代码、异常行为等检测，识别攻击、病毒、木马、勒索软件、Web 扫描、Webshell 后门访问、DDos、撞库攻击、SQL 注入、跨站脚本、命令执行等威胁。

支持 IPv6 协议流量数据采集；

3.1.2.3.3 资产及漏洞信息采集处理

支持通过网络流量和自动探测主动发现网络内主机设备、网络设备、安全设备、应用系统设备等资产信息进行采集，并自动对其操作系统、软件、服务、URL等指纹信息，以及资产漏洞信息、资产威胁信息进行采集识别。

支持以手动录入、批量导入、被动检测方式采集资产信息；

支持与业界知名漏扫引擎对接，实现对资产漏洞信息扫描采集，提供对应漏洞的修补建议及详细扫描报告。

支持对 IP、域名、资产、批量检测等目标的自定义扫描；

3.1.2.3.4 威胁情报信息采集处理

1. 支持威胁情报库、漏洞库的在线升级、手动升级、通过代理等安全可控方式在线升级。日常升级频率应不超过 24 小时，紧急情况要提供小时级更新。

2.支持本地采集多种类型的威胁情报，包含域名类威胁情报、IP 类威胁情报、文件类威胁情报、安全事件类威胁情报等类型。

3.应支持根据运营需要，导入自身或者其它相关方提供的威胁情报，导入的威胁情报支持通过统一的 API 接口查询使用。

4.应支持提供开放接口，以标准接口的方式来集成第三方威胁情报平台，接口返回数据应支持 JSON 格式。

5.应支持通过标准情报格式和传输标准和其它国家级、或者行业内情报平台进行数据情报共享。

6.应支持对已有的威胁情报增加自定义标记。支持自定义增加或删除威胁情报；可以对自定义的威胁情报状态进行管理，包括启用、禁用等。

7. 应支持按照 GB/T 36643-2018《信息安全技术网络安全威胁信息格式规范》标准或国际通用标准 STIX 2.0 等，对外进行情报共享和传输，可以和支持相应协议的设备进行互通。

8.支持通过查询接口、邮件等方式和上级平台的威胁情报进行比对，可以覆盖对僵尸网络、勒索软件、远控木马、窃密木马、黑市工具、恶意病毒等威胁类型情报的信息查询。

3.1.2.4 大数据存储系统

建立相应的流量数据、日志数据、告警数据、资产数据、资产漏洞数据、网

络威胁情报数据（包含病毒/木马、漏洞、安全事件、威胁情报等基础数据）、规则知识数据等数据库。

支持大数据存储相关算法模型库，包括关系型数据库、非关系型数据库、分布式索引存储、列存储引擎、图存储引擎、文本数据存储、二进制数据存储、内存缓存加速、分布式文件系统等。

支持对结构化数据、半结构化数据和非结构化数据进行存储，支持文本、关键值、对象等多种数据类型的存储，支持可伸缩的分布式数据存储架构，满足数据量持续增长需求。

支持分布式存储，按照使用场景对热数据和冷数据进行不同方式的存储。

支持数据迁移，支持存储数据的备份及异常恢复。

支持节点扩展，支持负载均衡。

数据存储时间按照网络安全法以及行业主管部门的规定来确定，其中操作日志数据存储时间不少于 6 个月。

支持高压缩比算法压缩，支持采用纠删码存储策略，在保障数据可靠性的前提下，降低数据存储冗余度。

3.1.2.5 研判分析系统

3.1.2.5.1 分析技术要求

支持通过机器学习、数据挖掘、关联分析等数据分析技术对政务网络的综合态势、攻击态势、威胁态势、资产态势、违规行为态势等进行分析，分析数据汇总至业务管理和态势呈现等模块；

机器学习算法应支持涵盖有监督与无监督学习模型，方法包括但不限于聚类分析和分类分析。

数据挖掘应支持从大量的数据中通过统计、在线分析处理、情报检索和模式识别等诸多方法，搜索隐藏于其中的信息。

关联分析应支持在分布式部署情况下提供不同大量复杂事件的关联分析。提供至少一百条预定义和自定义的关联规则，包括但不限于网络异常、暴力破解、账号异常等多种场景的规则，并支持预定义规则的更改。

沙箱分析应支持从分析文件类型，静态、动态方式描述，输出报告/检测结果；支持接收来自联动安全产品的可疑威胁对象，自动执行针对可疑文件及 URL

的分析检测。"

特征码匹配应支持将待检测内容与恶意流量特征、恶意文件特征、恶意代码特征等特征值进行匹配，然后根据匹配结果判断待检测的内容是否被感染。

支持场景化分析应支持基于关联分析技术提供丰富的场景化分析，包括但不限于：业务资产主动外连、异地账号登录、违规上传下载、弱口令等等。至少包括：

3.1.2.5.2 态势分析内容要求

支持综合态势分析，能够对网络的整体安全态势进行分析。

支持攻击态势分析，能够对来自网络内、外部的攻击行为进行分析。包括但不限于 APT 攻击、DDos 攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、SQL 注入、信息篡改、信息泄露、信息窃取等。

支持威胁态势分析，能够基于威胁情报进行威胁分析，包含对脆弱性分析。包括但不限于病毒、漏洞、蠕虫、木马程序、僵尸网络、恶意代码等；

支持利用威胁情报 IOC 对威胁进行实时检测，识别命令控制通信回联、恶意域名和 URL 的访问、高级持续性威胁等；

支持对 IP、域名、文件 Hash 等进行情报溯源，查询相关联的恶意样本信息、域名情报信息和 IP 情报信息等，并进行可视化呈现；

支持资产态势分析，能够针对资产的漏洞和配置弱点进行分析，自动计算出相关的风险指数。

支持按照单一资产和资产分组进行资产风险查询和展示，查询条件至少包括资产 IP 地址、资产名称、资产风险值、资产风险等级等维度。内容至少包含资产信息、漏洞信息、风险信息等字段；

支持图形化展示资产或资产分组告警及漏洞数量，可按照趋势、等级、处置状态等信息系进行展示；

支持违规行为分析，能够基于场景化分析等手段分析内部违规行为，包括但不限于访问频次超限、访问流量超限、文件外发、非法外联、非法访问、非法文件下载等。

支持对各类分析的数据和结论通过态势呈现系统进行展示。

3.1.2.6 业务管理系统

3.1.2.6.1 资产管理

支持对采集到的资产信息进行管理，能够将资产按照多种维度进行分组、分域管理，如设备类型、地理位置、组织结构、业务系统等，提供便捷的添加、修改、删除、查询与统计功能；

支持定期对资产信息和资产状态的变化进行扫描更新和记录；支持资产信息的批量导入和导出，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行赋值，自动计算资产价值，设置保护等级。

3.1.2.6.2 漏洞管理

支持导入主流第三方漏洞扫描报告，支持人工漏洞报告导入。

支持针对漏洞基本情况进行分析，获取漏洞的基本信息、受影响的资产和漏洞修复建议等，同时针对漏洞的影响情况进行综合评价，提供漏洞影响评分与评级。

支持提供用户人工验证漏洞信息能力。

支持通过 CVE 编号和 CNNVD 编号关联漏洞知识库中的信息；

3.1.2.6.3 风险管理

支持根据业务实际场景进行风险评估建模，针对资产风险、安全域风险、组织机构风险、业务系统风险等进行量化评估。

3.1.2.6.4 告警管理

支持对日志、安全事件、威胁情报等数据进行聚合、分析，实现基于告警来源、告警级别、受害主机等视角进行告警可视化展示。告警详情中支持：

提供基于“杀伤链”模型的可视化威胁告警统计图以及关联威胁日志统计功能；

能够关联并展示与该告警相关的原始日志、事件、资产、情报、漏洞等信息；能够提供攻击者和受害者信息，统计告警的发生次数和频率，能直观了解攻击发生的基本时间范围和影响。

3.1.2.6.5 报表管理

预置多种报表模板，覆盖范围包括：威胁态势、资产态势、漏洞态势、处置态势等。同时可按照业务要求，自定义事件范围、指标、维度、样式等参数配置

自定义报表；

支持 pdf、csv、word、HTML 等文件格式，对生成后的报表，可进行在线查看和下载，或者通过数据接口等方式进行下发和上报。

3.1.2.6.6 系统管理

支持提供自定义的安全预警指挥调度保障专项能力，能够针对博鳌重保、护网行动、全国两会等重要活动保障，提供重保工作平台，用于协调指挥相关的技术支持单位、安全人员、用户单位。

提供平台数据备份、升级更新、控制台等基本运维操作功能，可以对平台系统进行详细配置；

提供统一集中的用户管理，用户权限管理支持三权分立模式。

支持 RBAC，提供分组的增加、删除、修改、查询及权限分组管理，进行新增、编辑、删除操作时，需触发系统记录日志。

平台配置管理。支持对平台运行状态阈值的配置；支持对采集对象地址的配置；支持对平台参数的配置；支持对数据存储时间的配置；支持对账户和密码的配置，包括帐号锁定时间、密码有效周期、密码错误次数、密码最小长度、密码强度的配置等。

支持日志审计，系统应对用户的使用等操作行为应有完整的日志记录，便于审计跟踪和分析。系统应记录系统中发生的关键事件，包括审计内容和审计操作。系统应确保审计日志不可删改。审计内容包括：用户操作审计和系统事件审计。审计操作包括：审计查看、审计内容导出和审计内容统计。

支持对平台进行统一监控，配置专职人员对负责监测平台的运维管理；

支持平台运维人员实时获取服务器运行现状，包括不限于服务器名称、服务器 IP、CPU 使用率、内存使用情况、磁盘容量、系统性能监控过程中产生的异常事件告警。

3.1.2.6.7 通报处置管理

支持预警分级，将接收到的预警信息按照重要程度、影响范围等进行分级。

支持通过邮件、短信、企业微信等方式实现安全事件的预警通告。通告内容包括但不限于：告警名称、告警时间、告警类型、告警级别、告警对象、所属部门、告警描述等；

支持预警流程自定义，支持依照设定的流程发布信息通告。

支持可视化的预警流程、处置策略管理维护，协助安全分析人员进行规则和策略的开发和维护。

支持针对安全事件、漏洞、安全告警信息等进行工单任务创建与管理，包括工单新建、编辑、处置、以及工单统计概览。可以自定义工单流程，根据安全事件类型与级别进行工单流转，支持按照工单的接收时间、优先级、名称、类型和状态等条件查询工单的处置状态。工单任务完成后可以进行意见反馈，从工单完成效率，质量等方面进行任务评估。

根据网络安全事件威胁类型、威胁级别等要素判断是否启动自动处置流程，同时提供第三方事件响应平台、安全网关（防火墙、WEB 防火墙等）、服务器安全加固系统等标准接口，实现网络安全设备联动处置，协助网络安全态势感知平台进行应急处置工作。

3.1.2.6.8 系统接口建设管理

应支持通过 API 接口方式采集上报数据。平台数据接口应按照《政务网络安全监测平台数据总线结构规范》的要求进行建设和管理。

应采集下级平台上报的数据，包括但不限于总体态势、告警统计、风险状况、案例、重大安全事件、报表等信息。

应采集上级平台推送的数据，包括但不限于威胁情报、处置工单、案例、重大安全事件通告等信息。

支持上级平台的 GIS 地图页面调用。

3.1.2.7 态势呈现系统

3.1.2.7.1 综合态势

支持 B/S 结构，提供态势大屏入口，支持通过多种图形化的方式轮播呈现各安全态势专题及重要指标的情况，预置综合资产态势呈现、威胁态势呈现、漏洞态势呈现、综合态势、处置态势等模块；

综合安全态势呈现元素包括：网络资产情况、业务系统情况、流量情况、风险单位情况、风险单位 TOP5、风险资产情况、网络攻击阻断率、开放端口数、风险事件情况、威胁情况、告警类型等。

支持配置可视化基础支撑系统形成专项自定义态势；

支持根据决策者、管理人员和运维人员不同的需求和关注重点，进行多种态势的多维度展示；

支持在态势展示页面通过信息钻取查看安全事件的详情，可以多层钻取。

各页面加载时间小于 3 秒，各类检索操作返回时间小于 5 秒。

3.1.2.7.2 资产态势

支持按照不同的资产类别、地域、分组、风险级别、外联情况等维度实现资产态势呈现；

支持可视化地图实现海南全省地市县、各个所属行业的安全态势呈现；

3.1.2.7.3 威胁态势

支持可视化呈现内网中威胁告警和蔓延情况；

能够从攻击者维度和被攻击者维度提供对的攻击情况分析，对相关资产和资产组的风险、漏洞、威胁类型、等级、趋势、攻击手段等信息进行统计呈现。

3.1.2.7.4 处置态势

支持对预警、漏洞等通报处置任务进行全流程跟踪，结合预警处置各类型分布、时间趋势分布、区域、响应处理效率、最新预警处置处理进度等信息进行实时展现。

3.1.2.7.5 漏洞态势

支持统计展示全网漏洞类型分布情况、全网漏洞处置情况、漏洞级别分布情况等。

支持从资产类型、资产组、安全域等维度进行漏洞态势的呈现。具体包括：漏洞概要统计信息、高危漏洞监视、漏洞发现态势、漏洞总体安全态势、漏洞分布态势、漏洞数量趋势等内容。支持统计展示全网漏洞平均修复时间。

3.1.3政务数据监测监管平台技术要求

政务数据是海南省重要资产，政务数据的分布、流转需要完备的监管手段。需要在保证数据安全的前提下实现对数据价值进行充分挖掘，提升政务大数据价值。针对数据流转的每一个环节可能存在违规操作或者安全风险等行为进行检测和管控，需要对数据流转过程中涉及的各种行为进行全程的监管、安全态势呈现、协查取证分析、行为追溯等功能，保障政务数据使用安全。

3.1.3.1 部署方式需求

平台由控制中心和分布式代理两部分组成，其中：

控制中心包括敏感数据识别服务、数据安全标识服务、数据安全策略联动服务、数据安全态势感知服务和预警与响应服务五部分组成。

分布式安全代理支持云环境分布式部署，由异构数据源适配器、数据属性特征抽取、数据内容识别引擎、数据访问行为识别引擎和数据资产风险发现引擎 5 个部分组成。

3.1.3.2 部署范围要求

要求覆盖覆盖海南省政务外网、政务云及其上的政务应用，涉及到全省 89 家单位，750 个政务应用系统。

3.1.3.3 数据资产自动发现

支持从各种格式的数据中识别出敏感数据；应能够从结构化数据、半结构化和非结构化数据中识别出敏感数据。能够支持多种敏感数据识别模式，包括预定义模式、自定义模式、相似数据发现模式等。

支持在线和离线数据自动化梳理功能，支持基于规则和人工智能算法分析语义技术，对数据来源、存储位置、数据访问权限、数据格式类型等数据属性进行自动化分析和分类。

支持自动化采集敏感数据属性信息、数据梳理信息统计分析、敏感数据属性检索等功能。能够对敏感数据所分布的物理位置、逻辑位置（IP/数据库 / 表 / 列）、存储格式（结构化 / 非结构化）、状态、数据量、账号访问权限、用户权限变化、访问热点、安全防护措施等多维度属性信息进行自动化梳理。

提供网络扫描、数据流内容动态识别、分布式安全代理等多种数据资产动态发现、识别与资产注册功能。能够根据分类分级规则动态对网络流、数据库（Oracle、HIGH DB、SQL Server、Mysql、Elasticsearc、Greenplum、Libra MPP、HDFS、HBbase）所分布的各类数据资产进行自动化分类分级与数据资产登记注册服务。

提供数据资产目录自定义的添加、修改和删除功能，按照业务规则自动将发现的数据资产归并入特定目录节点。

3.1.3.4 数据资产分级分类

支持导入和自定义数据分类名称、数据分类规则、数据分类模型。

能够支持按照行业分类、主题分类、服务分类，根据数据内容的敏感程度、重要程度进行分级；内置经济管理、国土资源、财政、金融、外交和个人隐私等政务数据分类分级模型。

支持分级分类规则的创建和管理维护，支持定义分类名称、数据权限、分级、条件规则等属性；

支持数据分类发布审核，用户创建的数据分类需经过批准后才能被策略使用配置；

支持分类分级规则管理，可以提供数据分类分级配置管理、数据抽样、特征识别、数据分类分级构造和分类分级规则自动化生成等功能；

支持关键字、关键字排除、关键字对、词典模式检测；

支持正则表达式检测，支持通过自定义脚本对识别的敏感数据进行二次校验，提高内容识别准确率；

支持结构化数据指纹，支持指纹库管理；

支持非结构化数据指纹，能够依据指纹匹配的相似度进行响应，管理员可以对相似度进行设置和调整；

支持各种识别技术任意组合方式、支持出现属性方式、关键字、正则表达式最小出现次数、支持检测算法列外等。

3.1.3.5 访问行为分析与鉴权

支持数据资产权限动态梳理，具备数据资产访问途径跟踪、访问权限动态扫描和分析功能，可动态建立账号-业务-数据资产关联和访问权限模型，能够动态梳理敏感数据资产的访问权限、途径，动态追踪访问权限变化，建立重要区域、账号、业务系统、数据资产之间及访问权限关系清晰可见的全路径透视图。可精细化和细粒度地控制每个用户的实际权限，准确的为每个用户指定其可以访问的数据范围与权限。

支持根据数据资产访问权限动态梳理结果，制定权限控制策略功能，能够建立分布式数据资产访问权限控制机制，实现数据资产访问权限精细化和细粒度访问控制。

支持智能化敏感数据监控功能，能够对访问敏感业务数据及个人隐私数据的每一个访问语句提供智能化的安全监测功能，实时掌握数据资产的访问情况。

支持数据访问行为分析功能，能够对数据访问行为分析功能提供数据聚合分析、行为聚类分析、行为回归分析、行为模型构建、频繁模式挖掘、关联规则挖掘、事务特征分析、行为序列分析等，将低价值密度的原始数据加工为高价值密度的结果数据，通过数据访问行为识别引擎对外提供细粒度的数据访问行为分析服务。

3.1.3.6 数据安全标签

支持数据安全标签管理功能，能够提供数据安全标签属性定义、生成、绑定（单位/部门/角色/或用户）、修改、回收等数据安全标签管理等功能。

支持敏感数据全局唯一标识功能，能够为电子政务外网提供敏感数据流转监控和细粒度访问控制提供数据资产全局唯一标识，通过为敏感、高价值数据赋予数字安全标识，为敏感和高价值业务数据访问、流转通过细粒度强制存储控制安全机制。

支持敏感数据标签对应实体分页显示，支持根据标识、描述、状态查找实体。

支持基于深度学习的 OCR 技术对图片中的文字信息进行识别。

支持基于传统正则表达式和字典两种模式设置匹配规则；

3.1.3.7 数据安全预警与响应

支持通过静态、动态分析、对比、关联等方式进行数据分析和异常检测，感知和识别目标系统上发生的事件和行为，提炼和预测整体走向和趋势，在数据泄漏发生或入侵造成严重后果前及时采取行动，并记录数据违规使用流量；通过邮件、APP、短信等手段发送预警通报。

支持对数据安全事件实施追踪溯源，还原攻击过程、追踪攻击源头，提供详细的溯源报告；基于专家知识库提供事件分析和处置建议，对重大数据安全事件等突发事件进行响应处理，制定应急预案，当突发事件发生时，根据应急预案启动相应处理流程。

3.1.3.8 数据安全态势感知

支持数据分布态势展示，能够提供全网数据资产分布拓扑、敏感数据资产目录、敏感数据访问热点分布图、敏感数据资产访问权限表、数据资产访问途径全

路径透视图、数据源资产统计报表、敏感数据梳理报表、资产使用报表、资产对比分析报表等数据资产可视化展现功能。

支持数据流转态势展示，能够对全网业务数据异常流转过程进行实时监控，通过数据流向监管、实时流向分析、历史流向分析，提供全网数据流转路径可视化展示视图，为数据流转追溯与趋势分析提供支撑。

支持数据合规态势展示，能够根据数据使用态势模型自动计算数据使用的动态基线，形成数据合规使用和高危操作活动的态势曲线，从宏观层面刻画数据的安全运行态势变化趋势。

支持数据访问权限态势展示，能够根据访问权限态势模型自动计算数据权限的动态基线，形成数据使用的权限态势曲线，从宏观层面刻画数据的安全权限变化的态势。

3.1.3.9 系统管理

用户权限管理。应提供用户管理功能。包括用户整个生命周期的管理，提供对安全监测平台用户的创建、修改、删除和查询等功能。

提供统一集中的用户管理，支持被管理角色的创建、编辑、删除等基本功能。用户权限管理支持三权分立模式，可配置系统管理员、审计管理员与策略管理员共同进行系统管理，支持具备权限的用户查看系统中目前已创建的角色。

支持 RBAC 管理，提供分组的增加、删除、修改、查询及权限分组管理。可配置不同角色赋予不同系统功能模块的读写权限，未赋予此模块读写权限的用户，将无此功能模块的显示或配置的权限。用户基本信息需要包含角色名称、备注、权限等基本属性。用户角色查询时，支持通过角色名称来快速进行查询定位。具备权限的用户对角色信息进行新增、编辑、删除操作时，需触发系统记录日志。

支持对平台参数的配置；支持对数据存储时间的配置；支持对账户和密码的配置，包括帐号锁定时间、密码有效周期、密码错误次数、密码最小长度、密码强度的配置等。

支持日志审计，系统应对用户的使用等操作行为应有完整的日志记录，便于审计跟踪和分析。系统应记录系统中发生的关键事件，包括审计内容和审计操作。系统应确保审计日志不可删改。审计内容包括：用户操作审计和系统事件审计。审计操作包括：审计查看、审计内容导出和审计内容统计。

平台运维管理。配置专职人员对负责监测平台的运维管理。支持对平台进行统一监控，监视整个平台的运行状态，保证平台能够安全可靠地运行。支持记录系统运行日志，对运行异常记录异常系统日志，支持对日志的搜索、过滤、导入、导出等管理功能，支持将相关日志以 syslog 形式发送其他平台；支持平台运维人员实时获取服务器运行现状，以便对服务器进行维护。包括不限于服务器名称、服务器 IP、CPU 使用率、内存使用情况、磁盘容量、系统性能监控过程中产生的异常事件告警。

3.2其他要求

3.2.1电子政务外网网络安全监测运营和平台安全服务需求

3.2.1.1 运营团队要求（本项技术参数为实质性要求，投标人不满足视为无效投标）

岗位名称	人员数量	工作内容	服务期限
项目运营经理	1	总体把控项目中所涉及到的安全技术，开展相应的技术指导、安全数据分析、安全事件应急处置，负责项目技术工作的组织、检验、考核等工作，提供 5*8 安全运维驻场服务及重大活动节假日期间的重保值守服务。	2 年
威胁分析人员	2	对态势感知平台检测到的僵尸病毒、木马、蠕虫、勒索病毒、网络攻击、弱口令爆破、web 安全攻击、数据安全等安全威胁事件进行人工验证，确认事件的准确性，并评估事件对电子政务外网及在网络中部署的业务系统产生的危害。协助提供安全整改建议，在对委办厅局的安全通报整改进行验证，确认漏洞闭环处置。提供 5*8 安全运维驻场服务及重大活动节假日期间的重保值守服务。	2 年
运营监测人员	1	对已人工验证确认的安全事件，依据安全责任内主体进行分发，协助支持整改属于大数据管理局安全责任内内的威胁、漏洞及数据安全事件；对委办厅局安全事件进行通报处置，提供安全整改建议，跟	2 年

		踪整改进度并进行复查，提供 5*8 安全运维驻场服务及重大活动节假日期间的重保值守服务。	
处置验证人员	1	对态势感知平台检测到的网络设备漏洞、系统漏洞、中间件漏洞、web 应用漏洞进行人工验证，确认事件的准确性，并评估事件对电子政务外网及在网络中部署的业务系统产生的危害。协助提供安全整改建议，在对委办厅局的安全通报整改进行验证，确认漏洞闭环处置，提供 5*8 安全运维驻场服务及重大活动节假日期间的重保值守服务。	2 年

3.2.1.2 监测运营服务需求

服务项目	服务内容
全流量威胁分析服务	1、每周对全网终端及服务器所遭受的安全威胁进行一次安全分析：APT、远控木马、网络蠕虫、勒索病毒感染；活跃的僵尸网络；服务器上传恶意 Webshell；主机和服务器漏洞利用；恶意脚本上传和执行；数据违规存储；数据泄漏；数据高危操作行为；权限异常变动威胁等。 2、威胁事件的描述需包括但不限于以下部分：威胁最早及最近发生时间点；受害资产 IP 及相关信息；威胁类型、风险值及名称；基于威胁情报大数据得到的威胁来源 IP、地理位置、IOC 信息；攻击利用端口和协议；非法服务器外联和交互信息等。以专业技术分析当前遭受的威胁情况，为加强边界防御提升网络整体安全防护水平提供数据支撑。 3、需每周提供一次《全流量威胁分析报告》。
攻击者分析服务	1、每周通过采集本地的攻击数据，结合攻击数据的威胁情报信息对攻击者进行分析服务。从攻击者的视角，以专业技术分析当前存在的潜在攻击行为，为加强边界防御提升网络整体安全防护水平提供数据支撑。 2、需每周提供一次《攻击者分析报告》。
攻防演习防守及重保监测服务	在国家、行业、省级的攻防演习活动和各项重要保障活动中，供应商需提供攻防演习防守及重保监测服务，依托态势感知平台提供实时攻击告警，加强研判攻击事件，协助加固防守策略等。

3.1.1.3 平台安全服务需求（本项技术参数为实质性要求，投标人不满足视为无效投标）

按需对网络安全态势感知平台和政务数据监测监管与态势感知平台提供渗透测试服务、安全加固服务、基线扫描服务，并对由海南省大数据管理局建设运营的基础性、公共性电子政务信息系统提供渗透测试服务、漏洞扫描、基线扫描等管控服务，服务期限为 1 年。

对由海南省大数据管理局建设运营的基础性、公共性电子政务信息系统（包括：一体化、大数据公共服务平台、数据共享交换平台、互联网+监管、工改、业务中台等），按照采购人要求提供不少于 2 次的代码审计服务并提供审计报告。

1.渗透测试服务

1）服务内容

渗透测试服务包括信息泄露测试、常规漏洞测试、中间件漏洞测试、业务安全测试、通信安全测试、服务器安全测试和移动安全测试。

2）服务流程

本项目渗透测试服务将从服务准备、渗透测试、报告汇报、安全加固、渗透复测五个阶段开展。

3）服务标准

通过渗透测试工作，发现本项目部署软件平台存在的安全漏洞，同时检测平台的威胁防御能力，检验当前安全控制措施的有效性，提升海南省电子政务外网的安全性。

4）服务成果

服务交付以下成果：《渗透测试计划》、《系统渗透测试报告》。

通过渗透测试报告，直观展示系统当前安全状况，针对发现的安全弱点或漏洞提出改进性加固和修复建议，从而提升系统安全性。

2. 安全加固服务

1）服务内容

对本次项目部署平台的软硬件系统实施安全加固，保证信息系统抵御各种入侵行为、提高整体防御力、预防系统漏洞攻击、防止新增木马感染及破坏、防止外部黑客攻击，包括操作系统加固、中间件安全加固、数据库安全加固。

2）服务流程

安全加固服务的主要流程包括方案编制、测试与论证、数据备份、加固实施/安全加固回退、回归测试、总结与汇报共六个阶段。

3）服务标准

通过实施安全加固服务工作，及时对平台建设实施后发现的操作系统、中间件、数据库脆弱性进行处置，最大限度地增强各配套基础设施自身的安全抵抗力，提升网络安全保障体系的整体防御能力。

4）服务成果

方案编制阶段，由驻场安全服务人员编制《安全加固方案》，由应用系统开发商及相关厂商协助编制《安全加固回退方案》，并安全加固前 3 个工作日将《安全加固方案》与《安全加固回退方案》提交给海南省大数据局信息化相关负责人。

安全加固测试完成后，由驻场安全服务人员编制《安全加固测试报告》，提交给海南省大数据局相关负责人审核。

加固实施完成后，由驻场安全服务人员编制《安全加固报告》，并于安全加固后 3 个工作日内提交给海南省大数据局信息化相关负责人。

漏洞加固回归测试完成后，由验证人员编制《回归测试报告》并提交。

3. 基线扫描服务

1）服务内容

在新应用上线之前提供安全基线扫描，保证新建系统符合安全配置规范，避免因配置不当导致的安全事件。基线扫描服务包括操作系统基线扫描、数据库基线扫描、中间件基线扫描和配置基线扫描。

2）服务流程

基线扫描服务主要包括工具部署、任务制定、基线快照、扫描执行、报告处置五个阶段。

3）服务标准

通过对新应用实施上线前安全基线扫描，及时对扫描发现的问题进行整改加固，确保所有新应用“不带病上线”。

4）服务成果

通过基线扫描工具发现的基线配置检查结果，由安全服务人员进行二次分析，

最终编制《安全基线扫描报告》，以邮件形式发送给海南省大数据局相关系统负责人。

安全服务人员对现有信息资产安全配置基线进行更新后，形成《安全基线配置规范（修订版）》，以邮件形式发送给海南省大数据局相关系统负责人。

3.2.2网络安全体系规范编制需求

提供针对电子政务外网和政务管理单位、维护单位、使用单位的《电子政务外网网络安全管理办法》《电子政务外网数据安全管理办法》《电子政务外网安全审计管理办法》以及相关制度，对不同职责和角色的安全权责、工作要求进行说明，协助大数据局完善电子外网网络和数据安全体系。

3.2.3系统安全防护设计要求

应具备重要数据加密存储能力；

应具备口令强度策略、口令强度自动核查及用户登录超时退出机制，应采用符合国家密码管理局、工业和信息化部要求或相关行业主管部门规定的数字证书登录措施；

应具备监测自身运行状态能力，应支持状态异常告警；

应具备监测敏感数据操作日志，定期执行日志审计能力；

应支持备份重要系统信息和数据，支持系统快速恢复；

应采用统一的时钟源，支持标准时间自动同步，每天至少同步一次；

平台相关接口数据应采用符合国家密码管理局、工业和信息化部要求或相关行业主管部门规定的密码算法进行数据加密传输。

（四）其他相关要求

1、投标人必须提供详细的技术支持和服务方案。

2、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，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

B 包采购需求：

（一）标包名称:B 包海南省电子政务外网政务云密码服务平台建设项目

（二）项目概述

2.1 项目背景及目标

中央高度重视网络安全，2014 年成立中央网络安全和信息化领导小组，习近平总书记亲自担任组长，指出：“网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题”。2016 年 4 月 19 日，习总书记在“在网络安全和信息化工作座谈会上的讲话”中指出：“网络安全和信息化是相辅相成的。安全是发展的前提，发展是安全的保障，安全和发展要同步推进。要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力”。

同时，随着云计算、大数据技术的飞速发展，国家鼓励应用云计算技术整合改造现有电子政务信息系统，实现各领域政务信息系统整体部署和共建共用，因此各省依托政务外网资源陆续上线政务云平台，同时也汇聚了大量的政务数据，政务大数据作为国家的重要基础性、战略性资源，其安全成为当前热点问题。

海南省政务云数据安全及态势感知项目符合国家相关政策法规及监管的要求，将发挥密码技术在政务云平台安全运行、政务数据安全防护中的支撑作用。

2.2 项目建设内容

通过建设海南省电子政务外网政务云密码服务平台，为政务云平台及云上应用按需提供弹性密码服务。云密码服务平台以云密码资源池为基础，通过集成基础密码应用、终端密码应用等能力，为政务云平台及云上应用提供以商用密码为基础的密钥管理服务、密码运算服务、移动终端密码服务等，保证政务用户可信、政务数据可靠。

2.2.1 主要功能

海南省电子政务外网政务云密码服务平台基于云计算密码资源，为云上的应用提供数据加解密、数据签名验签、数据摘要等密码运算服务，为云上的应用提供统一的密钥管理服务。并基于移动终端安全服务，通过对接海南 RA，为移动终端提供数据安全、证书认证等服务。从而实现密码资源的统一建设和管理、密码服务的统一接口和服务、密码应用的统一调度和使用，主要功能要求如下：

2.2.1.1 密钥管理服务

通过云计算应用密钥管理系统，为云平台上的应用提供统一密钥管理服务。云密码资源池为云计算应用密钥管理系统提供密码运算支撑。

密钥管理包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理，云计算应用密钥管理系统参照《信息技术 安全技术 密钥管理》标准进行设计，通过对密钥全生命周期进行管理，满足信息系统三级密码应用要求。

对云平台提供的密钥管理，采用严格的鉴别机制，确保只有使用该服务的用户才能对其云计算应用密钥管理系统进行配置。

2.2.1.2 密码运算服务

密码运算服务主要是基于云密码资源池，为政务云环境下存在的大量业务系统，提供动态、弹性、可伸缩的加密/解密、签名/验签、数据摘要等基础密码运算服务，具备高可靠性、高安全性、易扩展能力。

云密码资源池通过对云密码机等硬件密码设备以集群的方式进行密码资源统一调度。云密码机采用虚拟化技术，在一台硬件密码设备上实现同时运行多个虚拟化的密码机（虚拟密码机），通过弹性调度技术，实现虚拟密码机密码服务性能的弹性扩展，支持虚拟化多种密码体系的虚拟密码机。

2.2.1.3 移动终端密码服务

通过移动终端密码服务为政务云终端提供数据加解密、密钥管理、身份认证、敏感信息安全访问、传输及存储加密等密码服务。

移动终端密码服务平台符合国家密码管理局三级密码模块要求并取得商密鉴定证书，主要由密码软卡、移动终端密码服务管理系统组成，分别与应用 APP 客户端、服务端集成，按需提供密码服务。

密码软卡是软件密码模块，以库文件的形式集成到业务应用中，为其提供加解密、签名验签、密钥管理、证书管理、身份认证、敏感信息安全访问、传输和存储服务。

移动终端密码服务管理系统提供密码资源集中管理服务，负责密码软卡管理、密钥管理、通过对接海南 RA 实现数字证书管理以及用户有关的敏感数据安全管理等。

2.2.2 采购需求清单

本次项目主要对海南省电子政务外网政务云密码服务平台相关软硬件产品、等保测评、培训服务和相关管理制度进行采购，具体清单如下：

序号	项目内容	
一	**软件产品**	
1	云计算应用密钥管理系统	购买 1 套云计算应用密钥管理系统，提供云环境下密钥生成、更新、存储、分发、导入、导出、使用、恢复、归档、销毁等环节进行管理。
2	移动终端密码服务平台	购买 1 套移动终端密码服务平台，由移动终端密码服务管理系统及密码软卡（1 万软卡授权）组成。负责移动终端密码运算，后台密码软卡管理、密钥管理,通过对接海南现有 CA 系统实现数字证书管理以及用户有关的敏感数据安全管理等。
3	密码资源池管理系统	购买 1 套密码资源池管理系统，密码资源池管理系统通过对云密码机等硬件密码设备以集群的方式进行密码资源统一调度。
二	**硬件产品**	
1	云密码机	购买 4 台云密码机，采用虚拟化技术，在一台硬件密码设备上实现同时运行多个虚拟化的密码机，通过弹性调度技术，实现密码服务性能的弹性扩展。
三	**安全测评**	
1	等保测评	提供项目 2 年质保期内等保三级测评服务
2	密码相关测评	遵循商密、国密相关政策法规和标准规范开展海南省电子政务外网政务云密码服务平台建设，通过密码测评。
四	**其他服务**	
1	密码使用管理办法编制服务	投标人需制定政务云密码使用管理办法，为政务云密码策略的制定、密码设备及系统的运维管理、密码应急处置、密码使用人员管理等提供指导。
2	系统使用培训	投标人必须针对用户管理、运维人员制定详细的培训计

	服务	划。为系统相关管理人员、业务人员、维护人员提供所需要的业务管理类、技术类、操作类的培训。
3	质保服务	项目完成终验后，提供 2 年的质保服务

（三）项目要求

3.1 技术参数要求

平台建设在满足全省工程建设项目审批业务办理需求基础上，还要满足国家对数据上传的考核要求。具体技术要求如下：

3.1.1 云计算应用密钥管理系统需求

投标人需提供云计算应用密钥管理系统，为政务云平台和云上的业务应用提供密钥管理服务。云计算应用密钥管理系统需满足以下要求。

3.1.1.1 功能要求

云计算应用密钥管理系统需支持对 SM1/2/3/4 算法的密钥全生命周期管理，并具备如下功能。

1） 密钥生成

云计算应用密钥管理系统支持密钥手动生成、服务使用者调用密钥申请接口被动生成两种方式。

云计算应用密钥管理系统提供手动生成密钥界面，选择服务使用者、算法类型、密钥类型、有效期，输入生成数量，系统调用密码设备生成密钥，并存储在数据库的密钥备用库中。

云计算应用密钥管理系统提供密钥申请接口，由服务使用者调用密钥申请接口，传入算法类型、密钥类型、有效期，生成数量等参数，系统调用密码设备生成密钥，并存储在数据库的密钥在用库中。

2） 密钥存储

云计算应用密钥管理系统对密钥数据以安全的方式进行加密存储，不会在密码设备或者密钥存储介质之外出现私钥明文，确保密钥数据的安全。

云计算密钥管理系统本地主密钥，由配备的密码设备产生并存储在密码设备内部。密钥加密密钥应由云计算应用密钥管理系统配备的密码设备产生，使用本地主密钥加密后存储于数据库中。密钥服务使用者的业务应用密钥，由云计算应用密钥管理系统配备的密码设备产生，使用密钥加密密钥加密后存储于数据库中。

3）密钥分发

云计算应用密钥管理系统采用 HTTPS 和符合《密码设备管理 对称密钥管理技术规范》(GMT 0051-2016)的交互协议，包括对象交互和数据传输等都采用自主、安全、可控的协议，保障云计算应用密钥管理系统与第三方业务系统、浏览器之间的交互协议安全。采取身份鉴别、数据完整性、数据机密性等安全措施，能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

云计算应用密钥管理系统采用 HTTPS 交互协议分发密钥时，密钥数据通过使用者的公钥加密保护后传输。

云计算应用密钥管理系统采用符合《密码设备管理 对称密钥管理技术规范》(GMT 0051-2016)的交互协议分发密钥时，密钥数据通过数据加密密钥保护后传输。

4）密钥导入与导出

云计算应用密钥管理系统采用四层密钥管理体系。最顶层是密码设备的本地主密钥;第二层是密钥加密密钥;第三层是用户主密钥,第四层是用户数据密钥。密钥导出时，对密钥进行加密，以密文形式导出到密码设备外部，防止明文密钥数据被非法获取或篡改。

5）密钥使用

提供可靠的身份认证机制，确定服务使用者身份及访问权限，杜绝服务使用者的数据被恶意访问、篡改、外泄等。服务使用者的密钥数据采用不同的加密密钥保护存储，支持密钥数据逻辑隔离，确保用户在安全的环境中使用密钥，确保一个用户的信息泄露不会影响到其他用户。云计算应用密钥管理系统能够按照密钥更换周期要求用户更换密钥。

6）密钥备份与恢复

支持单机密钥数据备份与双机密钥数据备份。单机部署情况下，数据备份一方面依靠物理服务器提供冗余磁盘对数据进行实时备份。一方面通过数据库脚本和应用程序对密钥数据、日志数据、整库数据根据备份策略自动备份或手动备份进行冷备份。双机备份部署情况下，支持数据的热备份，实现数据的实时备份与恢复。

云计算应用密钥管理系统对密钥备份与恢复操作进行记录，并生成审计信息;

审计信息包括备份或恢复的主体、备份或恢复的时间等，审计信息由审计员签名防止抵赖。

7）密钥归档

对历史密钥进行归档，生成包含校验值的归档文件，归档密钥用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。云计算应用密钥管理系统对密钥归档操作进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等，并对归档密钥进行数据备份。

8）密钥销毁

能够在用户密钥使用完毕后或者密钥泄漏等情况下对密钥进行销毁，保证密钥不可恢复。

3.1.1.2 性能要求

云计算应用密钥管理系统性能需满足如下要求。

序号	性能要求	
1	算法性能	SM1/SM4 生成不少于 5000 个/s。
2		SM2 生成速率不小于 5500 对/s。
8	系统性能	系统支持国密安全通道申请密钥：不少于 900 个/s。
9		最大并发访问次数：不少于 1000。
10		服务对象数量：不少于 500。
11		系统支持最大管理密钥数：不少于 1000 万。
12		密钥保存不少于 10 年。

3.1.1.3 其他要求

云计算应用密钥管理系统需具备国家认定的相关产品证书。

3.1.2 移动终端密码服务平台需求

投标人需提供移动终端密码服务管理系统及配套密码软卡，为移动端用户和移动应用提供数据加解密、密钥管理、身份认证、敏感信息安全的访问、传输及存储等密码服务。移动终端密码服务管理系统和密码软卡需满足以下要求。

3.1.2.1 功能要求

移动终端密码服务管理系统需具备如下安全功能。

1）提供生产授权服务；

2）提供在线初装数据下载功能；

3）提供移动密钥生成、分发、存储、备份、销毁等管理；

4）提供远程销毁等移动终端密码设备管理。

密码软卡需具备如下安全功能。

1）提供移动终端 SDK；

2）移动端支持 android 和 ios 操作系统；

3）移动端密码软模块支持 SM2/SM3/SM4/ZUK 等国密算法；

4）提供移动端安全随机数生成；

5）服务期内提供移动终端密码软模块免费升级服务。

针对政务 APP 提供移动终端安全存储、通道加密、证书认证、签名验签等安全服务。

1）安全存储服务：业务 APP 要对敏感信息进行加密时，调用密码软卡生成密钥，对数据明文进行加密，数据密文由业务 APP 保存时，密码软卡保存密钥，业务 APP 要对密文进行解密时，要调用密码软卡，获取密钥进行解密。

2）通道加密服务：针对业务 APP 与业务服务器之间通信提供 SSL 安全通道服务，支持双向认证，在认证通过后，协商生成会话密钥，双方可使用加密密钥进行数据加密传输。

3）证书认证服务：在用户访问业务 APP 时，基于密码软卡提供证书认证，支持双向认证，即客户端在身份认证之前请求验证服务器身份，服务器返回签名和证书文件，客户端验证服务器签名后，客户端协同运算生成签名信息，将客户端的签名信息和签名证书文件发送到服务器，服务器验证后完成双向认证。证书认证服务支持对接海南 RA，通过移动终端密码服务平台与海南 RA 的适配，满足移动端的证书签发需求，从而实现基于数字证书的身份认证。

4）签名验签服务：业务 APP 要对数据进行签名时，调用签名接口，通过密码软卡与移动终端密码服务协商密钥，对数据进行签名，对方收到有签名的数据，可基于签名证书进行核验，保障数据的真实性。

5）群组密钥管理服务：多方在群组通信时，移动终端密码服务为通讯生成一个群组密钥，并安全分发到通讯各方密码软卡。通信时，由通讯发起方调用密码软卡生成会话密钥，使用会话密钥加密通讯信息，同时使用群组密钥加密会话

密钥传输给通讯接收各方。接收方利用群组密钥解密获得会话密钥，最终获得通讯信息。

3.1.2.2 性能要求

移动终端密码服务管理系统和密码软卡性能需满足如下要求。

序号	性能要求	
1	移动终端密码服务管理系统	支持不低于 10 万移动客户端授权。
2		最大用户数不小于 100 万，支持同时在线用户数不小于 10 万，系统支持平滑扩容升级。
3	密码软卡	签名算法约 1.5 次/s，杂凑、对称算法加解密速度高于 50mbps。

3.1.2.3 其他要求

移动终端密码服务管理系统国家认定的相关产品证书。

密码软卡需具备国家认定的相关产品证书。

3.1.3 云密码资源池需求

投标人需提供云密码机及配套的密码资源池管理系统，为政务云平台和云上的业务应用提供密码运算服务。云密码机及密码资源池管理系统需满足以下要求。

3.1.3.1 功能要求

云密码机需具备如下安全功能。

1）提供对使用虚拟密码机的租户管理员进行 USBKey 证书认证、对业务系统进行证书认证的功能；

2）具备虚拟密码机间密钥安全隔离和访问控制功能；

可实现按需创建不同性能指标的虚拟密码机；提供支持虚拟密码机性能按需分配功能，一台云密码机上可同时运行不同性能、不同功能、不同版本的虚拟密码机的原厂证明材料，并加盖原厂鲜章；

3）支持虚拟密码机性能弹性调度功能，可实现创建弹性调度的虚拟密码机，根据业务繁忙程度对虚拟密码机的性能进行动态伸缩，充分利用密码资源；

4）具备接入 OpenStack 云计算管理系统功能；

支持虚拟密码机智能化集群，负载均衡功能：可创建虚拟密码机智能化集群，集群内置负载均衡器，集群内自动发现虚拟密码机、自动根据权重分配负载到虚拟密码机，提供高可用、高性能、弹性伸缩的密码服务。提供智能化集群、负载

均衡功能的原厂证明材料，并加盖原厂鲜章；

5）具备数据加密、解密；数字签名/验证；数据摘要；MAC 的产生、验证；单向散列。

6）支持对称算法：SM1/SM4/3DES/AES；支持非对称算法：SM2；支持杂凑算法：SM3/SHA1/SHA256；

7）支持安全管理功能，提供安全的远程管理功能。

密码资源池管理系统需具备如下安全功能。

a）支持三员的身份管理；

b）支持密码资源申请，为用户提供云密码资源申请界面，选择虚拟密码机类型匹配自身应用所需的密码运算能力，实现云密码资源申请操作请求；

c）支持密码资源审批，对用户的密码资源申请进行审批管理、资源状态查询；

d）支持密码资源模板管理；

e）支持镜像管理；

f）支持虚拟网络管理；

g）支持虚拟密码机管理，提供系统管理员负责虚拟密码机实例的启动、关闭、重启、终止操作；用户负责对自己申请创建的虚拟密码机实例进行启动、关闭、重启操作；

h）支持云密码机状态监控，系统管理员可监控所有云密码机和虚拟密码机资源总体使用情况；用户可监控自身云密码机和虚拟密码机的资源使用情况。支持以图形化方式直观展示云密码机和虚拟密码机实例状态。

3.1.3.2 性能要求

云密码机性能需满足如下要求。

序号	性能要求	
1	云密码机	SM2 签名速率不小于 210,000 次/秒。
2		SM2 验证速率不小于 97000 次/秒。
3		SM1 计算速率不小于 1.1Gbps。
4		SM3 计算速率不小于 8Gbps。
5		SM4 加解密速率不小于 8Gbps。提供 SM4 加密解密速率的原厂证明材料，

		并加盖原厂鲜章；
6		网络连接最大并发数不小于 3072 个。
7		单台设备可创建虚拟密码机数量不少于 96 个。提供单台云密码机中创建不少于 96 台虚拟密码机的原厂证明材料，并加盖原厂鲜章。

3.1.3.3 其他要求

云密码资源池应提供与政务云上业务应用对接的相关接口规范，为政务云上业务应用调用密码服务提供支撑。

云密码机需具备国家认定的相关产品证书。

3.1.4 系统管理需求

云密码机需具备如下系统管理功能：

1）安全管理功能：提供安全的远程管理功能；

移动终端密码服务平台需具备如下系统管理功能：

1）移动终端密码服务管理系统提供基于用户认证的密码软卡在线管理。

密码资源池管理系统需具备如下系统管理功能：

1）系统管理员、业务管理员、审计管理员、用户采用“用户名+口令+验证码”方式登录系统，实现身份鉴别及操作权限控制；

2）系统管理员、业务管理员、审计管理员创建及管理；

3）对需要申请和使用密码资源池的用户进行管理；

4）对系统运行日志、系统操作日志进行管理和审计，以及备份日志文件管理；

3.2 其他要求

3.2.1 密码应用标准规范编制需求

《电子政务外网密码使用管理办法》用于规范政务云平台密码的使用，为政务云密码策略的制定、密码设备及系统的运维管理、密码应急处置、密码使用人员管理等提供指导。

3.2.2 密码测评服务需求

海南省电子政务外网政务云密码服务平台基于海南省政务云统一的基础网络设施和安全设施进行建设，本次平台的建设需满足求信息系统密码应用第三级相关要求。

根据《信息系统密码应用基本要求》（GM/T 0054-2018）文件，信息系统密码应用三级要求主要包括技术要求、密钥管理要求及安全管理要求。

技术要求分别包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四大部分。

密钥管理包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程。

管理要求分成四大部分：　制度管理、人员管理、建设管理、应急管理。

3.2.3 平台处理能力及响应速度需求

平台应通过负载均衡、预处理等技术手段处理系统应用服务在用户访问的高峰时段的各项请求，不会出现延迟、死机等性能下降的现象，具体原则要求如下：

■ 可扩展

采用易于扩展的系统架构进行各项功能的开发实现，便于今后在进行业务功能扩展时能够快速实现功能调整，顺利实现与新系统、新功能的对接，最大程度的体现系统的兼容性。

■ 易用性

因为本系统涉及的业务点多面广、用户多、职能范围存在交叉。所以，要求注重系统的界面布局、菜单的设计、应用展示等方面的设计，遵循友好、直观，简洁的设计思路，体现对用户使用过程的正确引导。

■ 稳定性

本项目建设的互联网部署系统要能够满足 7*24 小时的运行要求，电子政务外网部署系统要求能够满足 7*24 小时的运行要求，系统可用性要求达到 99.99%。

■ 运行效率

运行效率要求包括：

（1）在现有的硬件系统条件下，开发的软件系统应能达到特定的运行速度，系统运行速度较快，能够达到管理数据的浏览、各种处理、查询统计等日常工作的响应要求，且该速度不以依赖特定的硬件能力为前提，以利于整体提高业务处理的工作效率；

（2）系统运行时，对系统硬件资源的利用率要合理，避免占用过多系统硬件资源或过于频繁的硬盘访问等，以提升整体运行速度；

（3）在网络稳定以及客户端软件性能达标的情况下，操作性界面单一操作的系统平均响应时间应小于 2 秒；系统应提供 7×24 小时的连续运行，平均故障修复时间小于 60 分钟；

（4）为了获得高性能，要尽量减少应用处理时间，如多采用并置、缓存、池化、并行化、分区等手段。

（四）其他相关要求

1、投标人必须提供详细的技术支持和服务方案。

2、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，如发现与其投标文件中的描述不一，代理机构将报政府采购主管部门严肃处理。

3、所投的“云计算应用密钥管理系统”、“云密码机”、“移动终端密码服务管理平台”等产品资质要求具备《商用密码产品认证证书》，并提供相关证明材料。

4、不满足上述合规性要求的产品不得投标。

C 包采购需求：

（一）标包名称：C包监理

（二）监理服务周期：本项目监理服务周期自签订合同之日起，至项目完成竣工验收。

（三）监理技术要求：

1、监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件开发及应用技术培训、服务能力评估、试运行（测试）、阶段性验收、竣工验收等全过程进行监督管理，从硬件监理、软件监理、系统集成监理等三个方面梳理该项目建设监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度， 最终实现监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当服务质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

2、监理目标控制方案

以项目服务合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工 程监理规范》 信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对项目全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同 措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

（1）监理质量目标控制

监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本 项目建设质量能达到建设单位要求的质量目标。确保本项目建设质量达到合同中规定的功能、技术参数等目标。 确保项目建设中的设备和各个节点满足相关国家（GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信 部信[2002]570 号《信息系统工程监理暂行规定》）、地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案 的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉 及用

户需求 调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。

要求监理在整个项目实施过程中做好对项目质量的事前控制，投标人应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软件开发、项目培训等提出项目监理的质量控制原则、方法、措施、工作流程和目标。

（2）监理进度目标控制

确保本项目按合同规定的工期完工。

依据合同所约定的工期目标，在确保质量和安全的原则下，采 用动态的控制方法，对进度进行主动控制，确保项目按规定的工 期完工。

通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的项目监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

（3）监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。

以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。

在项目建设中，合理减少项目变更，保护建设单位的经济利益。

3、项目监理重点难点分析

投标人应根据本项目建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展项目的监理服务工作。

（1）项目组织及总体技术方案的质量控制

1）协助审查项目建设方的投标书、合同及实施方案；

2）在技术上、经济上、性能上和风险上进行分析和评估，为采 购人提供建议；

3）协助审查项目建设方提交的组织实施方案和项目计划等相 关文档；

4）协助审查项目建设方的项目质量保证计划及质量控制体系；

5）参与制定项目质量控制的关键节点及关键路径。

（2）项目质量控制

1）组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。

2）系统集成质量控制审核系统总集成方案；对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；参与制定系统验收大纲；对设备安装、调试进行验收；对系统进行总体验收。

3)人员培训的质量控制 协助审查并确认培训计划，审定培训大纲；监督审查建设方实施其培训计划，并征求采购人的意见反馈；监督审查考核工作，评估培训效果；协助审核并确认培训总结报告。

4)文档、资料的质量控制 监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

（3）进度协调控制

1）组织措施：建立进度控制协调制度，落实进度控制责任。

2）编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、设备的采购、设备的安装调试、软件的编制、试运行等各方面内容，做到既要保证各子系统各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。

3）审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划完成情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上有无缺陷进行审查。要根据建设方所能提供的人员及设备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。

4）系统建设进度的现场检查：随时或定期、全面地对进度计划 的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加 强系统建设准备工作的检

查，在项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况， 确保准备工作符合要求，不影响后续工作的进行。

5）进度计划的分析与调整：要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

（4）投资控制

1）组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。

2）审查设计图纸和文件，审查建设方的施工组织设计和各项技术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。

3）严格督促建设方按合同实施，严格控制合同外项目的增加， 协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

（5）合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段 目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1）以合同为依据，本着“实事求是、公正”的原则，合情合理 地处理合同执行过程中的各种争议。

2）分析、跟踪和检查合同执行情况，确保项目建设方按时履约。

3）对合同的工期的延误和延期进行审核确认。

4）对合同变更、索赔等事宜进行审核确认。

5）根据合同约定，审核项目建设方的支付申请。

6）建立合同目录、编码和档案。

7）合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据， 合同外项目增加要严格

审 批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

（6）文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。

信息管理主要措施要求如下：

1）制定详细的信息收集、整理、汇总、分析、传递和利用制度， 力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。

2）在项目实施过程中做好监理日记和项目大事记。

3）做好双方合同、技术建设方案、测试文档、验收报告等各类 往来文件的存档。

4）建立必要的会议、例会制度，整理好会议纪要，并监督会议 有关事项的执行情况

5）立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。

6）建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类汇总，及时向采购人及有关各方报送。

7）监理项目验收时，应提交符合规定的有关项目的成套资料，包括印刷本和电子版。

（7）日常监理

1）掌握监理范围内涉及的各种技术及相关标准；

2）安排足够的监理人员，按项目需要派驻相应的专业人员进行项目监理，至少保证 1 名专职信息系统监理工程师在现场，随时为采购人提供服务，总监理工程师必需专职于本项目；

3）制定项目管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；

4）熟悉了解项目的业务需求，协助采购人对项目的目标、范围 和功能进行界定，参与并协助项目的设计方案交底审核工作；

5）建立健全科学合理的会议制度，并予以贯彻落实；

6）建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；

7）与采购方一起制定评审机制，在项目实施全过程中随时关注隐患苗头，如发现将会导致项目失败的情况出现时，应及时启动评审机制，组织专家对项目实施情况进行评审，对评审不合格的， 应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审），对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见。

4、项目各阶段的监理规划、实施

投标人应对本项目从设计施工到项目竣工验收阶段制定一整 套项目监理的工作流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶 段、质保期阶段等。

（1） 设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，项目监理单位 在设备/材料采购阶段监理工作主要有：

审核承包单位的设备采购计划和设备采购清单； 订货进货验证；组织到货验收；

鉴定、设备移交等。

（2）施工阶段监理

① 开工前的监理

1） 审核施工设计方案：开工前，由监理单位组织实施方案的 审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

2） 审核实施方案的合法性、合理性、与设计方案的符合性；

3） 审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

4） 审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

5） 审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

6） 审核《软件项目开发计划》。

② 施工准备阶段的监理

1）审批开工申请，确定开工日期；

2）了解承包商设备订单的定购和运输情况；

3）了解施工条件准备情况；

4）了解承建单位实施前期的人员组织、施工设备到位情况；

5）编制各个子项目监理细则；

6）签发开工令。

③ 施工阶段的监理

1）审核软件开发各个阶段文件；

2）协助采购人组织软件开发阶段评审；

3）材料、硬件设备、系统软件的供货计划的审核；

4）材料、硬件设备、系统软件的进场、开箱和检验；

5）促使项目中所使用的产品和服务符合合同及国家相关法律 法规和标准；

6）对施工各个阶段的安装工艺进行检查；

7）审核项目各个阶段进度计划；

8）督促、检查承建单位进度执行情况；

9）审查项目变更，提出监理意见；

10） 审查承建单位阶段款支付申请，提出监理意见；

11） 按周（月、旬）定期报告项目情况；

12）　组织召开项目例会和专项会议。

④ 试运行阶段的监理

1）协助建设方确认项目进入试运行；

2）监查系统的调试和试运行情况，记录系统试运行数据；

进行试运行期系统检测或测试，做出检测或测试报告；

对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；

3）进行试运行时间核算；

4）协助业主确认试运行通过。

（3）验收阶段监理

① 验收阶段

1）对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；

2）监督检查承建单位作好用户培训工作，检查用户文档；

3）组织系统初步验收；

4）审查承建单位提交的竣工文档；

5）参与项目竣工验收；

6）竣工资料收集整理齐全并装订，签署验收报告；

7）审核项目结算；

8）审查承建单位阶段款支付申请，提出监理意见；

9）向建设单位提交监理工作总结；

10）　将所有的监理材料汇总，编制监理业务手册，提交采购人；

11）　系统验收完毕进入保修阶段的审核与签发移交证书。

② 项目移交阶段

1）系统的设计方案、设计图纸和竣工资料的全部移交；

2）设备、软件、材料等的验收文档核实；

3）施工文档的移交；

4）竣工文档的移交；

5）项目的整体移交。

（4）质保期阶段监理

监理单位承诺依据委托监理合同约定的项目质量保修期规定 的时间、范围和内容开展工作主要有：

1）定期对项目进行回访，协助解决技术问题；

2）对项目建设单位提出的质量缺陷进行检查和记录；

3）对质量缺陷原因进行调查分析并确定责任归属；

4）检查承建单位质保期履约情况，督促执行；

5）审查承建单位阶段款支付申请，提出监理意见。 投标人应根据上述监理工作内容（但不局限于上述内容），分别制定详细的监理工作流程，使本项目的监理工作流程化、制度化。

5、监理工作要求

（1）监理工作制度要求

根据本项目的特色，本项目要求以现场监理为主要方式进行， 在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制，在整个项目建设期间，总监理工程师必须保证有三分之一工作日以上的时间到甲方现场，且必须在建设期间全程常驻至少一名监理工程师在甲方现场。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于 3 名专业工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

（2）监理项目组织要求

项目监理组织形式应根据项目的特点、项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑 有利于项目合同管理、有利于目标控控制、有利于决策指挥、有 利于信息沟通。要求投标人在报价方案中要明确项目监理的各项 运作，包括监理人员的相关 资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

（3）监理信息管理要求

投标人应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

1）做好监理日记及项目大事记；

2）做好合同批复等各类往来文件的批复和存档；

3）做好项目协调会、技术专题会等各项会议纪要；

4）管理好实施期间的各类、各方技术文档；

5）做好项目周报；

6）做好监理建议书、监理通知书存档；

7）阶段性项目总结。投标人应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合 管理。

6、监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，投标人应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

1）跟踪检查合同的执行情况，确保承建单位按时履约；

2）对合同工期的延误和延期进行审核确认；

3）对合同变更、索赔等事宜进行审核确认；

4）对合同终止进行审核确认；

5）根据合同约定，审核承建单位提交的支付申请，签发付款 凭证。要求对项目合同进行合理的管理，以完善整个项目建设的过程。

（四）监理服务准则

遵照国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》的规定，以“守法、诚信、公正、科学”的准则执业，维护建设方

与承建方的合法权益。具体应做到：

1. 执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责。

2. 不收受被监理单位的任何礼金。

3. 不泄漏所监理项目各方认为需要保密的事项。

4. 遵守国家的法律和政府的有关条例、规定和办法等。

5. 坚持公正的立场，独立、公正地处理有关各方的争议。

6. 坚持科学的态度和实事求是的原则。

7. 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务。

8. 不泄漏所监理的项目需保密的事项。

（五）监理依据

1. 国家 GB/T19668.1-19668.6《信息化工程监理规范》、信息产业部信部信[2002]570 号《信息系统工程监理暂行规定》和海南省有关信息系统项目建设和监理管理规范；

2. 建设单位与承建单位签订的合同

3. 建设单位与监理单位签订的委托监理合同

4. 本项目招标书、招标过程文件、各中标商的投标书

5. 国家有关合同、招投标、政府采购的法律法规

6. 部颁、地方政府的信息工程、信息工程监理的管理办法和规定

7. 建设工程和信息工程相关的国家、行业标准和规范

8. 建设工程和信息工程技术监督、工程验收规范

9. 与项目相关的技术资料

10. 其他与本项目适用的法律、法规和标准

11. 国家、地方及行业相关的技术标准

（六）安全保密要求

本项目要求投标人制定一整套监理安全保密制度，确定保密责 任人，同时要求投标人：

1. 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；

2. 监理单位各级组织严格履行保密职责；

3. 按照公司内部保密规定开展监理工作。

（七）监理验收要求

（1） 审核监理方应提交的各类监理文档和最终监理总结报告，综合评估

监理 方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。

（2） 本监理工作的最终验收由委托方组织。

（八） 其它要求

项目管理及施工组织 投标人须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控 制、质量管理、验收方法等内容。

三、评分表:

（1）A 包：

序号	评分项	分值
1	技术分	43
2	商务分	37
3	价格分	20
合计		100

（2）B 包：

序号	评分项	分值
1	技术分	50
2	商务分	25
3	价格分	25
合计		100

（3）C 包：

序号	评分项	分值
1	技术分	50
2	商务分	30
3	价格分	20
合计		100