

## 第三章 用户需求书

为加快推进项目实施，保障全厅信息系统、各类硬件、网络安全稳定运行，进一步规范和强化预算执行，除相关设备维修维护和网络链路租赁等经费外，其他系统软硬件运维、门户网站运维升级、网络安全等级保护测评、商用密码应用安全性评估需作为服务采购项目（329.89 万元），具体分为 5 个包：

**A 包，预算 54.73 万元。**对服务器、网络及基础软件运维，包括服务器、网络，防火墙、路由器、超算节点（完善下量），GIS 软件、数据库（DB2/ORACLE/达梦等）、EOS 应用集成运行平台、润乾集成报表软件、weblogic 中间件、e-link 多平台即时通讯系统、电子签章系统软件，确保硬件及软件安全稳定运行。

**B 包，预算 212.45 万元。**对生态环境综合监管（一期）系统运维及升级改造部分，包括数据资源中心，环境地理信息系统，放射源监管子系统，行政许可审批子系统，排污许可证管理子系统，环境应急管理子系统，环境监察移动执法子系统，环境影响评价管理系统，生态环境综合管理门户升级，海南省机动车环保检验管理系统升级项目，禁塑工作管理平台，海南省污染源调查管理信息系统，环境质量数据管理等系统以及相关升级改造。

对海南省生态环境监测信息系统运维工作，包括污染源监测综合管理系统，污染源在线监控系统，昌江核电厂辐射环境现场监测系统，大气环境综合信息管理系统，土壤环境信息综合管理，水环境综合信息管理，环保督察工作管理，清洁生产审核管理，生态环境监测数据共享利用及发布，生态环境监测网络建设项目管理，社会环境服务机构管理等系统。

对海南省生态环境综合办公系统运维及升级改造，包括厅综合门户系统、三套 OA 以及系统功能优化、部分系统海政通接入以及密评改造等升级改造。

**C 包，预算 14.83 万元。**包括海南省生态环境厅门户网站运维、安全服务以及智能互动云平台智能问答升级工作。

**D 包，预算 24 万元。**包括海南省生态环境综合管理平台、海南省生态环境厅门户网站、超级站多因子数据收集及在线解析系统、海南省生态环境综合办公系统四个信息系统等级保护测评工作。

**E包，预算23.88万元。**海南省生态环境综合管理平台、海南省生态环境厅门户网站、超级站多因子数据收集及在线解析系统、海南省生态环境综合办公系统四个信息系统的商用密码应用安全性评估工作。

# A包用户需求书

## 一、项目名称及采购内容

项目名称：海南省生态环境厅信息化运维项目（2024年）

采购内容：基础硬件及产品软件运维

预算额度：54.73万元。

## 二、采购需求

### （一）运维范围

#### （1）基础硬件运维列表

序号	运维对象	品牌型号	基本技术参数	单位	数量	用途
1	防火墙 高端	深信服 I840	高端防火墙 吞吐量 14Gbps, 并发连接数 400 万	台	1	网络连接
2	防火墙 中端	奇安信防火墙 NSG 3000-TE45 (2 台)	中端防火 吞吐量 1000-10000Mbps; 并发连接 高于 200 万	台	2	网络连接
3	网闸 中端	网御星云 SIS3000	中端安全隔离网闸吞吐量 400-800Mbps; 高端安全隔离网闸吞吐量大于 1000Mbps	台	1	网络连接
4	低端交换机 (接入级)	华为 S2700*9 台、 华为 S5700*26 台、 MP S3100*26 台、 MP S4300*4 台	低端交换机 一般用于接入的交换机	台	55	网络接入
5	路由器高端 (网点级)	H3C 8300	高端路由器: 高转发性能, 应用于核心、大型组网边界	台	1	核心网络架构

6	存储设备	ibm storwize v5000*1 台	中端网络负载均衡四层处理能力≤30 万 cps, 七层处理≤40 万 TPS, 最大连接数≤1500 万;	台	1	应用系统数据存储
7	光纤交换机	CISCO MDS 9148、 博科 200E*2 台	①最大支持端口: 24 口; ②接口类型: 支持 8/4/2GbpsFC 端口, 所有端口自动适应; ③交换机功能: 采用无阻塞构架, 提供无争议的、全双工的带宽, 每个交换机 192Gbps; ④冗余电源: 单电源; ⑤详细配置: 24 个 8G FC 端口, 24 端口激活, 含 24 个 SFP 模块, 任何端口都是通用、自动发现、自配置;	台	3	网络搭建设备
8	刀片计算节点	曙光 CB50-G20 计算刀片 (含刀箱)	双路计算刀片: 2*Intel Xeon E5-2680 v3 处理器 (12 核, 主频 2.5GHz); 8*8GB ECC Registered DDR4 内存: 4*300G 2.5 寸 10000 转 SAS 热插拔硬盘: 2*千兆以太网接口;	台	7	模式计算
9	刀片计算节点	曙光 CB50-G30 计算刀片 (含刀箱)	双路计算刀片: 2*Intel Xeon E5-2680 v3 处理器 (12 核, 主频 2.5GHz); 8*8GB ECC Registered DDR4 内存: 4*300G 2.5 寸 10000 转 SAS 热插拔硬盘: 2*千兆以太网接口;	台	4	
10	刀片计算节点	曙光 CB50-G20 计算刀片	双路计算刀片: 2*Intel Xeon E5-2680 v3 处理器 (12 核, 主频 2.5GHz); 8*8GB ECC Registered DDR4 内存: 4*300G 2.5 寸 10000 转 SAS 热插拔硬盘: 2*千兆以太网接口;	台	10	模式计算

1 1	刀片机箱	曙光 TC6600 刀片平台	机架式刀片机箱，至少支持 14 个双路计算刀片：1*管理模块，支持 IPMI 2.0, KVM over IP, 虚拟媒体等；支持冗余管理模块/冗余以太网 模块/冗余 QDR 交换模块/FDR 模块；支持双路、四路刀片混插：可扩展 10 个 PCIe x16 插槽：1*24 口千兆（万兆上联）交换模块：每个模块对外 4 个 RJ45 千兆接口和 2 个 SFP+ 万兆接口； 1*10G 万兆交换模块：对内 14 口互连， 对外 16 个 SFP+ 万兆端口+4 个 40G QSFP 端口：满足所有刀片全线速 FDR/EDR 互联： 10*冗余热插拔散热模块； 6*2000W 冗余电源模块； 上架导轨；	套	1	放置刀片
1 2	管理登陆节点	曙光 I620-G20	2U 机架式；2*Intel Xeon E5-2680 v3 处理器（12 核，主频 2.5GHz）； 板载 24 个内存插槽，8*16GB DDR4 ECC 内存； 4*600G 2.5 寸 10000 转 SAS 硬盘； 2*千兆以太网接口； 1*56Gb FDR InfiniBand HCA 卡：可扩展 24 个热插拔 2.5 寸或者 12 个 3.5 寸 SATA/SAS 接口 U 硬盘或固态硬盘；最大可支持 8 个 PCI-E 扩展插槽； 集成八口 SAS 卡，支持 RAID0/1； 集成系统管理芯片，支持 IPMI2.0、KVM over IP、 虚拟媒体等管理功能； 内置 DVD-RW 光驱； 550w 1+1 冗余服务器电源； 上架导轨；	台	1	调度模式
1 3	InfiniBand 交换机	InfiniBand 交换机	1U 36 FDR (56Gb/s) ports; 4.032Tb/s 交换容量 InfiniBand 交换机	台	1	数据交换

1 4	InfiniBand 高速网络	InfiniBand 及线 缆	3 米 FDR InfiniBand 铜缆	套	22	数据 传输
1 5	在线存储系 统	DS800-G20	4U60 盘位光纤存储系统： 2*控制器，采用 Active-Active 工作方式，采用存储专用 RSIC 处理芯片，有专用的 XOR 校验 芯片： 8*8GbFC 主机接 U：支持 IB、 万兆、千兆主机接 L1；24 均 TBSAS 硬盘： 48GB 高速缓存；存储数据磁盘 采用双硬件 Raid，系统整体可 靠性增强； 支持基于存储端的快照、本地 复制、远程镜像、动态磁盘资 源池等功能：支持万兆网络连 接，配置 4 个 Infiniband 接口 连接	套	1	存储 数据
1 6	备份存储系 统	DS600-G10	2 个控制器： 网络存储系统，支持 IP SAN, NAN，快照等功能： 主机 3U16 盘位，支持扩展至 64 个 硬盘位，支持 SSD、SAS、SATA 硬盘： 配置 16 个 3TBSAS 硬盘：支持 AID0, 1, 5, 6, 10, 50, 60； 双存储处理器：配备控制器后 备电池，满足 72 小时无电工 作；配置 16GB 高速缓存，最大 可扩展至 48GB；标配 4 个 1Gb ISCSI 主机接口，最大可扩展 至 10 个主机接口： 存储数据磁盘采用双硬件 Raid，系统整体可靠性增强：	套	1	存储 数据

1 7	I0 节点	曙光 I620-G20	<p>2U 机架式：  2*Intel Xeon E5 — 2680v3 处理器（12 核，主频 2.5GHz）；  板载 24 个内存插槽，配置 8 中 16GBDDR4 ECC 内存：2*600G 3.5 寸 15000 转 SAS 硬盘：  2*千兆以太网接口；  1*双端 UFC 8Gbps HBA 卡；  1*56Gb FDR InfiniBand HCA 卡：  可扩展 24 个热插拔 2.5 寸或者 12 个 3.5 寸 SATA/SAS 接 U 硬盘或固态硬盘；  最大可支持 8 个 PCI-E 扩展插槽：  集成八口 SAS 卡，支持 RAID0/1；  集成系统管理芯片，支持 IPMI2.0、KVMover IP、虚拟媒体等管理功能：  550W 1+1 冗余服务器电源：</p>	套	1	管理模式
1 8	操作系统	RedHat 64bit Linux 操作系统预装	RedHat 64bit Linux 操作系统预装	套	1	预报业务
1 9	集群软件	曙光 Gridvicw 集群综合管理系统 V3.2	曙光 Gridvicw 集群综合管理系统 V3.2（包含 12 个节点授权）	套	1	业务运行

20	应用开发环境（包括编译器、数学库、并行环境）	GNU 编译器，支持 C/C++/Fortran； Intel 编译器，支持 C/C++/Fortran； MKL、ACML、BLAS、LAPACK、ScaLAPACK、FFTW 等；OpenMP 并行环境；OpenMPI、MPICH2、MVPAICH2 等 MPI 并行环境（支持 InfiniBand 和以太网）； CUDA 驱动、编译器、调试器、工具包、SOK 等； CUDA FFT、CUDA BLAS 等； MIC 编译环境	GNU 编译器，支持 C/C++/Fortran；Intel 编译器，支持 C/C++/Fortran； MKL ACML、BLAS、LAPACK、ScaLAPACK、FFTW 等； OpenMP 并行环境； OpenMPI、MPICH2、MVPAICH2 等 MPI 并行环境（支持 InfiniBand 和以太网）； CUDA 驱动、编译器、调试器、工具包、SOK 等； CUDA FFT、CUDA BLAS 等； MIC 编译环境；	套	1	业务运行
21	千兆网络	千兆交换机	48 端口千兆交换机，48 个 10/100/1000base T 铜接口，2 个光接口；	台	1	数据传输
22		曙光集群控制台	1U 手动伸缩控制台（曙光 17”液晶显示器、鼠标、键盘、8 口切换器等）	台		数据传输
23		曙光 Cluskvm100	菊花链控制终端，每终端最大可支持 32 个节点	台		数据传输
24	服务器 HCA 卡	曙光单口 56Gb FDR InfiniBand HCA 卡	单口 56GbFDR InfiniBand HCA 卡	台	2	数据传输

25	服务器	Database、WORKER1、WEB	Windows server 2012 r2;24核; 2.5Ghz;128G;600G	台	1	预报业务
26		Worker	LinuxCentos7.7;32核; 2.4Ghz;128G;3.3T	台	1	预报业务
27	高性能图形工作站	THINK PAD P52	CPU主频 ≥2.0GHz; CPU数量 ≥2; 内存 ≥64GB; 硬盘 ≥1TB SSD 固态硬盘; 独立显卡 nVIDIA Quadro 4000 显卡 / 千兆网卡/标准键盘/光电鼠标 /Windows 7 64位专业版操作系统 / 22”宽屏液晶显示器	台	2	图形处理

## (2) 产品软件运维列表

### 数据库

包括 5 台 DB2 数据库，12 台达梦数据库，2 套 SQLSERVER 数据库、1 套 Postgresql 数据库、1 套 MongDB 集群以及 Oracle 数据库。

### 中间件

包括 3 套 weblogic 中间（其中两套 12c 版本，1 套 10 版本）、1 套应用集成运行平台（普元应用开发平台软件 V7.5(EOS Platform, 企业版)）、1 套企业门户平台软件 Portal（普元企业门户平台软件 PortalV7）。

### 办公和通讯产品

序号	区域	中间件名称	备注
1	政务外网	e-link 多平台即时通讯系统	即时通讯软件
2	政务外网	电子签章系统软件（管理端，包括 24 套数据证书认证服务）	电子签章系统软件（客户端）的管理
3	政务外网	电子签章系统软件（客户端）	支撑电子公文管理系统、行政许可审批系统、环境信访系统等业务系统的意

			见签批
4	政务外网	集成报表软件（集算报表专业版 5.0）	集算报表专业版 5.0

### GIS 软件产品

序号	区域	产品名称	备注
1	政务外网	GIS 桌面软件高级版 (ArcGIS Desktop 10.5 Advanced-S)	支撑省生态环境一张图系 统建设
2	政务外网	GIS 桌面软件空间分析 扩展模块 (ArcGIS Spatial Analyst 10.5 for Desktop-S)	支撑省生态环境一张图系 统建设
3	政务外网	GIS 企业级平台软件高 级版套件 (ArcGIS Enterprise 10.5 Advanced )	支撑省生态环境一张图系 统建设
4	政务外网	GIS 企业级服务器平台 影像大数据平台软件 (ArcGIS Image Server 10.5 )	支撑省生态环境一张图系 统建设

## (二) 运维内容

### (1) 基础网络及硬件运维服务

#### 1.1.1 日常工作

4、对基础网络及硬件运维列表中的设备资产进行资产使用情况登记。

- 5、提供硬件质保服务，包括但不限于硬件故障诊断、硬件故障处置及设备故障件更换等所需的所有费用。
- 6、在设备故障情况下，负责对故障设备进行维修或原厂返修。如需要备件顶替的，对备件进行现场安装调试。
- 7、维保服务费包括维修维护的人工费用、配件费用、备件费用、相关技术支持及培训在内的一切费用。
- 8、安排专人协助用户对资产进行梳理。

### 1.1.2 定期巡检工作

定期（每周）进行巡检，编写巡检记录表。

### 1.1.3 漏洞修复

积极配合用户等保测评、漏洞修复等相关工作。

### 1.1.4 运维报告

按月编写运维报告，包括日常问题记录及解决操作记录，巡检记录表、以及涉及漏洞修复内容。

## （2）数据库运维服务

包括 Oracle、DB2、sqlserver、Postgresql 和达梦等关系型数据库，以及 mongodb 数据库。

### 1.1.1 日常工作

- 9、保障数据库正常运行。
- 10、 数据库日常维护工作，包括维护用户、表、索引、视图、表空间等工作。
- 11、 配合用户进行等保测评等相关工作。
- 12、 使用监控软件进行监控，出现问题时及时处理。
- 13、 提供数据库相关的支持与咨询服务。

### 1.1.2 定期巡检工作

定期（每周）对数据库进行巡检工作，编写巡检记录表。

### 1.1.3 漏洞修复

积极配合用户漏洞修复等相关工作，包括修复前的测试验证及生产的修复工作。

### 1.1.4 备份恢复

定期对数据库进行备份操作，并在需要进行本机或异机的恢复操作。

### 1.1.5 性能优化

积极配合用户解决性能相关的问题，提出合理的性能优化建议并进行性能测试及验证工作。

### 1.1.6 运维报告

按月编写运维报告，包括日常问题记录及解决操作记录，巡检工作记录表、备份情况，性能优化工作记录，以及涉及漏洞修复内容等。

## (3) 中间件、办公和通讯、GIS 等软件运维

### 1.1.1 日常工作

- 14、保障中间件、办公和通讯、GIS 等软件正常运行。
- 15、中间件、办公和通讯、GIS 等软件日常维护工作，
- 16、对中间件、办公和通讯、GIS 等软件进行监控，出现问题时及时处理。
- 17、其他和中间件、办公和通讯、GIS 等相关的支持与咨询服务。

### 1.1.2 定期巡检工作

定期（每周）进行巡检，编写巡检记录表。

### 1.1.3 漏洞修复

积极配合用户等保测评、漏洞修复等相关工作，确保达到安全要求。

### 1.1.4 运维报告

按月编写运维报告，包括日常问题记录及解决操作记录，巡检记录表、以及涉及漏洞修复内容。

## (三) 响应服务

### 服务内容

针对巡检过程中发现的故障或隐患，及时消除不安全状态。响应采购人服务请求，及时处理故障，确保数据库正常运行。

提供 7\*24 小时的不间断处理，直至故障恢复。

### 响应时间

响应服务时间为工作时间 20 分钟，非工作时间响应时间 1 小时。级别一处理时限为 2 小时，级别二处理时限 4 小时，级别三处理时限 6 小时。

### 服务级别定义

#### 18、 级别一

造成运维软硬件不可用，影响相关系统或网络无法正常运行。

#### 19、 级别二

运维软硬件正常，但影响部分业务或网络正常运行。

#### 20、 级别三

软硬件性能优化、技术支持及咨询等服务。

### 服务要求

提供 7\*24 小时电话响应，远程+现场支持服务。

#### **（四）运维管理和考核办法**

根据软硬件产品特性，要求运维服务商须接受以下指标管理要求。7×24（含节假日）小时响应并处理，不符合故障处理要求扣除相应的考评分数，运维服务质量考核满分为100分，若年终服务考评分低于80分，将相应扣减服务费用。本考核方法是运维合同的重要组成部分，也是对运维工作进展考核的依据，目的是保证运维软硬件产品平稳运行，保障合同双方充分行使各自的职责和权益，本考核采用量化打分方式，按照考核细则进行年度考核和月度考核：考核评价：优秀：100-90分，良好：89-80分，合格：79-70分，一般：69-60，不合格：60以下。

月度考评全年累计有三个月为“一般”扣款人民币2万元，往后考评每累计增加一次“一般”扣款人民币2千元。月度考评全年累计有两次“不合格”扣款人民币2万元，往后考评每累计增加一次“不合格”扣款人民币3千元。上述情况不满足时，月度考评全年累计有一次“不合格”以及两次“一般”扣款人民币2万元。若因人为操作、违规操作、未及时响应等原因导致发生重大安全事故或对我单位产生重大影响的，每次扣款人民币2万元。对于运维的软硬件产品每发现或被通报1起弱口令时间，每次扣款人民币2千元。未经审批运维人员私自拷贝传输业务数据或违反保密管理规定，每次扣款人民币5千元。以上罚款如存在同一起事件参照最高罚款条款扣款，不进行重复罚款。

##### **（1）运维服务总体要求**

- 21、 提供7×24小时支撑服务；
- 22、 故障申告响应时限： 30分钟内；
- 23、 维护人员响应时间：见故障响应标准；
- 24、 故障恢复时限：见故障响应规格；
- 25、 故障的开始时间以用户申告记载并经运维方确认的时间为准，故障消除时间以运维方提供的并经用户确认的时间为准；
- 26、 网络中断，可根据客户提供详细的故障处理及分析报告；

27、 服务期内，运维方保障基础硬件和产品软件有效运行，保障过程中，涉及的软件产品性能和安全升级或漏洞修复等所产生的费用均包含在本次服务采购中，运维方承诺，采购人不再支付任何费用。

28、 具体服务期内平台、系统无故障率、故障指标承诺如下：

指标项目	承诺指标值（月）	指标提取及计算公式
I 级故障季发生次数	0 次	人工记录
II 级故障季发生次数	≤1 次	人工记录
III 级故障季发生次数	≤3 次	人工记录

## (2) 运维服务故障分级

为了确保在服务期内完成各项承诺指标, 严格根据故障级别进行故障处置, 故障分级和服务响应时间表如下所示。

故障级别	技术人员到场时间	提出解决方案	备件到场时间（涉及硬件）	解决时间
I 级：属于重特大故障；其具体现象为：系统崩溃	驻点人员立即到达现场	到达现场后 1 小时内提交故障解决方案	提出解决方案后 1 小时到达现场	8 小时以内
II 级：属于严重问题；其具体现象为：部分系统发生故障、或小面积瘫痪但不影响系统整体运行	驻点人员 30 分钟以内到达现场	到达现场后 1 小时内提交故障解决方案	提出解决方案后 1 小时到达现场	8 小时以内

<p>III 级：属于较严重问题； 其具体现象为：部分系统 小部分功能失效或出现报 错、告警或故障，但该子 系统仍能继续运行。</p>	<p>驻点人员 1 小时以内 到达现场</p>	<p>到达现场后 1 小时 内提交故障解决方 案</p>	<p>提出解决方案后 8 小时到达现场</p>	<p>12 小时 以内</p>
<p>IV 级：属于普通问题</p>	<p>2 小时以内 驻点人员 到达现场 或者立即 远程在线 解决</p>	<p>限时提交或到达现 场后 1 小时内提交 故障解决方案</p>	<p>视情况而定</p>	<p>24 小时 以内</p>

### (3) 运维服务考核细则

#### 运维服务

按照以下考核细则进行年度考核和月度考核（若因人为操作、违规操作、未及时响应等原因导致发生重大安全事故或对我单位产生重大影响的该月份考核直接为“不合格”）。

序号	考核项	考核项	考核要求	考核内容	考核方法	扣分说明
1	运维服务总体要求（20分）	1、维护	维护周期 12 个月，运行维护期内，运行运维公司提供 7×24 小时系统运行维护服务。	运行维护期内，运行运维单位提供运行维护服务时效性	通过办公电话、手机方式，抽查运行运维公司是否在工作时间段（每天 8 点-18 点）提供线上运维服务，其余时间段是否能提供 7×24 小时紧急运维服务	任何时间段接到用户反馈，未在半个小时内响应，扣 1 分；收到用户投诉，扣 1 分。
2		工作指标要求	运行维护期内，如甲方有重大事件保障、重大系统升级时，维护方应在 2 小时内指派专业技术人员到场协助。	紧急状态下，运维单位响应的及时性	重大事件保障、重大系统升级时，技术人员到场处理	有重大事件保障、重大系统升级时，协助人员未能到场处理，扣 1 分。

3	规范要求（18分）	2、维护工作基本要求	严格遵循安全规范操作制	数据库、硬件设备等相关操作的规范性和安全性	数据库升级、数据变更或设备升级处理需提前申请，经相关负责人员审批通过后方可实施。	未经审批，私自升级或变更操作，扣2分，如果导致数据丢失或出现运维事故，扣3分；其他未按照运维管理规范实施生产操作，扣1分；实施过程导致重大安全问题，按照I/II/III等级，分别扣3分、2分、1分。
			度，确保安全第一；	系统升级及数据变更相关操作的规范性和安全性	系统升级或数据变更处理需提前申请，告知系统负责人和数据管理人员，通过后方可实施。	未经审批，私自上线代码或修改数据，扣2分，如果导致系统出现异常，扣3分。其他未按照运维管理规范实施生产操作，扣1分；实施过程导致重大安全问题，按照I/II/III等级，分别扣3分、2分、1分。
			运维人员进行规范化、标准	运维人员变更及时填写	抽查实际运维人员是否	登记报备。运维人员变更，未报备登记，扣1分。

			化管理，确保 运维服务及时 响应	人员变更申 请单提交备 案		
				驻场运维人 员按照业主 上下班时间 正常上班，不 请假不得离 岗。	抽查驻场运维人员上下 班时间以及考勤情况。	上下班迟到，发现一 次扣 1 分；未请假离 岗，扣 2 分。
				是否签订安 全保密协议	抽查是否签订安全保密 协议	未签订安全保密协 议，扣 1 分。
			是否按照海南	数据日常管 理	数据拷贝传输，必须经 过审批后，通过安全介 质和网络进行传输	未经审批，跨业务、 跨系统、跨层级私自 拷贝传输数据，扣 2 分；违反保密管理规 定，处理数据，扣 2 分。
			省相关网络安 全要求	网络安全防 控管理	按照海南省电子政务云 管理规范、电子政务外 网网络安全管理规范、 海南省电子政务外网信 息系统安全基线配置管 理规范（标准）以及应 用系统运维管理制度等	发现一次安全问题 （含被外部门通 报），扣 1 分；发现 一次违反安全管理 规定，扣 1 分；发现 一次弱口令，扣 2 分。

					相关安全管理要求，开展巡检和抽查。	
					网络安全问题处理修复服务时效性	发现安全问题，存在高危风险，未能在 24 小时内处理，扣 2 分；
4	日常技术支持 (20分)	3、日常技术支持	对于软硬件产品故障，维护技术支持中心在电话支持和远程支持不能解决问题的情况下，故障响应时间小于 1 小时，2 小时内技术人员线上或现场确认故障问题及出具解决方案。	发生故障后，运维单位响应的及时性	系统故障是否在 24 小时内处理	超过规定时间未及时处理，每发生一起扣 1 分。
				软硬件日常运维工作及	接收运维需求后 8 小时内响应，评估合理时间内及时解决	接收运维需求任务后 8 小时未响应，扣 1 分；未在合理评估时间内解决的，扣 2 分；对于运维任务无

						任何理由迟迟不解决，未闭环处理，扣3分。
6	故障响应机制（10分）	4、	运维公司需制定故障维护响应机制。一般故障 4 小时内，重大故障和紧急要求 30 分钟内作出响应和评估，确定故障排除的时间和排除的方法。如不能确定故障，运维公司将协调公司和供应商的资源和客户确定现场服务的时间，保证系统在最快的时间内恢复。	运维单位故障维护响应机制制定情况；发生故障后，运维单位响应的及时性	抽查 1. 运维单位是否制定故障维护响应机制； 2. 一般故障是否在 4 小时内，重大故障和紧急情况下是否在 30 分钟内作出响应和评估	未制定故障维护响应机制，扣 1 分；超过规定时间未响应的，每发生一起扣 1 分。
7	定期巡检服务	7、	为了保证系统的正常运行，	运维单位巡检制度制定	每周核查： 1. 运维单位是否制定巡检制度； 2.	未制定巡检机制，扣 1 分；超过规定时间

	(10分)	期 巡 检 服 务	运维公司应设立巡检制度，对系统进行全面检查，排除存在的隐患，并向甲方提交巡检报告。	情况；巡检报告提交的时效性	是否每月5日前，提交上月运维报告	未提交报告等，每发生一起扣1分。运维报告内容质量差的
--	-------	-----------------------	---	---------------	------------------	----------------------------

### （五）验收要求

#### 29、 验收形式

提交年度运维服务报告，每月运维报告作为附件材料提供。

#### 30、 验收标准

完成合同约定运维服务内容。

#### 31、 验收方法

组织验收会议验收。

### 三、项目相关要求（带★的参数为重要参数，不满足作废标处理）

1、运维服务期（**服务期**）：项目运维服务期为12个月。

2、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

3、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。

4、报价人要保持同采购人的密切联系，遇有重大事项及时报告和反馈信息，尊重项目业主方的意见，接受项目业主方的提议、监督和指导。

5、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

★6、若签订合同日期晚于上年度服务截止期，成交供应商应向上一年度供应商支付超出上一年度运维服务期限的费用。费用计算规则=实际服务天数\*(上一年度合同金额/365)。

7、支付条件：

付款条件：计划分三笔款支付。

第一次支付：双方合同签订后 5 个工作日内，中标方提供正规发票后，支付中标额 50%款项；第二笔支付：中标方结清项目相关系统原运维厂商 2024 年已产生运维费用后，提交实施方案且提交一个月运维报告后，支付中标额 40%款项；第三笔支付：12 月，提交项目成果，支付项目尾款。

# B 包用户需求书

## 一、项目名称及采购内容

项目名称：海南省生态环境厅信息化运行维护项目（2024 年）

采购内容：应用系统、数据运维以及相应网络安全升级服务

预算额度：212.45 万元。

## 二、项目内容及要求

本项目旨在加强海南省生态环境厅正在使用的海南省生态环境综合监管平台（一期）、海南省生态环境监测信息系统、海南省污染源调查管理及资源环境承载能力监测预警系统、综合门户管理系统、生态环境电子公文系统等系统运行监控、日常维护以及部分功能升级，确保系统的正常运行，切实保障相关业务的正常开展，营造良好的营商环境，更好地利企便民。

运维服务的目标是，对现有的信息系统基础资源进行监控和管理，及时掌握信息系统资源现状和配置信息，反映信息系统资源的可用性情况和正常运行状况，创建一个可知可控的 IT 环境，保证信息系统的各类业务应用系统的可靠、高效、持续、安全运行。

采购单位：海南省环境科学研究院。

服务质量要求：中标方应按照国家相关规范、合同及甲方提出的具体要求，按时以书面形式提交运维管理考核中要求的相应报告。

项目需求

### （一）运维范围

本项目为海南省生态环境厅信息化运行维护项目（2024 年），主要运维系统项目包括：海南省生态环境综合监管平台（一期）建设项目、海南省生态环境监测信息、海南省污染源调查管理及资源环境承载能力监测预警、海南省生态环境综合办公等系统。

项目运维涉及以下四部分项目系统的应用系统及数据运维, 以及相应网络安全升级服务:

#### 1、海南省生态环境综合监管平台(一期)建设项目

运维服务包括数据资源中心、环境地理信息系统、放射源监管子系统、行政许可审批子系统、排污许可证管理子系统、环境应急管理子系统、环境监察移动执法子系统、环境影响评价管理系统、企收服务中心、污染源监管信息公开系统、海南省机动车环保检验管理系统等。

#### 2、海南省生态环境监测信息系统项目

运维服务包括污染源监测综合管理系统、污染源在线监控系统、昌江核电厂辐射环境现场监测系统、大气环境综合信息管理系统、土壤环境信息综合管理、水环境综合信息管理、环保督察工作管理、清洁生产审核管理、生态环境监测数据共享利用及发布、生态环境监测网络建设项目管理、社会环境服务机构管理、环境质量数据管理系统等系统。

#### 3、海南省污染源调查管理及资源环境承载能力监测预警系统项目

运维服务包括禁塑工作管理平台、海南省污染源调查管理信息系统等。

#### 32、 海南省生态环境综合办公系统

运维服务包括综合门户管理系统、生态环境电子公文系统、电子签章系统软件、即时通讯系统等。

#### 33、 系统升级内容

升级内容包括海南省生态环境综合办公系统(综合门户管理、生态环境电子公文、电子签章、即时通讯)部分功能升级以及对应应用接入海政通、海南省生态环境综合监管平台(一期)(环境影响评价系统、行政许可审批系统)部分功能升级。

## (二) 运维内容

### 1、基础服务内容

#### 34、 系统日常巡检

安排对定制应用系统、基础平台软件（中间件）、服务器操作系统及服务器资源状态开展定期巡检并做好巡检记录。服务内容包括检查系统功能是否正常稳定运行，核查业务系统中展示相关数据是否存在问题，以及系统使用情况分析；服务器操作系统及服务器资源使用状态等。结合实际应用及时优化性能参数，确保定制系统及产品软件稳定运行，及时记录巡检日志。巡检频次要求每周例行检查 1 次，每月至少大巡检 1 次，节假日重点检查。巡检记录每月汇总发由应用系统负责人确认留档。

### 35、 系统故障处理服务

对于系统故障，按要求及时跟进排查分析，及时解决恢复系统正常运行，及时上报系统故障分析报告。故障分析报告需提交给应用系统负责人并留档。

### 36、 数据归集及服务

按照海南省数据资源管理相关办法，开展数据资源梳理及编目，将业务数据归集至数据中心，同步开展数据归集监控及数据质量核查工作，数据归集统一使用省数据共享交换平台开展。数据质量核查工作需要每月进行，按要求分月、季度、以及年度提交数据归集及核查报告。

### 37、 系统功能完善及优化

提供原有功能缺陷以及便捷性等需要而产生的程序修改服务；根据业务新政策新要求新标准及行业发展趋势，以及应用系统用户的使用情况及运维人员反馈情况，评估当前应用的功能及性能，提出优化升级建议，对系统进行功能性完善和优化升级。

### 38、 程序及数据备份

根据系统特点，制定备份策略，按要求对系统代码、数据开展备份，保障系统稳定运行。系统源代码提交 git 代码仓库，同步提交系统开发环境程序。

### 39、 系统值守及指导服务

为保证应用系统的高稳定可用，提供每日 7×24 小时的电话、QQ、微信等在线支持服务，根据用户及服务人员的问题和咨询，进行解答和指导。

### 40、 系统培训和文档更新

对于新增功能变化需面向用户开展系统使用指导，根据甲方要求开展不定期系统培训。

系统文档需及时更新完善，对系统包括但不限于用户操作手册、部署手册、产品技术手册等。

#### 41、 运维台账管理

运维工程师必须记录运维台账，进行记录问题及其跟进处理解决。记录所有系统问题、故障、优化升级或者对应咨询沟通等等相关记录，明确发生时间、反馈人、问题需求描述、处理计划、处理措施、完成时间、是否通知或反馈用户等等闭环的整体记录。要求按照时限要求完成运维台账列举任务，并按月汇总至月度运维报告并提交业务负责人确认留档。

#### 42、 系统升级内容

#### 43、 综合门户管理系统

门户：门户应用系统的系统管理功能优化，增加按角色名称搜索功能，实现查询某个角色关联哪些应用系统。

信访系统：厅主办及交办市县的板件增加延迟申请流程；厅主办处室办理页面、交办市县办理经办人以及管理后台均可填写原由发起延迟申请，所有发起延迟申请任务均流转到“信访处分发环节”签批同意即可相应延迟最多30天，避免办件超时。增加受理和延期两类短信发送功能，以厅名义落款，并可查看发送信息记录，姓名和手机号从登记信息自动获取，信访受理人员在查询页面点击发送，1类 受理告知书：姓名你反应的信访事项，我厅已受理，将于60日内答复。2类 延期办理告知书：姓名你反应的信访事项，因情况复杂，根据信访工作条例规定，需延长办理期限30天，请耐心等待。信访发文后，在主办处室办理或是否反馈省厅环节提供获取盖章定稿功能，在信访办理文件页面点击获取发文自动读取发文数据。

问题反馈系统：问题清单新增时，问题分类选择硬件问题、网络问题或综合问题时，运维单位也要可以选择。新建基础库字典存放运维单位，当问题分类选择硬件问题、网络问题或综合问题这三类时运维单位从新建字典里读取。问题清单增加新增“所属系统”功能。系统故障增加新增“系统名称”

功能。

管理制度子系统：增加制度采集和文件交换功能。增加提供制度数据检索和详情查看。增加对接办公系统接口。系统权限设计和细分。

#### 44、 生态环境电子公文系统

会签收文功能：新增省厅会签收文流程、会签收文查询功能、会签收文管理功能。支持根据公文协同接收公文启动收文流程

统一流程引擎：提供对外流程引擎接口（包括流程实例接口、流程任务接口、常用语接口共20个），提供统一流程业务系统管理管理功能。

组织机构管理：在新系统中按旧系统重构组织机构功能，包括机构、岗位、人员的管理功能。从旧系统同步用户信息时，不同步旧用户的密码。人员增加配置不接收传阅任务。机构支持配置是否在机构树上显示岗位。

流程监控：支持已结束流程实例重启。在流程监控中可重启、终止、新建、完成活动实例。可重启、终止、下传任务。

通用签章管理：增加通用签章管理功能，支持屏蔽使用通用签章功能签写的意见。

收文发文：发文的公开属性增加“内部公开”选项，内部公开的发文只公开在政务外网门户不公开到互联网门。发文流程，机要室盖章完后，自动启动处室办文流程，在办文流程的主办处室分发环节增加“添加制度”功能，允许用户将当前发文文件传输至制度管理系统。收文流程-主办处室办理（各处室签批）环节增加“添加制度”功能，允许用户将当前收文文件传输至制度管理系统。

配合对接集成wps文档中台升级版本：配合wps文档中台的升级版本，进行对接对应的配置调整、测试及验证。

请示报告：主办处室办理环节增加“添加制度”功能，允许用户将当前请示文件传输至制度管理系统。

配合密评的安全升级：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。系统升级使用https协议，即浏览器需要通过https访问

应用系统。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。应用系统的重要数据（用户登录账号密码、身份证号码、手机号码）在存储时采用合规的密码技术保证重要数据的机密性。统一使用国产化加密接口加密数据。需要修改使用到身份证、手机号码的组织机构管理及短信发送功能，读取后数据需要先解密。系统操作日志使用密码技术保证日志记录的完整性。所有系统用户的操作行为日志是存储在数据库表，统一使用国产化算法保障完整性；增加前端展示日志功能和比对校验完整性功能。

#### 45、 电子签章系统软件

定制开发签章记住密码：电子签章业务，优化在不同业务系统中进行H5网页签章操作，操作内容包括插入ukey，输入密码和勾选记住密码。需要优化成在统一协议、域名和端口的情况下，在A业务系统中进行网页签章勾选记住密码后，需要在B、C、D等业务系统中进行签章时，无需再次输入签章密码；签章密码变更后需要手动重新输入密码

签章历史数据兼容展示等功能：在不同业务系统中实现，H2网页签章数据能兼容在H5网页签章中显示H2签章历史数据。目前厅业务系统升级改造集成了H5网页签章，但是原先生态厅的业务系统采用的H2网页签章，H2网页签章的历史数据需要在H5中兼容展示。

#### 46、 即时通讯系统

在即时通讯中涉及组织架构、账号密码、人员信息等部分，需要和“海南省生态环境综合管理平台”保持同步，并且配合密评的安全升级处理：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。系统升级使用https协议，即浏览器需要通过https访问应用系统。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。应用系统的重要数据（用户登录账号密码、身份证号码、手机号码）在存储时采用合规的密码技术保证重要数据的机密性。统一使用国产化加密接口加密数据。需要修改使用到身份证、手机号码的组织机构管理及短信发送功能，读取后数据需要先解密。系统操作日志使用密码技术保证日志记录的完整性。所有系统用户的操作行为日志是存储在数据库表，统一使用国产化算法保障完整性；增加前端展示日志功能和比对校验完整性功能。

#### 47、应用接入海政通

海南省生态环境厅电子公文管理系统：省厅办公系统的收文、发文、请示报告等签批流程页面支持，文件上传、在线预览、在线编辑等。

市县生态环境局电子公文管理系统：市县局办公系统的收文、发文、请示报告等签批流程页面支持，文件上传、在线预览、在线编辑等。

事业单位电子公文管理系统：事业单位办公系统的收文、发文、请示报告等签批流程页面支持，文件上传、在线预览、在线编辑等。

海南省生态环境厅差假管理系统：差假申请、签批、查看详情、查询。用车申请、签批、查看详情、查询等。

事业单位差假管理系统：差假申请、签批、查看详情、查询。用车申请、签批、查看详情、查询等。

信访管理系统：信访系统案件签批、在线转办、案件查询、文件在线预览等功能。

依申请公开：依申请公开申请流程签批、查询、文件在线预览。

领导日程：查询领导日程信息。

#### 48、环境影响评价管理系统

涉及数据管理、数据查询、技术评估文件管理、评估退件、二次评估等功能新增、升级、优化。

#### 49、行政许可审批子系统

涉及市县数据归集、生态环境领域政务服务事项、电子证照、统一办事入口、环评上报兼容辐洋辐射等功能新增、升级、优化。

### 3、系统安全及密评安全升级

#### (1) 安全升级服务

及时做好系统及软件产品漏洞修复和升级，对等保测评、渗透测试等安全评估发现的问题，及时整改完善，包括但不限于应用代码开发、配置、数据库表变更及补丁升级等。

#### 50、密码升级服务

采用省大数据管理局提供的政务云密码资源服务，结合系统实际情况，开展密码升级改造，确保系统密评工作完成。

#### 4、驻点服务

驻点服务人员需要按时打卡上下班，工作日上班时间是8:00-18:00.

序号	运维服务项目	单位	数量	备注
1	驻点人员	人	2	

#### 5、运维材料要求

巡检记录每月汇总发由应用系统负责人确认留档。

按月、季度以及年度提交数据归集及核查报告。

按月提交运维报告，并提交业务负责人确认留档。运维结束前提交年度整体运维报告。运维报告包括但不限于以下内容：运维整体情况、当月运维存在问题及解决处置情况、重大故障及响应情况、漏洞修复及安全保障情况、巡检及监测预警情况、各类备份及下月运维计划等内容，同步提供日常运维支撑材料（如运维台账、升级单、巡检报告、计划措施、驻点人员考勤记录等）。

系统发生故障影响导致系统无法使用，需及时解决并提交系统故障报告。报告包括故障描述、故障原因、影响范围、解决措施、事故总结及整改意见等。

系统如需升级优化，需提交系统升级实施单。升级实施单包括升级原因、升级事项、影响范围及风险评估、实施计划、预计升级时间等。

运维公司和甲方需签署公对公保密协议，以及驻场和远程运维人员的个人保密协议。

### （三）服务要求

#### 服务响应

## 1. 响应时间

响应服务时间为工作时间 20 分钟，非工作时间响应时间 1 小时。级别一处理时限为 2 小时，级别二处理时限 4 小时，级别三处理时限 6 小时。按错误级别：程序错误 24 小时内完成，数据错误 8 小时内完成，配置错误 4 小时内完成。

## 2. 服务级别定义

级别一：造成系统或者产品软件不可用，影响相关业务系统不能正常访问。

级别二：系统或者产品软件访问正常，但影响部分业务正常运行。

级别三：系统或者产品软件性能优化、系统或者产品软件技术支持及咨询等服务。

## 服务方式

1. 电话支持服务（7×24 小时），需保持服务电话 24 小时畅通，“系统”出现问题及时响应；

2. 远程诊断、远程维护；

3. 日常咨询服务；涉及系统使用和系统优化等日常咨询,需当日安排驻场运维人员上门或者电话回复，详细记录和解答咨询；

4. 配合做好网络安全防护工作，如“系统”存在安全风险，负责对该安全风险进行修复；

5. 技术支持服务：若甲方的软硬件、系统出现任何故障，远程运维或者现场运维人员接到电话、邮件、传真、短信、微信等方式通知维修后，应在约定时限内响应，提供现场或者远程技术支持。远程运维的公司，问题无法远程解决时，工程师应在 2 日内到达故障现场(差旅及食宿费由运维单位自)，分析故障，找出故障原因。无论远程还是现场运维，原则上 24 小时内解决故障或提出书面替代方案，以书面的方式提交故障报告，并将相关文档进行备案记录，以备日后查询。未在约定期限内完成维护义务的，甲方有权委托第三方技术单位代替履行维护义务，有义务做好配合，产生费用由乙方承担。

## 维护服务要求

1. 按照运维管理制度，做好运维保障工作，同时按照运维地上下班作息时间做好日常技术服务工作；
2. 做好系统日常巡检、客户提出的问题处理、客户使用操作解答等工作，确保系统稳定提供服务；按要求每月提交运维工作报告，运维期限结束后提供总运维工作报告；
3. 提供售后维护服务过程中，对获知的数据信息等负有保密责任，非经书面同意，不得向任何第三方披露，开展运维技术人员均签订保密协议；
4. 提供技术服务过程中所形成的知识产权归海南省环境科学研究所所有；
5. 不得在非授权情况下，将系统、程序和数据违规下载传输至非授权的存储空间或者公有云服务器。所有系统定制开发代码均需提交代码库中，并及时更新。

## （四）运维管理和考核办法

2024年海南省生态环境厅信息化运行维护项目将加强考核管理，通过制定质量考核办法和机制，提升运维效率，保证信息系统平稳运行。

根据系统特性，要求运维服务商须接受以下指标管理要求。7×24（含节假日）小时响应并处理，不符合故障处理要求扣除相应的考评分数，运维服务质量考核满分为100分，若年终服务考评分低于80分，将相应扣减服务费用。本考核方法是运维合同的重要组成部分，也是对运维工作进展考核的依据，目的是保证运维单位信息系统平稳运行，保障合同双方充分行使各自的职责和权益，本考核采用量化打分方式，按照考核细则进行年度考核和月度考核：考核评价：优秀：100-90分，良好：89-80分，合格：79-70分，一般：69-60，不合格：60以下。

月度考评全年累计有三个月为“一般”扣款人民币2万元，往后考评每累计增加一次“一般”扣款人民币2千元。月度考评全年累计有两次“不合格”扣款人民币2万元，往后考评每累计增加一次“不合格”扣款人民币3千元。上述情

况不满足时，月度考评全年累计有一次“不合格”以及两次“一般”扣款人民币2万元。若因人为操作、违规操作、未及时响应等原因导致发生重大安全事故或对我单位产生重大影响的，每次扣款人民币2万元。对于运维的软硬件产品每发现或被通报1起弱口令时间，每次扣款人民币2千元。未经审批运维人员私自拷贝传输业务数据或违反保密管理规定，每次扣款人民币5千元。以上罚款如存在同一起事件参照最高罚款条款扣款，不进行重复罚款。

#### 51、 运维服务总体要求

- 52、 提供7×24小时支撑服务；
- 53、 故障申告响应时限：30分钟内；
- 54、 维护人员、设备备件到达现场时间：见故障响应标准；
- 55、 故障恢复时限：见故障响应规格；
- 56、 故障的开始时间以用户申告记载并经运维方确认的时间为准，故障消除时间以运维方提供的并经用户确认的时间为准；
- 57、 网络中断，可根据客户提供详细的故障处理及分析报告；
- 58、 服务期内，运维方保障系统有效运行，保障过程中，涉及的系统升级优化等所产生的费用均包含在本次服务采购中，运维方承诺，采购人不再支付任何费用。
- 59、 具体服务期内平台、系统无故障率、故障指标承诺如下：

指标项目	承诺指标值（月）	指标提取及计算公式
I级故障季发生次数	0次	人工记录
II级故障季发生次数	≤1次	人工记录
III级故障季发生次数	≤3次	人工记录

#### 60、 运维服务故障分级

为了确保在服务期内完成各项承诺指标，严格根据故障级别进行故障处置，故障分级和服务响应时间表如下所示。

故障级别	技术人员到场时间	提出解决方案	解决时间
I 级：属于重特大故障；其具体现象为：系统崩溃	驻点人员立即到达现场	到达现场后 1 小时内提交故障解决方案	8 小时以内
II 级：属于严重问题；其具体现象为：部分系统发生故障、或小面积瘫痪但不影响系统整体运行	驻点人员 30 分钟以内到达现场	到达现场后 1 小时内提交故障解决方案	8 小时以内
III 级：属于较严重问题；其具体现象为：部分系统小部分功能失效或出现报错、告警或故障，但该子系统仍能继续运行。	驻点人员 1 小时以内到达现场	到达现场后 1 小时内提交故障解决方案	12 小时以内
IV 级：属于普通问题	2 小时以内驻点人员到达现场或者立即远程在线解决	限时提交或到达现场后 1 小时内提交故障解决方案	24 小时以内

## 61、 运维服务考核细则

### 运维服务总体考核项

#### 运维服务

按照以下考核细则进行年度考核和月度考核（若因人为操作、违规操作、未及时响应等原因导致发生重大安全事故或对我单位产生重大影响的该月份

考核直接为“不合格”）。

序号	考核项	考核项	考核要求	考核内容	考核方法	扣分说明
1	（一） 运维服 务总体 要求 （20 分）	1、 维 护 工 作 指 标 要 求	维护周期 12 个月，运行维护期内，运行运维公司提供 7×24 小时系统运行维护服务。	运行维护期内，运行运维单位提供运行维护服务 时效性	通过办公电话、手机方式，抽查运行运维公司是否在工作时间段（每天 8 点-18 点）提供线上运维服务，其余时间段是否能提供 7×24 小时紧急运维服务	任何时间段接到用户反馈，未在半个小时内响应，扣 1 分；收到用户投诉，扣 1 分。
2			运行维护期内，如甲方有重大事件保障、重大系统升级时，维护方应在 2 小时内指派专业技术人员到场协助。	紧急状态下，运维单位响应的及时性	重大事件保障、重大系统升级时，技术人员到场处理	有重大事件保障、重大系统升级时，协助人员未能到场处理，扣 1 分。
3	规范要求（18 分）	2、 维 护 工	严格遵循安全规范操作制度，确保安全第一；	数据库、硬件设备等相关操作的规范性和安全性	数据库升级、数据变更或设备升级处理需提前申请，经相关负责人员审批通过后才可实施。	未经审批，私自升级或变更操作，扣 2 分，如果导致数据丢失或出现运维事故，扣

		作 基 本 要 求			3分；其他未按照运维管理规范实施生产操作，扣1分；实施过程导致重大安全问题，按照I/II/III等级，分别扣3分、2分、1分。
			系统升级及数据变更相关操作的规范性和安全性	系统升级或数据变更处理需提前申请，告知系统负责人和数据管理人员，通过后才可实施。	未经审批，私自上线代码或修改数据，扣2分，如果导致系统出现异常，扣3分。其他未按照运维管理规范实施生产操作，扣1分；实施过程导致重大安全问题，按照I/II/III等级，分别扣3分、2分、1分。
		运维人员进行规范化、标准化管理，确保运维服务及时	运维人员变更及时填写人员变更申请表提交备案	抽查实际运维人员是否登记报备。	运维人员变更，未报备登记，扣1分。
		响应	驻场运维人	抽查驻场运维人员上下	上下班迟到，发现一

				<p>员按照业主 上下班时间 正常上班,不 请假不得离 岗。</p>	<p>班时间以及考勤情况。</p>	<p>次扣 1 分; 未请假离 岗, 扣 2 分。</p>
				<p>是否签订安 全保密协议</p>	<p>抽查是否签订安全保密 协议</p>	<p>未签订安全保密协 议, 扣 1 分。</p>
			<p>是否按照海南 省相关网络安 全要求</p>	<p>数据日常管 理</p>	<p>数据拷贝传输, 必须经 过审批后, 通过安全介 质和网络进行传输</p>	<p>未经审批, 跨业务、 跨系统、跨层级私自 拷贝传输数据, 扣 2 分; 违反保密管理规 定, 处理数据, 扣 2 分。</p>
				<p>网络安全防 控管理</p>	<p>按照海南省电子政务云 管理规范、电子政务外 网网络安全管理规范、 海南省电子政务外网信 息系统安全基线配置管 理规范(标准)以及应 用系统运维管理制度等 相关安全管理要求, 开 展巡检和抽查。</p>	<p>发现一次安全问题 (含被外部门通 报), 扣 1 分; 发现 一次违反安全管理 规定, 扣 1 分; 发现 一次弱口令, 扣 2 分。</p>
					<p>网络安全问题处理修复 服务时效性</p>	<p>发现安全问题, 存在 高危风险, 未能在 24</p>

						小时内处理,扣2分;
4	日常技术支持 (20分)	3、日常技术支持	对于软硬件产品故障,维护技术支持中心在电话支持和远程支持不能解决问题的情况下,故障响应时间小于1小时,2小时内技术人员线上或现场并确定故障问题及出具解决方案。	发生故障后,运维单位响应的及时性	系统故障是否在24小时内处理	超过规定时间未及时处理,每发生一起扣1分。
				软硬件日常运维工作及时性	接收运维需求后8小时响应,评估合理时间内及时解决	接收运维需求任务后8小时未响应,扣1分;未在合理评估时间内解决的,扣2分;对于运维任务无任何理由迟迟不解决,未闭环处理,扣3分。

6	故障响应机制 (10分)	4、故障响应机制	<p>运维公司需制定故障维护响应机制。一般故障 4 小时内，重大故障和紧急要求</p> <p>30 分钟内作出响应和评估，确定故障排除的时间和排除方法。如不能确定故障，运维公司将协调公司和供应商的资源和客户确定现场服务的时间，保证系统在最快的时间内恢复。</p>	<p>运维单位故障维护响应机制制定情况；发生故障后，运维单位响应的及时性</p>	<p>抽查 1. 运维单位是否制定故障维护响应机制； 2. 一般故障是否在 4 小时内，重大故障和紧急情况下是否在 30 分钟内作出响应和评估</p>	<p>未制定故障维护响应机制，扣 1 分；超过规定时间未响应的，每发生一起扣 1 分。</p>
7	定期巡检服务 (10分)	7、定期巡检	<p>为了保证系统的正常运行，运维公司应设立巡检制度，对系统进行全</p>	<p>运维单位巡检制度制定情况；巡检报告提交的时效性</p>	<p>每周核查：1. 运维单位是否制定巡检制度； 2. 是否每月 5 日前，提交上月运维报告</p>	<p>未制定巡检机制，扣 1 分；超过规定时间未提交报告等，每发生一起扣 1 分。运维报告内容质量差的</p>

		服 务	面的检查，排除存在的隐患，并向甲方提交巡检报告。			
--	--	--------	--------------------------	--	--	--

### 三、项目相关要求（带★的参数为重要参数，不满足作废标处理）

1、运维服务期（服务期）：项目运维服务期为 12 个月。

2、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

3、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。

4、报价人要保持同采购人的密切联系，遇有重大事项及时报告和反馈信息，尊重项目业主方的意见，接受项目业主方的提议、监督和指导。

5、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

★6、若签订合同日期晚于上年度服务截止期，中标单位应向上一年度供应商支付超出上一年度运维服务期限的费用。费用计算规则=实际服务天数\*（上一年度合同金额/365）。

7、支付条件：

付款条件：计划分三笔款支付。

第一次支付：双方合同签订后 5 个工作日内，中标方提供正规发票后，支付中标额 50%款项；第二笔支付：中标方结清项目相关系统原运维厂商 2024 年已产生运维费用后，提交提交实施方案且提交一个月运维报告后，支付中标额 40%款项；第三笔支付：12 月，提交项目成果，支付项目尾款。

# C包用户需求书

## 一、项目名称及采购内容

项目名称：海南省生态环境厅信息化运维项目（2024年）

采购内容：门户网站信息化系统运维

预算额度：14.83万元

## 二、项目内容及要求

### 一）项目概况

海南省生态环境厅门户网站信息化系统运维即将超出维保期，需要继续对系统的软硬件设备进行日常的运维，出现故障及时得到处理和维修。通过对在用系统开展良好的运维服务，监控和管理现有的信息系统基础资源，及时掌握信息系统资源现状和配置信息，反映信息系统资源的可用性情况和健康状况，创建一个可知可控的IT环境，从而保证信息系统的各类业务应用系统的可靠、高效、持续、安全运行，运维服务主要包括针对门户网站的日常基础运维服务，包括对前端页面基础组件和后台管理应用软件的维护，及时响应解决客户技术问题，回答客户对于站点管理的相关咨询服务；除此以外还包括客户提出的基于门户网站的个性化服务需求，包括监测云平台的监测整改服务，等保测评结果的整改服务，重大节日及活动专人值班保障活动等，为门户网站的良好运行提供技术保障。

为了更好的体现门户网站的公共服务能力，本次还增加了在门户网站页面的智能问答功能，通过建立知识库，梳理常见问题，建立智能问答库，实现在线问答功能。

1、采购单位：海南省环境科学研究院。

2、服务质量要求：中标方应按照国家相关规范、合同及甲方提出的具体要求，按时以书面形式提交成果。

## 二) 项目需求

### 62、 运维服务内容及要求如下表:

序号	运维服务项目	单位	数量	备注
1	门户网站技术 运维服务(基础 运维)	次/年	12.0 0	基础软件巡检服务:对海南省生态环境厅门户网站的基础应用前端软件进行日常巡检与维护,定时多次进行例行巡检,保障前端应用软件正常进行。对数据库及其他数据存储系统进行监控、配置调整、优化、升级和漏洞修复,数据库建立完善的数据备份和恢复机制,定期检查数据备份和恢复备份机制是否有效,对前端基础应用软件提供例行技术支持。
2	网站内容管理 平台及互动应 用系统安全运 维服务(基础运 维)	系统/ 年	1.00	网站日常巡检服务:单位网站的页面和应用功能组件进行日常巡检,确保页面(含主页、重要栏目页面)的信息、图表和附件的可用性以及链接的可用性和准确性,保证应用功能正常运行。
3	故障处理服务 (基础运维)	系统/ 年	1.00	及时处理网站的内容管理平台及互动应用系统的运行故障,制定完善可行的常见故障处理方案,对紧急故障做到 7×24 小时应急响应。
4	安全整改服务 (个性化运维)	系统/ 年	1.00	主动发现、收集、分析系统安全漏洞并进行必要的安全加固,根据【开普云】网站监测报告以及等保测评机构反馈的测评报告,对平台进行安全漏洞修复。
5	重要活动支持 服务(个性化运 维)	次/年	2.00	在重大活动期间【重要会议、以及重要节假日】执行对所有业务支持系统及门户网站的 7*24 小时安全监控,重点监控影响到系统稳定安全运行的重点安全事件的发生,包括安全攻击(重点包括 DOS 攻击、恶意木马、病毒攻击等)、关键敏感数据泄露等,并提供安全事故应急响应技术保障,在任一系统任一安全隐患发生时,及时启动响应的应急预案。
6	应急响应和处	年	1.00	在发生确切的安全事件时,应急响应实施人员及时采

	置服务(个性化运维)	(不限次)		取行动限制事件扩散和影响的范围,限制潜在的损失与破坏服务基础上,实施人员协助客户检查所有受影响的系统,在准确判断安全事件原因的基础上,提出基于安全事件整体安全解决方案,排除系统安全风险并协助追查事件来源、提出解决方案、协助后续处置。
7	网站共性页面运维服务(个性化运维)	年(不限次)	1.00	对站点进行共性页面运维服务,主要包括模板调整、页面布局调整、应用功能组件维护等内容方面的建设与运行维护(不含各站点个性化内容)。
8	政务互动问答应用系统知识库更新服务	年(不限次)	1.00	<ol style="list-style-type: none"> <li>1. 基于全省政府集约化平台为基础,授权使用集约化平台站点开通问答功能,功能包括:智能辅助引擎、流程引导、人性化问答、智能化学习、细致化用户、个性化配置、互动数据分析等功能。</li> <li>2. 在海南省生态环境厅门户网站建立知识库,共享集约化平台政务数据库,依托平台多年的政务服务数据,完善管网数据不全的问题,赋能单位自身知识库内容,提高政务问答服务体验。</li> <li>3. 包含知识库优化服务,提供现场优化服务。</li> <li>4. 完成智能互动栏目手机端适配,一次性适配,可过手机端自适应使用问答服务。</li> <li>5. 打通集约化平台资源库与智能互动问答平台知识库之间的数据接口,建立统一的规范标准,提供可控的、可衡量、全天候的、人机互动的政务互动服务,包括分词库、同义词库、语料库、基础问答库。</li> </ol>

### 63、 运维服务质量考核

根据信息系统特性,运维供应商须接受运维服务质量考核指标管理要求,采购人采用年度服务考核指标作为年度服务质量考核标准。按月考核,满分100分,若年终服务考评分低于95分,按合同金额的3%扣除,在80-89分按合同金额的10%扣除。若因人为操作、违规操作等原因导致发生重大安全事故或对我单

位产生重大影响的，每次扣款人民币 2 万元。未经审批运维人员私自拷贝传输业务数据或违反保密管理规定，每次扣款人民币 1 千元。以上罚款如存在同一起时间参照最高罚款条款扣款，不进行重复罚款。具体内容以合同为主。

## 2.1 故障处理时间及考核要求

编号	故障等级	故障定义	故障处理时间	考评分值
1	特级事故	现有网络或系统停机，或遭到严重攻击行为或安全事件，对信息系统的业务运作有重大影响，导致 50% 以上的业务系统中断，数据全部丢失或部分丢失且无法恢复；	远程响应时间 <10 分钟，事故解决时间 <8 小时。	1. 如远程响应时间超过 10 分钟，扣 0.5 分； 2. 8 小时内事故无法解决，扣 4 分；
2	一级事故	门户网站发生故障，导致 30% 以上和 50% 以下的业务系统中断。	远程响应时间 <10 分钟，事故解决时间 <4 小时。	1. 如远程响应时间超过 10 分钟，扣 0.5 分； 2. 如 4 小时内事故无法解决，扣 3 分；
3	二级事故	站点发生故障，导致 10% 以上业务系统中断。	远程响应时间 <10 分钟，事故解决时间 <2 个小时。	1. 如远程响应时间超过 10 分钟，扣 0.5 分； 2. 如 2 小时内事故无法解决，扣 2 分；
4	三级事故	站点发生故障，导致个别业务	远程响应时间 <10 分钟，事	1. 如远程响应时间超过 10 分钟，扣 0.5 分；

		系统中断。	故解决时间 <30 分钟。	2. 如 30 分钟内事故无法解决，扣 1 分；
--	--	-------	------------------	--------------------------

### 其他考核内容

编号	考核项	考核要求	考核内容	考评分值
1	月度服务报告	未按时提交月度服务报告	每月月底至次月 5 日期间	未按时提交月度服务报告扣 1 分；
2	日常巡检报告	未按时提交巡检报告	每月月底至次月 5 日期间	未按时提交日常巡检报告扣 1 分；
3	年度服务报告	未按时提交年度服务报告	12 月 31 日至次年 1 月 5 日期间	未按时提交年度服务报告扣 3 分；
4	日常运维	维护周期 12 个月，运行维护期内，运维公司在工作日期间提供 5*8 小时系统运行维护服务。	运行维护期内，运行运维单位提供运行维护服务时效性	接收运维需求任务后 8 小时未响应，扣 1 分；未在 8 小时内解决的，扣 2 分；超出 8 小时未响应，且超出 8 小时未解决运维需求，未闭环处理，扣 3 分。运维人员变更，未报备登记，扣 1 分。
5	个性化服务	接收运维需求后 8 小时响应，运维公司根据个性化服务需求内容评估合理服务时间并及时解决。	接收运维需求后 8 小时响应，根据个性化服务需求内容评估合理服务时间并及时解决。	接收运维需求任务后 8 小时未响应，扣 1 分；未在合理评估时间内解决的，扣 2 分；超出 8 小时未响应，且超出 8 小时未解决运维需求，未闭环处理，扣 3 分。
6	安全服务	按照海南省电子政务云管理规范、电子政务外网网络安全管理规范、海南省电子政务	按照海南省电子政务云管理规范、电子政务外网网络安全管理规范、海南省电	未经审批，私自升级系统或开展数据操作，扣 2 分，如果导致数据丢失或出现运维事故，扣 3 分；其他未按照运维管理规范实施生产操作，扣 1 分；

		外网信息系统安全基线配置管理规范（标准）以及应用系统运维管理制度等相关安全管理要求，做好网络安全工作。	子政务外网信息系统安全基线配置管理规范（标准）以及应用系统运维管理制度等相关安全管理要求，做好网络安全工作。	实施过程导致重大安全问题，按照 I/II/III 等级，分别扣 3 分、2 分、1 分。未签订安全保密协议，扣 1 分。违反保密管理规定，处理数据，扣 2 分。发现安全问题，存在高风险，未能在 24 小时内处理，扣 2 分；
--	--	---	--	--

## 2.2 故障升级报告机制

优先级别	通告路径（通知）
特级事故	登记→事件经理； 离最终期限 2 小时→事件处理人、事件经理，采购单位项目经理； 已超时→事件处理人、事件经理、采购单位项目经理、采购单位部门领导→采购单位分管领导。
一级事故	登记→事件经理； 离最终期限 4 小时→事件处理人、采购单位项目经理； 已超时→事件处理人、事件经理、采购单位项目经理、采购单位部门领导。
二级事故	登记→事件经理； 离最终期限 6 小时→事件处理人； 已超时→事件处理人、事件经理、采购单位具体负责人。
三级事故	登记→事件经理； 离最终期限 12 小时→事件处理人； 已超时→事件处理人、事件经理、采购单位具体负责人。

## 2.3 运维服务时间参数说明

运维服务时间指标中各项参数说明如下：

参数	定义
响应时间	从服务台转入或其他系统转入或直接申告故障到得到响应的时 间。
到现场时间	需现场服务时，从申告故障到工程师到达现场的时间。
业务恢复时间	从申告故障，到工程师彻底或临时解决故障、恢复业务的时间 间隔。
时间分析时间	从故障临时解决/恢复业务到工程师提供事件情况分析报告的 时间。
升级时间	从申告故障，到故障被升级到更高一级管理人员的时间间隔。

## 2.4 运维服务量化指标

运维服务质量指标中各项参数说明如下，其中交付内容也作为后期验收文档：

序号	衡量指标	指标说明	目标值
1	《运维服务月报》	系统运维管理月报告	按月提供
2	《运维管理年度报告》	系统运维管理年度报 告	按年提供
3	《日常巡检表》	每天的日常巡检表	按月提供
4	《故障记录表》	每月的故障记录表	按月提供
5	《故障分析报告》	系统故障的分析报告	按次（如果有）
6	《系统升级记录表》	系统升级记录表	按次（如果有）
7	《特殊时期 7*24 小时值班 记录表》	特殊时期 7*24 小时值 班记录表	按次提供

## 三、项目相关要求

1、运维服务期（**服务期**）：运维服务期为合同签订之日起至 2025 年 9 月 23 日止。

2、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

3、投标人必须根据所投产品的服务要求、重要指标编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投标书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。

4、报价人要保持同采购人的密切联系，遇有重大事项及时报告和反馈信息，尊重项目业主方的意见，接受项目业主方的提议、监督和指导。

5、投标人必须如实地对招标文件中各项技术要求作出明确的逐项响应承诺，并对其真实性负责。

#### **四、支付方式**

1、签订项目合同后，采购人待省财政资金下达且收到供应商开具正式有效发票之日起5个工作日内，向供应商支付合同款的50%；（按照合同为准）

2、完成政务互动问答应用系统建设服务内容，交付上线后供应商提交试运行申请，双方签字确认后进入试运行期，正常运行3个月后，采购人待省财政资金下达且收到供应商正式有效发票之日起5个工作日内，向供应商支付合同款30%；（按合同为准）

3、完成项目运维服务内容，提交交付成果并验收合格后，采购人待省财政资金下达且收到供应商正式有效发票之日起5个工作日内，向供应商支付合同款20%。（按合同为准）

# D 包用户需求书

## 一、项目名称及采购内容

项目名称：海南省生态环境厅信息化运维项目（2024 年）

采购内容：网络安全等级保护测评

预算额度：24 万元。

## 二、项目内容及要求

### 一）项目概况

为提升海南省生态环境厅网络与信息安全防护水平，通过对在用系统开展网络安全等级保护测评，及时掌握信息系统资源现状和配置信息，反映信息系统资源的可用性情况和健康状况，创建一个可知可控的 IT 环境，从而保证信息系统的各类业务应用系统的可靠、高效、持续、安全运行。

1、采购单位：海南省环境科学研究院。

2、服务质量要求：中标方应按照国家相关规范、合同及甲方提出的具体要求，按时以书面形式提交成果。

### 二）项目需求

依据《信息安全等级保护管理办法》（公通字[2007]43 号）、《海南省深化信息安全等级保护工作方案》（琼等保办[2010]3 号）和《海南省信息化条例》文件的要求规定和建议，在信息安全等级保护安全整改建设项目验收前，需委托具备资质的等保测评机构，对安全整改建设项目的建设效果进行等级测评。

测评内容：分别对技术类和管理类进行测评。包含：物理安全、网络安全、主机安全、应用安全、数据安全及备份恢复、安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理十个层面测评。

本次评估对象为海南省生态环境厅 4 个三级信息系统。

序号	系统名称	网络安全保护等级
----	------	----------

1	海南省生态环境综合管理平台	第三级
2	海南省生态环境厅门户网站	第三级
3	超级站多因子数据收集及在线解析系统	第三级
4	海南省生态环境综合办公系统	第三级
5	整改指导	/
6	网络安全培训	/

### 三、项目相关要求

1、服务期限（**服务期**）：在采购人下达测评任务通知后 60 天内提交测评方案、整改建议、测评报告。

2、中标单位在签订合同时应按招标文件要求及投标承诺将拟派人员资料报采购单位备案，合同签订后，未经采购单位同意，不得更换。

3、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。

4、报价人要保持同采购人的密切联系，遇有重大事项及时报告和反馈信息，尊重项目业主方的意见，接受项目业主方的提议、监督和指导。

5、投标人必须如实地对招标文件中各项技术要求作出明确的逐项响应承诺，并对其真实性负责。

6、付款条件：本项目共分三次付款。合同签订后 5 个工作日内，付合同金额的 50%；提交商用密码应用安全性评估实施方案后 5 个工作日内，付合同金额的 30%；在完成正式评估报告并提交到当地密码管理部门备案后 5 个工作日内，付合同金额的 20%。

# E 包用户需求书

## 一、项目名称及采购内容

项目名称：海南省生态环境厅信息化运维项目（2024 年）

采购内容：商用密码应用安全性评估

预算额度：23.88 万元

## 二、项目背景

密码是保障网络安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。近年来密码在维护国家安全、促进经济社会发展、保护人民群众利益方面发挥了越来越重要的作用，国家对重要领域商用密码的应用、基础支撑能力的提升以及安全性评估、审查制度等不断提出明确要求。2019 年 10 月 26 日第十三届全国人民代表大会常务委员会第十四次会议通过《中华人民共和国密码法》第二十七条明确要求：“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。”。2023 年 7 月 1 日国务院发布生效修订后的《商用密码管理条例》第三十八条明确要求：“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。”。因此，采购人认真贯彻执行和国家密码管理局的商用密码管理要求，对信息系统开展商用密码应用安全性评估工作。

## 三、项目目标

为全面贯彻总体国家安全观和网络强国战略，深入贯彻落实习近平总书记关于核心技术自主可控重要批示精神和工作安排，持续推进商用密码工作，依据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《国家政务信息化项目建设管理办法》、《信息系统密码应用基本要求》、《商用密码应用安全性评估管理办法》等法律法规、制度和规范；经研究，拟通过购买评估服务的方式，对指定的信息系统开展密码应用安全性评估。

通过密码应用安全性评估掌握信息系统密码应用情况，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，提出下步整改举措，推动整改措施落实，为提升信息系统安全奠定基础，推动密码应用水平不断提升。

## 四、项目依据

### 4.1 法律依据

- a) 《中华人民共和国密码法》
- b) 《中华人民共和国网络安全法》

### 4.2 法规要求

- 64、《商用密码管理条例》
- 65、《商用密码应用安全性评估管理办法》
- 66、《国家政务信息化项目建设管理办法》
- 67、《关于规范商用密码应用安全性评估结果备案工作的通知》

### 4.3 遵循的主要标准

- 68、GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
- 69、GB/T 43207-2023 《信息安全技术 信息系统密码应用设计指南》
- 70、GB/T 43206-2023 《信息安全技术 信息系统密码应用测评要求》
- 71、GM/T 0116-2021 《信息系统密码应用测评过程指南》
- 72、T/GDCCA0001-2022 《信息系统密码应用方案评估规范》
- 73、T/GDCCA 0002-2022 《信息系统密码应用方案评估过程指南》
- 74、《政务信息系统密码应用与安全性评估工作指南》
- 75、《商用密码应用安全性评估量化评估规则》
- 76、《信息系统密码应用高风险判定指引》

## 五、被测系统

本次评估对象为海南省生态环境厅 4 个三级信息系统。

序号	系统名称	网络安全保护等级
1	海南省生态环境综合管理平台	第三级

2	海南省生态环境厅门户网站	第三级
3	超级站多因子数据收集及在线解析系统	第三级
4	海南省生态环境综合办公系统	第三级
5	整改指导	/
6	密码应用安全培训	/

## 六、评估服务内容

依据 GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》、GB/T 43207-2023 《信息系统密码应用测评要求》、GM/T 0116-2021 《信息系统密码应用测评过程指南》、《政务信息系统密码应用与安全性评估工作指南》和信息系统自身的安全需求分析，对被评估系统进行商用密码应用安全性评估，为重要网络和信息系统的密码安全提供科学评价，逐步规范网络运营者的密码使用和管理行为，推动提升我单位密码应用水平。具体服务内容如下：

### 6.1 密码应用方案评估服务：

引入密码管理部门认定具有商用密码应用安全性评估资质的评估机构，依据 T/GDCCA0001-2022 《信息系统密码应用方案评估规范》、T/GDCCA 0002-2022 《信息系统密码应用方案评估过程指南》针对指定信息系统密码应用方案的完整性、准确性、可行性等方面进行分析并出具报告，并协助运营单位完成结果备案。

### 6.2 密码应用安全性评估服务：

针对上述信息系统按照评估后的密码应用方案建设情况，引入密码管理部门认定具有商用密码应用安全性评估资质的评估机构，对指定的信息系统进行商用密码应用安全性评估，依据《商用密码应用安全性评估量化评估规则》综合判定，指导密码应用消减重要安全风险后出具《密码应用系统安全性评估报告》（具体名称另行约定），并协助运营单位完成密评结果备案。

## 七、技术要求

### 7.1 商用密码总体要求评估

(1) 密码算法合规性评估：本项目商用密码应用关于信息系统使用的密码算法是否符合法律、法规的规定和密码相关国家标准、行业标准的有关要求。

(2) 密码技术合规性评估：本项目商用密码应用关于信息系统使用的密码技术是否遵循密码相关国家标准和行业标准。

(3) 密码产品合规性评估：本项目商用密码应用关于信息系统使用的密码产品与密码模块是否通过国家密码管理部门核准。

(4) 密码服务合规性评估：本项目商用密码应用关于信息系统使用的密码服务是否通过国家密码管理部门许可。

### 7.2 密码技术应用评估

从物理和环境、网络和通信、设备和计算、应用和数据 4 个层面对商用密码应用关于信息系统的密码技术设计情况进行分析与评估。

物理和环境密码安全设计评估：分析评估密码应用是否合理、合规的利用商用密码完整性、真实性功能，对影响信息系统安全防护效能的物理和环境层面因素是否得到有效控制。

网络和通信密码安全设计评估：分析评估密码应用是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的网络和通信层面因素是否得到有效控制。

设备和计算层面评估：分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性功能，对影响信息系统安全防护效能的设备和计算层面因素是否得到有效控制。

应用和数据层面评估：分析评估信息系统是否合理、合规的利用商用密码机密性、完整性、真实性以及不可否认性功能，对影响信息系统安全防护效能的应用和数据层面因素是否得到有效控制。

### 7.3 安全管理评估

分析评估本项目商用密码应用对影响商用密码防护效能的管理制度与措施是否进行规划和设计。管理制度与措施包括但不限于下列典型维度：安全管理制度，密钥管理、人员管控，信息系统实施，应急预案。

## 7.4 云平台评估技术要求

云平台测评与一般信息系统基本一致，但由于云平台还需要为云上应用提供计算、存储、网络、密码等资源，还应关注云平台自身的密码应用以及对云租户提供的密码服务。即要分别对云平台支持的每类服务模式（IaaS、PaaS、SaaS）进行密码应用测评，应包括被完全评估的支撑能力和被部分评估的支撑能力。

**被完全评估的支撑能力：**指的是云平台中的某些测评对象，这些测评对象同时用于支撑云平台和云上应用，将同时作为云平台和云上应用的测评对象。即该支撑能力有明确的测评结果（包括量化评估、风险评价等）。

**被部分评估的支撑能力：**指的是云平台提供的某些支撑服务，这些支撑服务仅用于云上应用而不用于云平台，或者将服务于云平台 and 云上应用的不同测评对象。该支撑能力必须结合云上应用的密码应用一起评估，因此无法在云平台测评时进行“完全评估”，只能进行“部分评估”。

## 八、评估方法 8.1 人员访谈

与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，一般应基本覆盖所有的密码应用相关人员类型，在数量上可以抽样。

### 8.2 配置检查

利用上机验证的方式检查密码设备、数据库、安全设备、应用系统等配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实（包括日志审计等），评估其实施的正确性和有效性，检查配置的完整性，从而测试系统是否达到可用性和可靠性的要求。

### 8.3 文档审查

检查制度、策略、操作规程、制度执行情况记录等文档（包括安全方针文件、安全管理制度、安全管理的执行过程文档、系统设计方案、密码设备的技术资料、系统和产品的实际配置说明、系统的各种运行记录文档、机房建设相关资料、机房出入记录等过程记录文档）的完整性，以及这些文件之间的内部一致性。

### 8.4 实地查看

通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，评估其是否达到了相应等级的密码应用安全要求。

#### 8.5 工具检测

通过使用安全检测工具及手段，检测被测对象的安全性脆弱性，验证检测结果的有效性，从而评估系统是否达到密码安全有效的要求。

### 九、项目实施要求 9.1 服务能力要求

77、 投标供应商应使用自主研发或有授权的密码测评工具，并保证工具安全可靠，不得影响或损毁采购人业务系统服务或数据。

78、 投标供应商应使用自主研发或有授权的商用密码应用安全性评估作业或管理系统对本项目的全过程，从项目管理、信息处理、数据分析、报告生成等各方面进行规范作业和管理控制。

#### 9.2 实施要求

79、 投标供应商必须具备独立完成本项目的能力；

80、 投标供应商提供的资格、资质等证明文件应真实有效；

81、 投标供应商应对了解到的信息保密，并提供保密承诺；

82、 投标供应商应在项目现场实施周期内，中标方必须为本项目成立评估小组，所需电脑等设备自行提供；

83、 项目必须按照商用密码应用安全性评估的标准要求开展。

84、 服务期间成交供应商应提供 7×24 服务响应（7×24 小时工程师 2 小时内作好服务应答和反馈）。需要现场支撑时，需在 3 小时内安排至少 1 名具有服务能力的工程师到达现场处理。

85、 成交供应商应具备本地化服务能力配备服务团队，在广州本地有固定办公场所或注册服务机构，保证积极响应项目服务需求和持续提供项目服务。

#### 9.3 保密要求

86、 投标供应商须签订保密协议，对其因身份、职务、职业或技术关系而知悉的采购人商业秘密和党政机关保密信息应严格保守，保证不被披露或使用，包括意外或过失。

87、 投标供应商不得以竞争为目的、或出于私利、或为第三人谋利而擅自保存、披露、使用采购人商业秘密和党政机关保密信息；不得直接或间接地向无关人员泄露采购人的商业秘密和党政机关保密信息；不得向不承担保密义务的任何第三人披露采购人的商业秘密和党政机关保密信息。投标供应商在从事政府项目时，不得擅自记录、复制、拍摄、摘抄、收藏在工作中涉及的保密信息，严禁将涉及政府项目的任何资料、数据透露或以其他方式提供给项目以外的其他方或投标供应商内部与该项目无关的任何人员。

88、 投标供应商对于工作期间知悉采购人的商业秘密和党政机关保密信息（包括业务信息在内）或工作过程中接触到的政府机关文件（包括内部发文、各类通知及会议记录等）的内容，同样承担保密责任，严禁将政府机关内部会议、谈话内容泄露给无关人员；不得翻阅与工作无关的文件和资料。

89、 严禁泄露在工作中接触到的政府机关科技研究、发明、装备器材及其技术资料和政府工作信息。

## 十、交付物

项目成果包括但不限于下列文档：

服务名称	交付物名称	数量
商用密码应用安全性评估服务	《密码应用方案》	1 份
	《商用密码应用安全性评估实施方案》	1 份
	《商用密码应用安全性评估报告》	1 份/每系统

## 十一、其它约定

1、 签订合同： 中标人应于接到中标通知书 5 个工作日内与招标人签订正式合同。

2、 交货（服务）地点： 《客户名称》或系统部署地点。

3、 服务期限（自签订合同之日起计）： 一年内。

4、 服务技术要求： 此项目需按照国家最新的密评标准实施。

5、 验收要求： 项目时间自本项目启动之日起至提交商用密码应用安全性评估报告到备案止；在通过项目交付物审核之后，本项目完成验收。

6、 付款条件： 本项目共分三次付款。合同签订后 5 个工作日内，付合同金额的 50%；提交商用密码应用安全性评估实施方案后 5 个工作日内，付合同金

额的 30%；在完成正式评估报告并提交到当地密码管理部门备案后 5 个工作日内，付合同金额的 20%。