第三章 采购需求

项目编号	ZB2024-0101
项目名称	海南省海防监控系统安全达标升级改造项目
预算金额	387.9949 万元
标包	A/B 包
分包预算（最高限价）	A 包：382.4310 万元；B 包：5.5639 万元
采购方式	公开招标
采购需求	A 包：海南省海防监控系统安全达标升级改造项目（集成服务）B 包：海南省海防监控系统安全达标升级改造项目（监理服务）
合同履行期限/工期	A 包：本项目总建设周期为 6 个月，第一阶段工期为 3 个月，第二阶段工期为 3 个月；B 包：本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。
建设地点	用户指定地点
是否接受联合体投标	A/B 包：不接受联合体投标
备注	**本项目从项目立项、报建、报批及经过专家评审论证。** **本项目项目类别为：服务**

A包采购需求

一、技术要求

1 建设目标

1.1 总体目标

《中华人民共和国网络安全法》明确指出国家实行网络安全等级保护制度，中共海南省委军民融合发展委员会办公室已对海南省HF监控系统定级备案，定级为第三级。为做好网信系统网络安全工作，根据海南社会管理信息化平台建设领导小组统一部署，2021年12月，中共海南省委军民融合发展委员会办公室委托两家第三方机构分别对海南省HF监控系统开展网络安全等级保护测评和商用密码应用安全性评估工作。根据《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）开展网络安全达标升级改造，保障基础设施网络与信息系统安全。

因此，本项目将在上一年度网络安全等级保护测评的基础上，针对测评发现的安全问题进行整改，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）对海南省HF监控系统网络安全进行达标升级改造建设，并通过等保三级测评，达到等级测评结论“良”。

同时贯彻落实《中国人民共和国密码法》关于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》、《海南政务信息化项目建设管理办法》、《关于进一步明确省政务信息化项目建设密码应用有关要求》的通知（琼国密局字〔2021〕2号）进行密码应用建设；依据《海南省政务信息化项目建设管理实施细则（暂行）》第八条（五）根据国家密码管理有关法律法规和标准规范的要求，关键信息基础设施、网络安全等级保护第三级及以上、面向社会服务等重要非涉密政务信息项目应同步规划、同步建设、同步运行密码保障系统，并定期进行评估。

本项目将在上一年度商用密码应用安全性评估的基础上依据《信息安全技术

信息系统密码应用基本要求》（GB/T39786-2021）进行密码应用建设升级改造，并通过密码应用安全性评估。

1.1.1 第一阶段目标

第一阶段等级保护建设目标为初步达成信息系统网络安全等级保护基本要求中安全计算环境部分对安全审计与恶意代码防范的要求；第一阶段密码应用安全性建设目标为初步达成信息系统密码应用基本要求中对重要数据安全传输的要求。

1.1.2 第二阶段目标

第二阶段的等级保护建设目标为完成对安全物理环境、安全管理中心和物联网边界防护的升级改造建设；第二阶段密码应用安全性建设目标为完成重要数据安全存储和身份鉴别的升级改造建设；第二阶段网络安全服务建设目标为完善安全管理体系建设，完成对网络安全等级保护建设和密码应用安全性建设成果的检验，巩固海南省 HF 监控系统网络安全达标升级改造项目建设成果。

2 建设内容

本项目按照国家与海南省各项政策法规开展设计，通过新建与利旧，完成以下升级改造内容：

一、等级保护建设内容

根据上一年度等保测评，从安全物理环境、安全通信网络、安全区域边界、安全计算环境等各方面进行安全防护设计，同时统一的安全管理中心保障了安全管理措施和防护的有效协同及一体化管理，以等级保护安全框架为依据和参考，在满足国家法律法规和标准体系的前提下通过“一中心、三防护”的安全设计对海南省 HF 监控系统等级保护进行升级改造建设。

等级保护建设内容分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心五个部分。总体建设内容为静电手环 60 个、视频监控系统 1 套、一体化二联机柜 1 套、视频防火墙 14 台、数据库审计设备 1 台、终端防病毒服务端 1 套、终端防病毒客户端 110 个、服务器防病毒 60 套、态势感知平台 1 套、省中心流量探针 1 台、分中心流量探针 14 台。

1.安全物理环境方面建设内容为静电手环 60 个、视频监控系统 1 套、一体化二联机柜 1 套；

2.安全通信网络方面建设内容与密码应用安全性建设中网络和通信安全方面建设内容一致；

3.安全区域边界方面建设内容为视频防火墙 14 台；

4.安全计算环境方面建设内容为数据库审计设备 1 台、终端防病毒服务端 1 套、终端防病毒客户端 110 个、服务器防病毒 60 套；

5.安全管理中心方面建设内容为态势感知平台 1 套、省中心流量探针 1 台、分中心流量探针 14 台。

二、密码应用安全性建设内容

根据上一年度密码应用安全性评估，围绕《国家政务信息化项目建设管理办法》中关于政务信息系统在系统规划阶段的密码应用要求，综合考虑本系统物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用方案，对海南省 HF 监控系统网络安全密码应用进行升级改造建设，最终为系统的安全可靠运行提供全面高效的密码支撑。

密码应用安全性建设内容分为物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理六个部分。核心建设为身份鉴别、重要数据在传输中的机密性与完整性、重要数据在存储中的机密性与完整性。总体建设内容为动态密码服务器 2 台、国密浏览器 110 个、签名验签服务器 1 台、配套业务系统身份证书 1 套、BHF 网络/数据加密机 15 台。

1.身份鉴别方面建设内容为动态密码服务器 2 台；

2.重要数据在传输中的机密性与完整性方面建设内容为国密浏览器 110 个、BHF 网络/数据加密机 15 台；

3.重要数据在存储中的机密性与完整性方面建设内容为签名验签服务器 1 台、配套业务系统身份证书 1 套、BHF 网络/数据加密机 15 台。

三、网络安全服务建设内容

依据《网络安全等级保护基本要求》及组织网络安全管理工作的特点从安全策略、管理制度、制定和发布以及评审和修订等方面进行安全运营制度设计，开展漏洞扫描服务、渗透测试服务、安全加固服务等网络安全服务内容，检测海南省 HF 监控系统升级改造的成果。

网络安全服务建设内容为在完成等级保护建设和密码应用安全性建设后开

展安全管理制度建设服务 1 次、漏洞扫描服务 1 次、渗透测试服务 1 次、安全加固服务 1 次、应急演练服务 1 次、网络安全意识培训服务 1 次。

综合以上建设内容，提升海南省 HF 监控系统关键信息基础设施网络与信息系统安全防护能力，构筑新型可信网络安全防御体系。

2.1 第一阶段建设内容

一、第一阶段等级保护建设内容

本项目第一阶段的等级保护建设内容为在省中心中部署 1 台数据库审计设备；在 14 个分中心中部署终端防病毒服务端 1 套、终端防病毒客户端 110 个、服务器防病毒 60 套，在省中心新增 1 套一体化二联机柜，数据库审计设备能够对等级保护中日志审计要求进行补充完善，对保障储存在数据库中重要数据的安全起到了积极作用，终端防病毒能使办公终端构筑完善的病毒防御体系，有效抵御外界网络病毒的攻击；数据库安全审计与恶意代码防范能够与现有安全设备构成网络安全防御的基础，应该放在第一阶段重点建设。

二、第一阶段密码应用安全性建设内容

本项目第一阶段的密码应用建设内容为在省中心和 14 个分中心部署国密浏览器 110 个、BHF 网络/数据加密机 15 台。同时能满足《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）中安全通信网络对通信过程中重要数据的完整性、保密性要求，应该放在第一阶段重点建设。

第一阶段建设内容如下表所示：

表 1- 1 项目第一阶段建设部署设备表

序号	种类	数量	部署位置
1	数据库审计	1	省中心
2	终端防病毒服务端	1	省中心
3	终端防病毒客户端	110	省中心及 14 个分中心
4	服务器防病毒	60	省中心及 14 个分中心
5	BHF 网络/数据加密机	15	省中心及 14 个分中心
6	国密浏览器	110	省中心及 14 个分中心
7	一体化机柜	1	省中心

2.2 第二阶段建设内容

一、第二阶段等级保护建设内容

本项目第二阶段的等级保护建设内容为在省中心和各分中心部署态势感知平台以及配套的流量探针，建立对设备信息的集中管控，达到《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）安全管理中心通用要求中对集中管控的要求；在各分中心部署视频防火墙，达到《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）中对物联网感知节点的扩展要求；为洋浦分中心更换视频监控系统；为各机房配置防静电手环。

二、第二阶段密码应用安全性建设内容

第二阶段的密码应用建设内容为在省中心部署 1 台签名验签服务器以及配套业务系统身份证书，能够保障系统中各种重要数据存储的保密性和完整性；在省中心部署 2 台动态密码服务器，能提供使用国密技术的动态身份验证，能满足《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）、《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）中对身份鉴别的要求。

三、第二阶段网络安全服务建设内容

第二阶段的网络安全服务建设内容为在完成等级保护建设和密码应用安全性建设后开展安全管理制度建设服务 1 次、漏洞扫描服务 1 次、渗透测试服务 1 次、安全加固服务 1 次、应急演练服务 1 次、网络安全意识培训服务 1 次，完善安全管理体系，并检验等级保护建设和密码应用安全性建设的成果。

第二阶段建设内容如下表所示：

表 1- 2 项目第二阶段建设部署设备表

序号	种类	数量	部署位置
1	态势感知平台	1	省中心
2	省中心流量探针	1	省中心
3	分中心流量探针	14	各分中心
4	视频防火墙	14	各分中心
5	静电手环	60	省中心和各分中心
6	视频监控系统	1	洋浦分中心
7	签名验签服务器	1	省中心

序号	种类	数量	部署位置
8	业务系统身份证书	1	省中心
9	动态密码服务器	2	省中心

3 建设周期与地点

1.总建设周期为 6 个月。第一阶段建设周期为 3 个月，第二阶段建设周期为 3 个月；

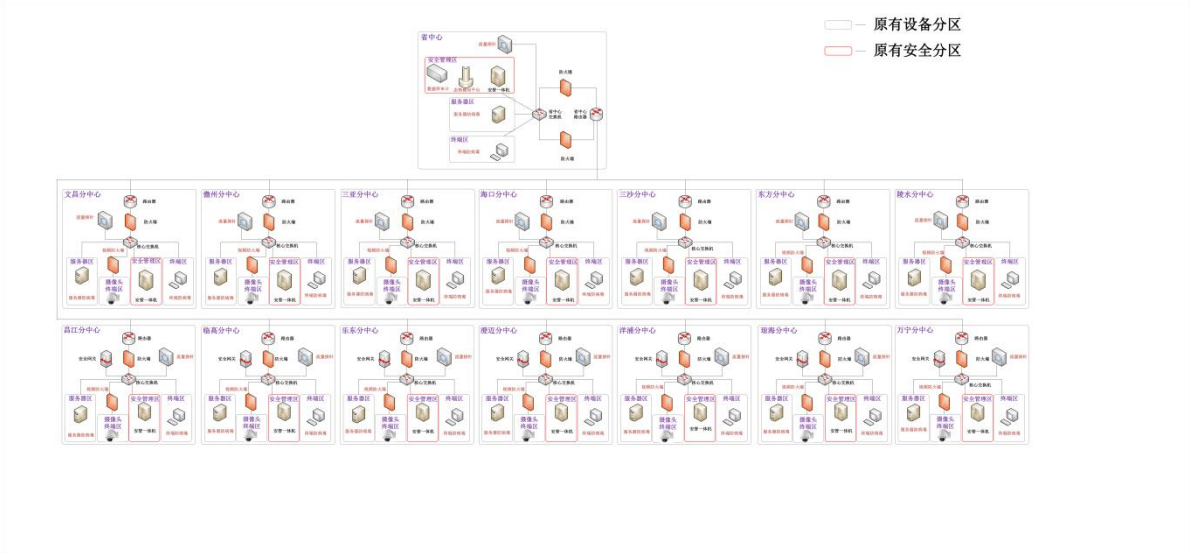
2.建设地点：海南省。

4 网络安全建设方案

4.1 总体拓扑设计

依据等级保护基本技术要求，结合实际业务保障需要，规划总体网络拓扑，以原高性能核心路由器作为该局域网的核心，承担全网的路由转发任务。根据等保 2.0 三级网络安全建设要求，在整体网络区域的通信网络、区域边界、计算环境、管理中心新增相关网络安全设备对系统进行有效防护，同时利旧使用原有安全防护设备。升级改造后网络拓扑图如下图所示：

红色字体为本次安全建设新增设备。



4. 2 安全物理环境

1.设备部署及功能说明

本项目机房物理安全标准遵循国家等级保护三级要求进行防护：

1)防盗窃和防破坏

洋浦分中心机房内配置 1 套视频监控系统并安排专人值守，确保能正常使用。

2)防火

启用洋浦分中心机房内已安装的七氟丙烷火灾自动消防系统。

3)防静电

省中心和 14 个分中心配置防静电手环，每个中心配置 4 个静电手环，共配置 60 个防静电手环。

4.3 安全通信网络

1.设备部署及功能说明

1)网络区域划分

根据承担功能和部署设备的不同，将整体网络划分为不同的安全区域，根据各个安全区域的应用特点分别部署和配置相应保护措施和安全策略，保障业务的连续性、安全性和可靠性；体现“整体防护、突出重点”的建设原则。

本项目按访问对象和等级保护要求的不同可划分为以下区域：

省中心：服务器区、终端区、安全管理区；

14 个分中心：服务器区、摄像头终端区、安全管理区、终端区。

2)通信传输数据保护

本项目通过在省中心和分中心之间均部署遵循《边海防网络/数据加密机规范》（GM/T0026-2014）的边海防网络/数据加密机，采用 SSL 协议的方式通过基于国密的 SM3 算法建立安全可靠的传输通道，保证通信过程中数据的完整性；采用 SSL 协议的方式通过基于国密的 SM4 算法建立安全可靠的传输通道，保证通信过程中数据的机密性。

4.4 安全区域边界

1.设备部署及功能说明

1)防火墙设置

对各中心部署的防火墙设备进行策略控制，根据业务需要制定防火墙的访问控制策略，在缺省拒绝所有通信的基础上，仅允许业务所需的访问连接和数据通信。防火墙均配置入侵防御和防病毒功能。确保所有跨越边界的访问和所有流入、流出的数据均通过其受控接口进行通信、接受安全检查和处理。

2)堡垒机

各中心部署的安管一体机包含堡垒机运维审计功能，设置堡垒机运维审计策略，通过堡垒机运维审计将所有 IT 组件的管理运维端口，通过策略路由的方式，交由堡垒主机代理。实现运维单点登录，统一管理运维账号，管理运维授权，并对运维用户操作进行审计记录，并通过堡垒机实现对运维角色与权限的划分，分为系统管理员、审计管理员、安全管理员等，对远程访问的用户行为进行审计，并生成审计报表。

3)日志审计

开启各中心部署的安管一体机中的日志审计功能，对防火墙审计记录和堡垒机审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖，确保留存时间超过 6 个月。

2. 整改措施及说明

1)各中心边界防火墙访问控制策略细化到地址、端口。关闭最后一条访问控制策略为允许所有网络通信的策略。

2)各中心边界防火墙上的 IPS 模块按照等保测评要求定时更新 IPS 特征库，特征库更新版本时间不晚于一个月。

3)各中心边界防火墙上的 AV 模块按照等保测评要求定时更新 AV 特征库，特征库更新版本时间不晚于一个月。

4. 5 安全计算环境

1.设备部署及功能说明

1)服务器防病毒

省中心与 14 个分中心新加装服务器防病毒，实现对服务器病毒的查杀与检测，满足三级安全计算环境对恶意代码防范的要求

2)数据库审计

省中心新部署数据库审计设备负责对省中心、昌江分中心、澄迈分中心、乐

东分中心、临高分中心、琼海分中心、万宁分中心、洋浦分中心进行审计，对数据库的访问和操作行为进行审计，记录日志；对数据库攻击行为进行检测与告警，满足三级安全计算环境对安全审计的要求。

4.6 安全管理中心

1.设备部署及功能说明

1)态势感知平台

在省中心安全管理区部署态势感知平台，可实现对安全态势觉察、跟踪、预测和预警，全面实时掌握网络安全态势，及时掌握网络安全威胁、风险和隐患，及时监测漏洞、病毒木马、网络攻击等情况。

2)流量探针

在省中心核心交换机、14 个分中心核心交换机旁路部署流量探针系统，接镜像端口；将其它安全域的流量镜像至探针，进行入侵行为检测；审计记录可通过报表展示给管理人员，并将各中心设备运行状态报告发送至态势感知平台，进行综合的安全态势分析和展示。

4.7 设备功能要求

4.7.1 数据库审计

本项目数据库审计设备包含以下功能：

1.精细审计粒度

支持对来源、目标、源应用程序、SQL 操作响应时间与返回行数、SQL 操作成功与否等信息的审计。支持 DDL、DML、DCL、TCL、Login、Logout 等多种数据库存操作类型的审计。

2.风险智能分析

内置了丰富多样的特征库：威胁访问特征库、SQL 注入特征库等，并进行自动告警；提供了智能自动建模功能：通过自学习，自动建立数据库访问的用户模型，可形成不同级别的预警。

3.态势感知能力

基于深度分析引擎，自动分析数据库的交互情况：SQL 交互量、TCP 会话量、威胁行为、网络流量。实时对数据库进行分值评估，为管理层提供数据库优化的依据和建议报告

4.实时在线监测

实时监测在线会话列表，帮助用户实时了解数据库的访问情况：源 IP、账户、访问时间、访问时长等。实时监测到每个会话地风险情况，通过快速的智能定位功能，可以帮助用户及时定位风险 SQL 语句操作。

5.输出合规报表

内置多种报表模板，可以按照告警规则名称、违规账户、违规 IP 等形成丰富的报表；定期地输出审计报表，以统计最近数据库的访问情况、操作情况、违规情况以及异常情况。

6.API 接口联运

系统开放了全部数据接口：审计数据接口、告警数据库接口、配置接口、策略接口等。允许第三方平台对接并调用数据库审计与防护系统的接口，让数据分析变得更智能。

4.7.2 终端防病毒

本项目终端防病毒软件包含以下功能：

终端防病毒系统一般为两层构架，即：中心服务端和终端软件。中心服务端部署于服务器中；终端软件授权安装在被保护办公终端上。

中心服务端负责制定终端软件防病毒策略，在内网建立全网统一的升级服务器，由中心服务端通过手动方式获得最新的病毒特征库，分发到分中心的各个办公终端上，实现终端杀毒、终端优化、系统漏洞补丁修复、程序守护、风险帐号（影子帐号等）优化、DDOS 防火墙、ARP 防火墙、应用防火墙、防 CC 攻击、防入侵防提权、防篡改、安全策略设置等，使终端免受攻击，同时，终端软件可以为安全管理平台提供关于病毒威胁和事件的监控、审计日志，为视频专网的病毒防护管理提供必要的信息。

4.7.3 服务器防病毒

本项目服务器防病毒软件包含以下功能：

针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能，服务器防病毒软件为用户提供服务器网络安全防护功能,可以帮助用户抵御外界对核心服务器的攻击,提升服务器安全性。具备有 DDOS 防火墙，ARP 防火墙，Web 防火墙进行攻击防护，同时还有各种防暴力破解防护以及黑白名单的 IP 添加。

4.7.4 态势感知平台

本项目态势感知平台包含以下功能：

1.安全态势感知

安全感知是态势感知平台的主要功能承载模块，它向管理人员提供了相关安全态势的全部信息，具体如下：

1)失陷态势感知：失陷态势感知包含了主机（被划分为服务器、终端）、账号及网站等对象的相关失陷详情；在主机失陷中会具体将失陷的阶段进行列举；而对于账号等失陷一般通过用户行为分析方式进行判断；

2)网络威胁态势感知：网络威胁态势包含各个方向的攻击及相关威胁情况，包括外部威胁、外连威胁及内部互连等；每个方向上的相关攻击威胁会包含若干子类，这可以使用户对于攻击威胁有更清晰的认识，如扫描探测、风险访问、异常连接、C&C 回连通讯、隐蔽通道、恶意软件下载等；

3)行为风险态势感知：包含对于一些主机或网络互连策略违反等相关信息；如违反访问控制策略（需要管理人员进行定义何为合法的、何为非法的访问策略）；

4)数据风险态势感知：将针对数据库的相关安全问题单独列出，包括针对端口的风险访问、针对数据库的攻击、针对数据库的扫描及口令猜测等；

5)业务安全态势感知：主要针对网站相关安全问题进行计算和呈现，包括各类针对网站的攻击（扫描）、挂马、篡改等；

6)脆弱性态势感知：包含对于系统内相关资产的主机漏洞、配置违反及明文传输等风险信息；

7)病毒态势感知：针对从各个来源获取的文件病毒检查结果，统计和分析相关问题，管理人员也可以从界面下载相关可疑文件内容。

2.资产管理

安全资产是态势感知平台的核心管理对象，安全管理中的资产具备如下两类属性：

1)基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 核 IPv6 格式）、响应人（出现安全问题应由何人处理）、登录凭证（获取配置、安全基线检查等使用）、上架信息、运行状态（包括 CPU、内存、磁盘、网络流量）等；

2)安全属性：完整性、可用性、保密性、风险信息、开放端口、安全事件、漏洞、安全基线违规问题等。

为了提供一定的扩展性和灵活性，系统可支持管理人员定义多个自定义属性，属性的类型包括数值型、日期型、字符型等，支持管理人员录入、导入或自动发现资产。

3.拓扑管理

态势感知平台的拓扑管理中提供了丰富的图元和工具，让管理人员可以编辑出多种多样的拓扑图。

1)工具包括：点选模式、框选模式、浏览模式、普通连线、折线、曲线、放大、缩小、1 比 1 展示、纵览展示、导出图片和打印预览。

2)图元分为：背景类、设备类和其它类三大类，系统自带部分图元，同时支持用户自己上传。设备类图元可绑定资产，其它类中的人员可绑定系统中的用户信息，其它类中的视图图元可绑定系统中的视图信息。

3)端口信息配置：拓扑图中的连线中可配置连线两端的设备的端口信息。

4)子拓扑图配置：除设备类和背景类图元外，其它图元都可以创建下一级拓扑图。

4.告警管理

态势感知平台的告警管理能帮助管理人员管理源于网络流量分析、安全事件及日志分析、安全基线违规、高危漏洞、高危端口开放等的特别安全问题，告警管理中包括了如下功能：

1)告警监控：监控系统内存在的各种告警；可以通过定义过滤器以监控需要特别关注的告警信息；用户也可以根据个人需求，设置告警的提示音、界面显示方式等；用户可以对其需要特别关注的告警进行标识（被称作标签），在需要的时候可以通过标签对这些告警进行搜索；

2)告警处理：处理监控列表中相关告警；针对告警，用户可以清除、确认（不能确定是否需要处理）或转工单；

3)策略定义：用户可以定义各类告警产生的策略（系统内置了部分策略）；在告警策略中可以设定对于安全数据的筛选条件、归并字段、时长、次数、状态变迁以及命中后产生何种响应；响应包括：发送邮件（可以发送给策略制定人、资产响应人，也可以发送给制定的用户）、发送 Syslog 或 SNMP Trap（可发送给系统管理中配置的 4 个 Syslog 服务器或者发送给自定义的 2 个 Syslog 服务器）、执行外部程序或脚本（需预先将程序和脚本部署在安全态势感知与管控平台系统核心处理分析服务器上）、暂存数据（用户可以将数据保存在临时表中作为其它策略的输入）等；策略可以和相关的知识进行关联，以便于用户进行处理。

5.安全事件和日志管理

态势感知平台的安全事件管理主要完成对事件的集中收集、管理和分析。主要的功能包括事件收集、事件集中处理；在安全事件管理中，管理人员可以自由地定义对于原始事件的查询方式，查询的结果可以直接生成为报告并导出到外部文件中。

6.事件收集

态势感知平台的事件收集主要是对事件采集和格式化的过程，支持以下事件源：

➢防火墙、入侵检测系统等安全设备；

➢操作系统记录的重要安全相关的日志和事件告警，支持 Windows 2000/2003/NT/XP/Vista/7/2008/8/10/2010/2016 等，各种版本的 Linux/Unix 系统；

➢各种类型的数据库日志，例如 Oracle、MySQL 等；

➢防病毒系统、访问控制系统、用户集中管理和认证系统；

➢各种应用系统的日志，如 Apache、Tomcat、IIS 等。

态势感知平台能够通过多种方式收集事件源发送的安全事件：

1)Syslog 方式：以 Syslog 方式接收安全事件；

2)SNMP trap：接收来自设备的 SNMP Trap 的事件；

3)镜像接入：可以从网卡上直接接收相关事件或日志；

4)数据库方式：可以通过 JDBC 数据库接口获取事件源存放在各种数据库中的安全相关信息；支持的数据库类型包括 Oracle、Microsoft SQLServer、DB2、MySQL 和 Sysbase；

5)网络 Socket 接口方式：可以通过 TCP/IP 网络，以 Socket 通信的方式获得安全事件；

6)本地文件方式：可以通过读取事件源的日志文件，来获取其中与安全有关的信息；

7)WMI 方式：支持 Windows 设备主动通过 WMI 方式去采集安全事件，一个采集器支持多个 Windows 设备的 WMI 接入；

8)第三方代理或者应用程序：第三方的应用程序或者代理可以通过以上方式或者标准输出直接将安全事件转发给安全事件采集。

7.事件处理

态势感知平台的安全事件管理不仅可以处理普通的事件或日志，也可以对多行事件、UTF-8 编码的事件进行处理和分析。

标准化后的事件主要包括了类似于事件名称、严重级别、分类、源（地址、端口、主机、用户等）、目的（地址、端口、主机、用户等）、网络、采集器信息等字段；标准化后的事件可以根据相关规则和资产进行关联。

态势感知平台除了内置一些主流系统或设备脚本外，可提供的脚本定义语言，能定义任何符合管理人员需求的事件标准化策略。

8.漏洞管理

态势感知平台内置扫描器，支持分布式的漏洞扫描模式以及集中的漏洞分析和处理。漏洞是脆弱性的一个子集，专指可通过扫描器发现的脆弱性，其中部分具有国际上标准的 CVE 编号以及 CVND（国家信息安全漏洞共享平台）编号等。

在漏洞管理中，能够集中查看、统计系统存在的系统漏洞，以及目标网页所存在的 Web 漏洞。还可以制定扫描策略及任务，对系统内安全资产进行一次或周期性的扫描；支持设置 IPv4 地址段或选择资产的方式扫描对象；也可以支持对单个 IPv6 地址对象扫描。

态势感知平台的漏洞管理主要有以下功能：

1)漏洞查看：列表查看登录用户权限范围存在的漏洞，显示某漏洞在哪些资产上存在（列表中显示相关资产数量，点击可查看具体哪些资产存在此漏洞）；可显示相关漏洞的全部详细情况；

2)扫描任务管理：漏洞任务管理包括三个部分：正在执行的任务、已定义的任务和任务执行的结果，即漏洞扫描报告，报告可以导出为 Word、PDF、HTML 等格式；对于正在执行的任务用户可以停止、暂停或继续任务的执行；如果用户不指定任何策略，系统也可以使用默认策略对所指定的对象进行扫描；

3)扫描策略管理：通过选择系统内存在的插件，用户可以自定义漏洞扫描策略；

4)提供扫描插件的升级功能。

9.安全基线管理

安全基线是指各类系统、设备的安全配置标准；而安全基线的违规问题是指实际的系统或设备的配置违反了基线的要求。例如是否存在不允许的用户账号、账号的口令策略存在一定问题（不满足复杂度、长度、更改时间的要求）等等。

安全基线可被划分为账号类、口令类、授权类、日志配置类、路由配置类等等，例如：应删除或锁定与设备运行、维护等工作无关的账号等。

态势感知平台支持的系统或设备包括：

➢主流操作系统：包括如 CentOS、Redhat、SUSE、IBM AIX、SUN Solaris、Windows 等；

➢主流路由器/交换机：如思科、Juniper、华为等；

➢主流防火墙：如思科 PIX/ASA、Juniper Netscreen、华为一道门、Fortigate

等；

➢主流数据库：如 Oracle、MySQL、Sybase、MS SQL Server 等；

➢主流 Web 中间件：如 Apache、Tomcat、Websphere、Weblogic、IIS 等。

态势感知平台的安全基线管理主要具备如下功能：

1)安全基线违规问题查看：列表查看登录用户权限范围存在的安全基线违规问题，显示某违规问题在哪些资产上存在；

2)安全基线检查任务管理：任务管理包括三个部分：正在执行的任务、已定义的任务和任务执行的结果，即检查报告，报告可以导出为 Word、PDF、HTML 等格式；

3)策略管理：用户可以自定义基线检查策略（通过选择系统内的基线项进行组合；另外，可设定用户自定义基准值，例如口令长度要求）。

4.7.5 流量探针

本项目流量探针包含以下功能：

1.流量采集深度包解析

采用零拷贝、全程无锁化技术处理网络流量数据包，而且充分利用 CPU 向量化指令对各类模式进行识别或匹配，故即使在超大流量情况下，也能保证系统整体处理无延时；独有的智能协议识别技术，可高速、准确地识别上千种应用，检测各种协议伪装行为；支持 HTTP、TLS、SMTP、POP3、IMAP、FTP、SMB、RDP、SSH、Telnet 等应用协议的精准解码、元数据提取及存储、搜索、统计功能，并对可疑网络流量进行了全包留存。

2.攻击检测

内置多种网络攻击检测策略，支持对一般网络攻击、明文传输、过期系统或软件、木马检测、隐蔽通道、电子加密货币活动、勒索软件进行检测，支持检测的类型可达 34 种。

1)网络攻击检测：支持对一般的网络攻击进行检测，检测的类型包括端口扫描、拒绝服务攻击、漏洞利用攻击、SQL 注入攻击、缓冲区溢出攻击、Webshell 及其它类型的注入攻击；

2)明文传输检测：对网络传输中存在的明文传输行为进行检测；

3)过期系统或软件检测：支持对可能存在过期的系统或软件进行检测；

4)木马检测：支持对各类木马活动进行检测，包括但不限于木马软件下载、木马登录/回连以及其他木马通讯行为；

5)隐蔽通道检测：支持对各类隧道检测，对协议改写、安全洋葱等存在隐蔽通道的行为检测；

6)电子加密货币活动检测：支持对主流电子加密货币活动进行检测，包括但不限于比特币、莱特币、门罗币等；

7)勒索软件检测：支持对各类勒索软件进行检测，包括其登录行为、横向扩散行为等，检测的类型包括但不限于永恒之蓝、GandCrab、Satan 等。

3.文件检测

支持从 HTTP、FTP、SMB、邮件、QQ 等应用协议中还原各类文件，支持 MS Office 文件、Mac Office 文件、HTML、Flash、RTF、PDF，以及 Zip、RAR、Dmg、Tar、Gizp、CHM、BinHex、SIS 等归档文件。

4.文件静态扫描

对还原的文件进行加密检测、启发式扫描、威胁情报检测、数据泄密检测。

1)加密文件检测：支持对各类加密文件进行检测；

2)启发式扫描：支持对各类文件进行启发式扫描，检测威胁内容包含但不限于一般病毒、木马、蠕虫、各类灰件（含广告）、勒索软件等；

3)威胁情报检测：支持对各类文件进行恶意软件威胁情报匹配；

4)数据泄密检测：支持根据用户自定义的敏感词库，对各类传输文件进行扫描，检测内容中包含敏感词的文件，防止核心数据外泄。

5.威胁情报检测

整合威胁情报库，支持对各类恶意 IP、恶意域名、恶意 URL 以及恶意邮箱进行检测；检测的类型包括僵尸网络、木马回连、隐蔽通道、电子加密货币矿池等。

6.网络质量检测

具备发现带宽占用异常、ARP 风暴、ICMP Flood、TCP 建连时延过长、TCP 重传过多、TCP 零窗口过多等网络质量异常的能力。

7.异常行为检测

集成了网络自主研发的智能动态基线、模式信息熵等生成算法，通过一段时

间对学习对象的流量特征分析、建模，智能生成该对象多维度的网络特征，实施多维度的纵深检测机制，增加检测的准确性，降低误报概率。

4.7.6 视频防火墙

本项目视频防火墙包含以下内容：

1.终端识别

采用多种终端指纹技术，对全网资产进行扫描识别，可以发现全网网络资产，并识别终端类型，包括视频终端，windows，linux，网络设备，苹果终端，安卓终端等终端类型。

2.视频设备发现

根据接口中携带的信息对终端进行识别，可以识别出摄像头的序列号，型号，品牌等信息。

3.终端指纹识别

通过设备指纹识别技术，针对其他终端如电脑，手机终端，根据终端的应用流量特征识别终端的类型。可识别 windows，linux，网络设备等终端。

4.终端准入

对终端指纹识别技术，识别后的终端，通过准入策略对指定的 IP 网段，指定的终端类型，进行自动准入。同时进行终端指纹绑定检查，未被准入策略准入的终端被认定为私接终端。

5.终端阻断

对于私接/仿冒终端可以根据阻断策略，进行流量阻断或者交换机联动阻断。

串接部署，可以直接对网络流量进行数据包阻断；旁路部署，支持通过 SNMP 协议和交换机联动，配置 MAC 阻断列表到交换机中，从接入层面对终端进行阻断。

6.风险评估

通过主动端口扫描，漏洞扫描，弱口令扫描技术，主动发现存在风险的终端。采用针对视频终端定制的漏洞库，以及弱口令库，能有效评估视频专网中的风险。

7.应用识别

控制异常流量首先是要能够准确地基于应用进行精细化的访问控制，而这依赖于高效、精确的应用识别。支持基于深度包检测，深度流检测以及智能行为分

析三种应用识别技术。准确识别视频网络中各种视频流量。

8.漏洞防护

支持对多达几万种漏洞进行识别和防护，并已经加入视频专网中特有漏洞，漏洞库一直在持续维护更新。

可以在视频专网漏洞被发现后，通过及时的漏洞库升级，对还未进行安全固件更新的漏洞终端设备进行及时有效的防护。

9.病毒在线查杀

支持在线不影响业务的情况下对 HTTP，FTP 中上传下载的文件，进行查杀，有效防止在视频终端设备被攻破的情况下，对终端植入病毒，从而进行更广泛的传播，造成更大的危害。

4.8 等级保护建设设备清单

表 5-15 等级保护建设设备清单

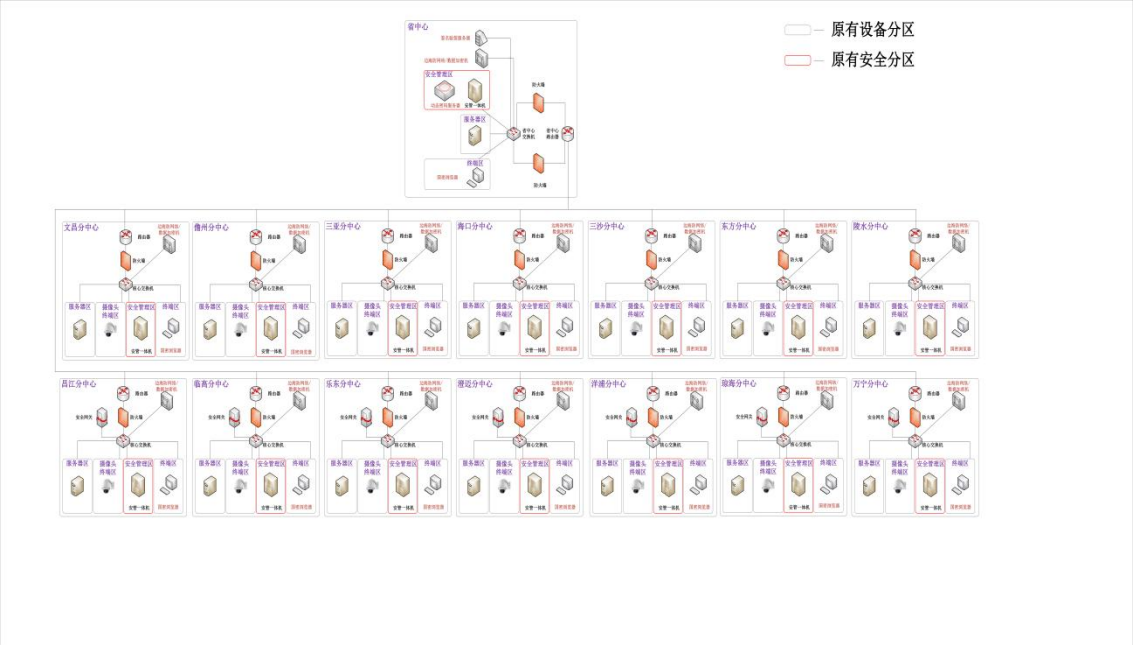
序号	种类	数量	部署位置
1	数据库审计	1	省中心
2	终端防病毒服务端	1	省中心
3	终端防病毒客户端	110	省中心和各分中心
4	服务器防病毒	60	省中心和各分中心
5	态势感知平台	1	省中心安全管理区
6	省中心流量探针	1	省中心
7	分中心流量探针	14	各分中心
8	视频防火墙	14	各分中心
9	静电手环	60	省中心和各分中心
10	视频监控系统	1	洋浦分中心
11	一体化机柜	1	省中心

5 密码应用建设方案

5.1 总体拓扑设计

依据密码应用安全性保护基本技术要求，结合实际业务保障需要，规划总体网络拓扑，以原高性能核心路由器作为该局域网的核心，承担全网的路由转发任务。根据《信息系统密码应用基本要求》（GM/T 39786-2021）的第三级建设要求，在整体网络区域新增相关密码安全设备对系统进行有效防护。升级改造后网络拓扑图如下图所示：

红色字体为本次安全建设新增设备



5.2 总体设计方案

5.1.1 物理和环境安全

1.身份鉴别

海南省 HF 监控系统各机房均部署了门禁系统对进出人员进行身份鉴别。对于身份鉴别的风险点采用以上措施进行缓解，本项目不涉及此项建设。

2.门禁记录完整性保护

电子门禁记录数据保存在数据库中，本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用国密 SM3 算法的数字签名技术或 HMAC 技术对进出机房日志等数据进行摘要，生成摘要值，验证时通过相同的数据、算法再算出摘要值进行比对，确保相关数据的完整性，其中所使用的密钥对由签名验签服务器的密码模块生成，存储在密码卡中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。

3.视频监控记录数据存储完整性

对于可以观看视频监控记录数据的机房，本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用国密 SM3 算法的数字签名技术或 HMAC 技术对视频监控记录数据进行摘要，生成摘要值，验证时通过相同的数据、算法再算出摘要值进行比对，确保相关数据的完整性，其中所使用的密钥对由签名验签服务器的密码模块生成，存储在密码卡中，不涉及密钥分发、导入与导出，密钥的备份与恢复、归档和销毁由密码设备管理员负责。

表 5- 16 物理和环境安全密码设备表

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
签名验签服务器	签名验签、数字信封、数据加解密	非对称 SM2 算法 杂凑 SM3 算法 对称 SM4 算法	遵循 GM/T 0060-2018《签名验签服务器机检测规范》;

5.1.2 网络和通信安全

本项目涉及四条通信信道，第一条是前端感知节点将采集的视频流回传到海南省 HF 监控系统的通信信道，第二条是业务人员用于访问海南省 HF 监控系统的通信信道，第三条是运维人员用于进行运维管理的通信信道，第四条是省中心和分中心之间用于传输数据的信息交互通道。

●前端感知节点将采集的视频流回传到业务系统的通信信道

需要依托于前端设备升级为具有安全功能的前端设备来完成后续数据的安全采集和数据的安全传输，由于硬件升级的投资过大，本项目不涉及此项。

●业务人员用于访问海防监控系统的通信信道

1.身份鉴别

本项目通过部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过建立安全可靠的传输通道，通过 BHF 网络/数据加密机识别服务器端的真实性，保证了通信实体身份的真实性。

2.通信过程中数据的完整性

本项目通过部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过建立安全可靠的传输通道，通过国密 SM3 算法的密码技术对通信链路进行完整性保护。

3.通信过程中重要数据的机密性

本项目通过部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过建立安全可靠的传输通道，通过国密 SM4 算法的密码技术对通信链路进行机密性保护。

4.网络边界访问控制信息的完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用基于国密 SM2 算法的数字签名技术对访问控制信息进行完整性保护。

●运维人员用于进行运维管理的通信信道

1.身份鉴别

本项目通过部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/

数据加密机,采用 SSL 协议的方式通过建立安全可靠的传输通道，通过 BHF 网络/数据加密机识别服务器端的真实性，保证了通信实体身份的真实性。

2.通信过程中数据的完整性

本项目通过部署本期需要部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机,采用 SSL 协议的方式通过基于国密的 SM3 算法建立安全可靠的传输通道，保证通信过程中数据的完整性。

3.通信过程中重要数据的机密性

本项目通过部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过基于国密的 SM4 算法建立安全可靠的传输通道，保证通信过程中数据的机密性。

4.网络边界访问控制信息的完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用基于国密 SM2 算法的数字签名技术或 HMAC 密码技术对访问控制信息进行完整性保护。

●省中心和 14 个分中心之间用来传输数据的信息交互信道

1.身份鉴别

本项目在省中心和分中心系统之间均部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机,采用 SSL 协议的方式通过建立安全可靠的传输通道，通过 BHF 网络/数据加密机识别双方身份，保证了通信实体身份的真实性。

2.通信数据完整性

本项目在省中心和分中心系统之间均部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机,采用 SSL 协议的方式通过基于国密的 SM3 算法建立安全可靠的传输通道，保证通信过程中数据的完整性。

3.通信过程中重要数据的机密性

本项目在省中心和分中心系统之间均部署遵循《SSL VPN 技术规范》（GM/T 0024-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过基于国密的 SM4 算法建立安全可靠的传输通道，保证通信过程中数据的机密性。

4.网络边界访问控制信息完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》(GM/T 0003-2012)、《SM3 密码杂凑算法》(GM/T 0004-2012)、《SM4 分组密码算法》(GM/T 0002-2012)的签名验签服务器和 BHF 网络/数据加密机，采用基于国密 SM2 算法的数字签名技术对访问控制信息进行完整性保护。

表 5- 17 网络和通信安全密码设备表

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
BHF 网络/数据加密机	建立国密 SSL 安全通道，为业务人员提供安全的访问通道，保证数据传输的机密性与完整性；同时能够对存储数据加密	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	遵循《国密 SSL 安全网关产品规范》(GM/T 0026)；
签名验签服务器	签名验签、数字信封	非对 SM2 算法 杂凑 SM3 算法 对称 SM4 算法	遵循《签名验签服务器机检测规范》(GM/T 0060-2018)；
国密浏览器	配合建立国密 SSL 通道，保证通道的机密性、完整性	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	《SM2 椭圆曲线公钥密码算法》(GM/T 0003-2012)、《SM3 密码杂凑算法》(GM/T 0004-2012)、《SM4 分组密码算法》(GM/T 0002-2012)。

5.1.3 设备和计算安全

设备与计算安全主要关注服务器的操作系统与核心数据库的安全，设备与计算安全建设设计方案内容如下：

1.身份鉴别

本项目通过部署遵循《动态口令密码应用技术规范》(GM/T 0021-2012)的动态密码服务器，采用双因素的方式进行认证(静态密码+硬件令牌/短信验证码)，

动态密码系统可以配合移动令牌使用，或者基于密码技术生成的短信验证码提交给动态口令服务器进行验证，用于保证登录身份的真实性。

2.远程管理通道安全

本项目通过部署遵循《BHF 网络/数据加密机规范》（GM/T0026-2014）的 BHF 网络/数据加密机，采用 SSL 协议的方式通过建立安全可靠的传输通道，保证远程管理通道的安全。

3.访问控制信息完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用国密 SM3 算法的数字签名技术对访问控制信息进行完整性保护。

4.日志记录完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用国密 SM3 算法的数字签名技术对日志记录进行完整性保护。

表 5- 18 设备和计算安全密码设备及服务

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
BHF 网络/数据加密机	建立国密 SSL 安全通道，为业务人员提供安全的访问通道，保证数据传输的机密性与完整性；同时能够对存储数据加密	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	遵循《国密 SSL 安全网关产品规范》（GM/T 0026）；
签名验签服务器	签名验签、数字信封	非对 SM2 算法 杂凑 SM3 算法 对称 SM4 算法	遵循《签名验签服务器机检测规范》（GM/T 0060-2018）；
动态密码服务器	可配合动态令牌、手	杂凑 SM3 算法	《动态口令密码应用技

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
	机短信等方式实现双因子认证		术规范》（GM/T 0021-2012）。
国密浏览器	配合建立国密 SSL 通道，保证通道的机密性、完整性	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）。

5.1.4 应用和数据安全

1.身份鉴别

本项目通过部署遵循《动态口令密码应用技术规范》（GM/T 0021-2012）的动态密码服务器，采用双因素的方式进行认证（静态密码+硬件令牌/短信验证码），动态密码系统可以配合移动令牌使用，或者基于密码技术生成的短信验证码提交给动态口令服务器进行验证，用于保证登录身份的真实性。

2.访问控制信息完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，采用基于国密 SM3 算法的数字签名技术和 HMAC 技术对访问控制信息进行完整性保护。

3.重要数据传输机密性

本项目通过部署遵循《BHF 网络/数据加密机规范》（GM/T0026-2014）的 BHF 网络/数据加密机通过 SSL 协议采用基于国密 SM4 算法建立安全可靠的传输通道，保证了通信过程中重要数据的机密性。

4.重要数据存储机密性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的

签名验签服务器和 BHF 网络/数据加密机，通过基于国密 SM4 算法的数字信封技术或加解密技术保证重要数据在存储过程中的机密性。

5.数据传输完整性

本项目通过部署遵循《BHF 网络/数据加密机规范》（GM/T0026-2014）的 BHF 网络/数据加密机，通过 SSL 协议采用国密 SM3 算法建立安全可靠的传输通道，保证了通信过程中重要数据的完整性。

6.数据存储完整性

本项目通过部署遵循《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）的签名验签服务器和 BHF 网络/数据加密机，通过基于国密 SM3 算法的数字签名技术保证重要数据在存储过程中的完整性。

表 5- 19 应用和数据安全密码设备及服务

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
BHF 网络/数据加密机	建立国密 SSL 安全通道，为业务人员提供安全的访问通道，保证数据传输的机密性与完整性；同时能够对存储数据加密	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	遵循《国密 SSL 安全网关产品规范》（GM/T 0026）；
签名验签服务器	签名验签、数字信封	非对 SM2 算法 杂凑 SM3 算法 对称 SM4 算法	遵循《签名验签服务器机检测规范》（GM/T 0060-2018）；
动态密码服务器	可配合动态令牌、手机短信等方式实现双因子认证	杂凑 SM3 算法	《动态口令密码应用技术规范》（GM/T 0021-2012）。
国密浏览器	配合建立国密 SSL 通道，保证通道的机密性、完整性	支持 SM2、SM3、SM4 算法，支持国密算法的 SSL 协议	《SM2 椭圆曲线公钥密码算法》（GM/T 0003-2012）、《SM3 密码

产品和服务名称	主要功能	涉及的密码算法和协议	遵循的标准
			杂凑算法》（GM/T 0004-2012）、《SM4 分组密码算法》（GM/T 0002-2012）。

5.3 密钥管理

本系统使用的业务系统身份证书由第三方 CA 颁发，为部署在本系统中的各密码设备和域名颁发数字证书。

本系统选用通过检测认证的签名验签服务器等商用密码产品，根据这些商用密码产品提供的安全策略，制定密钥管理方案，并严格遵照该方案进行使用和实施。

本系统的密钥按类型可分为设备密钥、用户密钥和数据加密密钥。其中设备密钥和用户密钥包括签名密钥对和加密密钥对，签名密钥对产生于各密码设备中，代表设备或用户的身份，其密钥证书由 CA 颁发，其生命周期管理由设备管理员根据指定的密钥管理规则进行管理，其更换周期遵循 CA 的密钥更新策略。数据加密密钥更换周期应遵循密钥管理规则制定的密钥更新策略。组织与职责

密钥管理主要由密码操作员、密钥管理员和密码审计员组成，并由业务部门安排相应人员担任。密钥管理员与密码操作员不得为同一人，且不得从事任何业务数据处理的工作。

●业务部门指定专门的密码操作员，其职责：负责密钥的生成、使用、分发、更新、销毁过程管理。

●业务部门指定专门的密钥管理员，其职责：负责密钥保管，确保密钥可用性、完整性、唯一性。

●业务部门指定专门的密码审计员，其职责：负责对密钥管理过程中的操作活动进行监督，确保操作过程的合规性。

5.3.1 密钥生成与保管

密钥生成必须以应用系统的需求或到期更换等规定的要求作为依据，密钥必须由不同部门或团队的两人（或以上）共同生成。

密钥生成申请应由信息系统所属责任部门密码操作员填写《密钥生成/装载和启用/分发申请表》，并经业务部门负责人和所属信息系统责任部门负责人审批后，交由密码审计员负责召集密码操作员进行密钥生成。

密钥生成应使用硬件加密机或其他安全的密钥生成工具，确保密钥的生成随机性。

密钥生成采用分段操作方式，分段次数不应小于两次。

密钥生成后，密码操作员记录下自己的分段密钥内容当场装入信封，并进行封口，由密码审计员在封存密钥的信封上加盖密封章或签名后，交由密钥管理员保管。封存过程中密码操作员、密钥管理员和密码审计员必须同时在场。

密钥管理员应在安全区域（如机要室或档案室）配备保险容器（如保险柜），用以存放密钥组件与密钥档案资料。

密钥分量应以信封密封保管，并信封上注明使用密钥的设备名称、密钥类型、使用期限、封存日期、使用人等信息。

密码操作员、密钥管理员临时离岗或调离岗位时，应进行所保管密钥交接工作，条件允许情况下，及时更新密钥，岗位临时替代者在离岗人员返岗后应进行交接。

密钥组件存取、使用情况应由密钥保管人员作好记录，记录也应存放在保险容器内，视同密钥组件处理。密钥记录保存期限应不低于记录对象的生命周期。

5.3.2 密钥申请与使用

密钥使用时，应由信息系统所属责任部门密码操作员填写《密钥生成/装载和启用/分发申请表》，并经其部门负责人审批后，交由密码审计员组织密码操作员和密钥管理员进行密钥的装载和启用。

在启用密钥之前，密码审计员应对密钥组件保管信封密封章或签名的完整性进行检查，同时对信封上所记录的密钥使用人信息与到场的密码操作员信息进行核对，在核对无误并在《密钥生成/装载和启用/分发申请表》上签名确认后，方可由密码操作员取用密钥组件。如人员信息不符，则应有原密码操作员的授权书或口头声明。

密钥装载和启用采用分段操作方式。密钥装载过程中，除当段密钥注入人和密码审计员，与此无关的人员均须离开。

密钥装载和启用完成后，已开封的密钥保管信封需重新封装，由密码审计员加盖密封章或签名后，交由原来的保管人员保管。密码操作员、密钥管理员和密码审计员在《密钥生成/装载和启用/分发申请表》上签字确认。

5.3.3 密钥分发与传送

针对外联机构分发给本单位的密钥，本单位应派出信息系统所属责任部门密码操作员接受密钥，在封存后移交相应的密钥保管人进行保管。

密钥组件不得采用电子邮件、传真、电传、电话等方式直接传递，传输过程中必须确保密钥的机密性和完整性。

5.3.4 密钥检查与更新

密钥管理员应不定期检查保管的密钥信封是否有被拆封，对检查结果进行登记。如果密钥失密，或者怀疑失密，应及时报告部门负责人，以便及时更新密钥。

密钥的更新应由业务部门密码操作员填写《密钥生成/装载和启用/分发申请表》，并经密码操作员所在部门负责人审批后，交由密码审计员组织密钥的更新生成与分发。

5.3.5 密钥销毁

当密钥已失效时，必须及时销毁密钥。失效密钥包括过期密钥、废除密钥、泄漏（含被攻破）密钥：

●过期密钥是指当密钥超过了生存期。

●废除密钥是指在测试环境中不再使用的密钥、生产环境中因应用程序的修改不再使用的密钥、存放介质发生损坏的密钥、设备报废或废弃在设备中不再使用的密钥等。

●泄漏密钥是指密钥在其生命周期内被泄漏或怀疑可能泄漏以及密钥被攻破等情况。

当密钥失效时，应由密码操作员填写《密钥生成/装载和启用/分发申请表》说明原因，并由业务部门负责人审批。

密钥销毁操作由密码操作员和密钥管理员共同进行，密码审计员负责监督。如果保存有密钥副本，也应当一起销毁。

密钥资料销毁的情况应记录在案，包括销毁时间、操作员、密码审计员等要

素。销毁记录由销毁人和密码审计员签字后与相关资料一同保存。

5.4 安全管理

系统建设应用需要完善的安全管理制度，保障各系统的安全管理。系统应用的安全管理主要包括安全制度的管理、安全人员的管理、系统安全实施的安全管理以及系统应急响应的安全管理。

5.4.1 安全制度管理

根据《基本要求》中安全管理制度方面的要求，制定与本系统相适应的密码安全管理制度和操作规范，内容包含密码建设、运维、人员、设备、密钥等 6 个方面，并同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

密码安全管理制度和操作规范发布后，每年年底，在项目建设单位内部组织专家和密码相关人员对密码安全管理制度和操作规范在使用过程中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的安全管理制度进行修订。

5.4.2 安全人员管理

根据《基本要求》中安全管理人员方面的要求，对本系统现有的人员管理制度进行补充和完善。

1.设置内部密码专题培训机制，每 3 个月组织一次，由内部人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规和标准规范、商用密码应用、商用密码应用安全性评估等多个方面，使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行；

2.在本系统完成密码应用改造后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品；

3.结合本系统情况，分别设立密钥管理员、安全审计员、密码操作员等岗位，明确各岗位职责，每个岗位均由 2 人担任；

4.在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理人员、

安全审计人员、密码操作人员与单位订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

5.4.3 安全实施管理

完成本方案编制后，委托密评机构对本方案进行评估，评估通过后，将本系统密码应用改造方案向密码管理部门备案，并同步对本系统进行密码应用改造，选用通过检测认证合格的商用密码产品，合规、正确、有效的建设密码保障系统。

依据评估通过的密码应用方案改造完成后，委托密评机构对本系统进行密评，密评通过后上线运行，上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

5.4.4 应急响应

根据《基本要求》中安全管理应急方面的要求，对本系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施；当本系统发生密码相关安全事件时，在事发后 3 小时内向省政府办公厅和省密码管理局进行报告；事件处置完成后 2 个工作日内，向省密码管理局汇报安全事件发生情况及处置情况。

5.5 设备功能要求

5.5.1 国密浏览器

国密浏览器全面支持主流 CPU、操作系统、流版签办公插件、1080p 及 4K 高清视频流畅播放、显卡硬件加速、用户隐私数据保护等，高效满足日常办公需求，打造 Web 应用统一支撑平台，建立基于浏览器的 Web 生态标准体系，主要是可以采用国密算法套件基于国密的单双向通信加密，能够满足国密改造要求。

1.高版本内核支持

国密浏览器应采用目前国内浏览器使用的最高版本及性能的内核 Chromium 86 内核。Chromium 86 内核中，CSS 属性与值 API 可让开发人员将变量注册为完整的自定义属性；新的 Native File System API，让开发人员可以构建功能强大的 Web 应用程序，与用户本地设备上的文件进行交互，同时 Chromium 86

内核的强韧性能，可以给用户带来快如闪电的网页浏览体验。

2.支持国密通讯算法

国密浏览器支持基于国家商用密码算法模块和国产安全协议模块，包括但不限于《GM/T 0003-2012 SM2 椭圆曲线公钥密码算法》、《GM/T 0004-2012 SM3 密码杂凑算法》、《GM/T 0002-2012 SM4 分组密码算法》等商用密码算法，并实现《GM/T 0024-2014 SSL VPN 技术规范》所规定的国密 SSL 协议进行网络通信端点之间的单、双向认证，更加有效地提高了网络信息通信的安全性。

3.国密信任证书管理

国密浏览器在界面中提供证书配置管理功能，用户通过配置界面将需要内置的国密证书导入到浏览器的信任列表中，就可以方便的访问国密加密站点。

4.USBkey 驱动管理

在国密加密通讯的双向认证过程中，浏览器需要通过读取 USB Key 中的证书来验证用户的身份，而浏览器需要通过加载 USB Key 的驱动才能正常识别到 USB Key 设备。但是由于缺乏统一的标准，各 USB Key 厂商对于自己设备的驱动文件存放路径是不同的，这就导致浏览器在加载 USB Key 时经常会出现驱动加载失败导致无法识别 USB key 的问题出现。国密浏览器提供国密 USB Key 的驱动管理功能，可以将海南省 HF 监控系统所使用的 USB Key 的驱动文件在管理界面中进行配置，从而保障浏览器启动后能够正常识别设备驱动。

5.5.2BHF 网络/数据加密机

BHF 网络/数据加密机支持基于证书的服务器和客户端身份认证，提供数据在传输过程中的机密性和完整性保护。全面支持 SSL/TLS 协议，配合设备自带的负载均衡、防火墙、HTTP 压缩等功能，为系统提供全方位的安全代理和应用加速服务，设备具备商用密码产品认证证书，遵循 GM/T 0024-2014《SSL VPN 技术规范》。同时也能够为信息系统提供高性能的数据加解密服务。

5.5.3 动态密码服务器

动态密码服务器结合时间、事件或挑战信息，生成每隔一段时间变化一次的动态密码（口令），避免静态口令泄露带来的安全隐患，为用户的合法身份认证提供了简捷、有效的认证手段。产品具备商用密码产品认证证书，遵循 GM/T

0021-2012《动态口令密码应用技术规范》。可以配合移动令牌使用，给移动令牌发送采用密码技术生成的验证码，主要用于对用户身份真实性的鉴别。

5.5.4 签名验签服务器

签名验签服务器能提供对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并对签名数据验证其签名真实性和有效性；支持不同 CA 的用户证书验证，提供 CRL/OCSP 等多种方式的证书有效性验证。满足用户在网络行为中不可否认、信息完整性、私密性等需求。产品具备商用密码产品认证证书，遵循 GM/T 0003-2012《SM2 椭圆曲线公钥密码算法》、GM/T 0004-2012《SM3 密码杂凑算法》、GM/T 0002-2012《SM4 分组密码算法》。其中包含的功能有：数字签名（完整性、抗抵赖性、不可否认性）、数据加密（机密性）、数字信封（机密性）。同时签名验签服务器能够提供对密钥的保护与管理。

5.6 密码应用建设设备清单

表 5- 20 密码应用设备清单

序号	设备名称	单位	数量	部署位置
1	国密浏览器	个	110	省中心和各分中心
2	动态密码服务器	台	2	省中心
3	BHF 网络/数据加密机	台	15	省中心和各分中心
4	签名验签服务器	台	1	省中心
5	业务系统身份证书	张/年	1	省中心

6 采购清单

硬件设备购置

序号	名 称	技术参数	单位	数量	备注
一	等级保护建设				
1	数据库审计	1、≤2U 机架式结构,2 个千兆电口，2 个万兆光口，2 个扩展槽，吞吐：10Gbps，可审计流量：2Gbps，峰值 SQL 处理能力：65000 条/s，日处理能力：5000 万条，4TB 硬盘，14 个 Agent 授权；3 年规则库升级许可； 2、支持细粒度解析 30+种数据库协议，包括关系型数据库、国产化数据库等；3、支持会话回放功能，支持播放速度调节； 4、支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理，进行隐私保护，敏感保护规则可自定义； 5、支持系统阈值设置，支持 CPU 报警设置、硬盘报警、内存报警功能。	套	1	数据库审计部署在省中心，负责对各中心数据库进行数据库审计，按照单节点审计流量 200M 计算，总计 8 个节点，计算冗余后可审计流量设定为 2G
2	态势感知平台	1、≤2U 机架式结构，≥2 个千兆电口，≥4 个 USB，存储≥6TB，内存≥32G；软硬件一体形态，提供态势分析、安全监测、安全处置、安全分析、资产管理、治理中心、知识情报等功能模块；包含 300 日志源授权； 2、支持已处置及未处置告警统计、告警人员处置分布、告警级别分布、告警类型分布，告警趋势、最新告警等告警信息展示； 3、支持恶意程序发生、传播、影响进行总体分析，包括恶意程序个数、恶意程序传播源数、攻击资产数、感染资产数等； 4、支持恶意程序分析，分析维度包括恶意程序数、影响资产数、恶意程序、被感染资产的可疑行为分布、威胁列表等； 5、支持高危端口/服务分析，分析	台	1	态势感知平台部署省中心的安全管理区中，承担一部分的网络管理和入侵检测的职能，包含日志源授权，能够对接第三方安全设备作为日志源节点，满足态势感知平台对分中心安全设备日志集中汇总的需求；配置治理中心模块，支持联动其他类型设备是联动防御策略管理，满足对安全策略、恶意代码、补丁升级等安全

		维度包括影响资产数、日志类型分布、高危端口发现趋势、威胁列表等。			相关事项进行集中管理
3	省中心流量探针	1、≤2U 机架式结构， ≥2 个 10/100/1000BASE-T 接口，≥2 个万兆 SFP 插槽；最大并发连接数：300W，综合检测能力：5G； 2、支持作为探针设备为态势感知提供安全数据； 3、支持独立的攻击检测引擎，支持多种以上的攻击规则库； 4、支持多种操作系统的僵尸主机检测，并对规则可设置相应警告、联动阻断动作； 5、支持隐蔽通信检测，支持对 HTTP、FTP、SMTP、IMAP、POP3、TELENT 等服务的隐蔽通信检测，可设置相应警告、联动阻断动作。	台	1	省中心流量探针部署省中心，负责采集省中心安全设备的日志与状态，同时能够对入侵攻击进行检测
4	分中心流量探针	1、≤2U 机架式结构， ≥2 个 10/100/1000BASE-T 接口；最大并发连接数：120W，综合检测能力：2G； 2、支持作为探针设备为态势感知提供安全数据； 3、支持独立的攻击检测引擎，支持多种以上的攻击规则库； 4、支持多种操作系统的僵尸主机检测，并对规则可设置相应警告、联动阻断动作； 5、支持隐蔽通信检测，支持对 HTTP、FTP、SMTP、IMAP、POP3、TELENT 等服务的隐蔽通信检测，可设置相应警告、联动阻断动作。	台	14	分中心流量探针部署在各分中心,每个分中心 1 台，负责采集各分中心安全设备的日志与状态，同时能够对入侵攻击进行检测
5	视频防火墙	1、1U 机架式结构，6 个千兆电口，4G 内存，支持 100 台设备探测和分析； 2、支持发现主流安防厂商视频监控设备，实现资产发现、准入控制等功能； 3、支持设备主动发现功能，能够获取视频专网中常用在网设备的 IP 和 MAC 地址、品牌、型号、 所属地址组、部门、发现时间等信息；	套	14	视频防火墙部署在各分中心，每个分中心 1 台，能够支持对每个分中心所有感知节点进行探测和分析，实现对感知节点进行指纹认证

		4、支持设备接入监测，对摄像头、CVR 等视频专用设备自动准入； 5、支持对待准入设备进行批量准入、阻断等操作； 6、支持通过 IP 地址、MAC 地址、设备类型、设备状态等信息设置复合条件查询设备准入信息。			
6	静电手环	静电手环	套	60	部署在各中心机房，每个中心机房 4 套，用于机房维修人员佩戴来降低静电对机柜中设备的破坏
7	视频监控系统	1、200 万半球网络摄像机，采用高性能 200 万像素 1/2.8 英寸 CMOS 图像传感器，最大可输出 200 万(1920×1080)@25fps； 支持 ROI，SMART H.264/H.265； 内置红外补光灯，最大红外监控距离 30 米； 支持报警 2 进 2 出，音频 1 进 1 出； 最大支持 256G Micro SD 卡； 支持 MIC； 支持 DC12V/POE 供电方式，支持 12V 电源返送，最大电流 165mA； 支持 IP67、IK10 防护等级； 2、4TB 监控硬盘； 3、4 路硬盘录像机； 4、系统布线。	套	1	部署在洋浦分中心，用于替代已经损坏的视频监控系统，采用与其他中心机房部署的摄像头相同的配置，起到安全物理环境中防盗窃与防破坏的效果
8	机柜	1、一体化二联柜，含全封闭式冷热通道或冷通道，系统控制组件，应急通风组件，照明组件，LED 背景灯光组件（可展示模块内告警情况），机柜门禁，配电单，PDU（每机柜 28 位以上），1 台 8KW 机架式空调（变频），动环监控（温湿度、空调、烟雾、漏水，短信模块，声光报警，高清触摸屏）； 2、全密封一体柜，含全封闭式冷热通道或冷通道，支持上线进线，前单开玻离门，后金属密闭门； 3、机架式空调机组采用全直流变频压缩机； 4、监控系统应具备自主知识产权，	套	1	一体化二联机柜部署在省中心机房中，采用与省中心机房部署的机柜相同的功能配置，用于容纳新部署在省中心机房的设备

		提供软件著作权证书； 5、本地显示系统应不小于 10 寸电容触摸屏，安装于微模块机柜前门。			
二	密码应用建设				
1	签名验签服务器	1、标准 1U 设备，双电源 400W-600W，≥2 核 4 线程 CPU X1，≥1T 硬盘，≥8G 内存，≥4 个千兆电口； 2、性能要求：签名：RSA2048：≥1000TPS，SM2：≥20KTPS；验签：RSA2048：≥22000TPS，SM2：≥15KTPS； 3、支持 SM2、SM3、SM4 国产密码算法； 4、支持 Attached/Detached/RAW 签名验签、数字信封加密/解密、签名二维码生成、PDF 电子签章、XMLSignature 等多种签名验签及数据加解密服务，支持 RSA 算法和国密算法； 5、支持多种证书状态查询服务：CRL 证书查询方式；OCSP 证书状态查询方式； 6、系统监控功能要求：支持监控服务器内存、CPU、网络和硬盘等系统重要参数，日志监控； 7、支持对称加密、非对称加密、数字信封、数字签名（提供签名客户端，完成客户端签名）、HMAC 等密码服务； 8、支持过滤弱算法，保证高强度的算法被使用； 9、具备商用密码产品认证证书。	台	1	签名验签服务器部署在省中心，负责保障所有分中心重要数据存储的机密性与完整性
2	动态密码服务器	1、标准 1U 设备，双电源 400W-600W，≥2 核 4 线程 CPU X1，≥1T 硬盘，≥8G 内存，≥4 个千兆电口； 2、支持≥5000 用户，响应性能≥500TPS； 3、支持 SM2、SM3、SM4 算法； 4、支持多种终端形态，包括：时间型令牌，事件形令牌，多键令牌，	台	2	动态密码服务器部署在省中心的安全管理区，选择双机热备来防止出现当 1 台设备发生故障时，运维人员无法进行双因子身份认证的问题

		手机软件、手机短信、二维矩阵等多种方式；实现应用系统身份鉴别双因子认证； 5、支持令牌管理，包括创建、冻结、解冻和作废令牌等，手工同步令牌密码、获取令牌解锁码等操作； 6、具备商用密码产品认证证书； 7、能够提供 windows、linux、AIX 系统客户端软件，为系统用户提供动态密码验证登录系统； 8、客户端与动态口令系统支持单向 SSL 加密通道。			
3	BHF 网络/数据加密机	1、用于安全性高，高速、高性能的应用环境支持对称算法，为信息安全传输系统提供高性能的数据加解密服务，为主机数据安全存储系统、身份认证系统以及对称、非对称密钥管理系统的主要密码设备和核心构件； 2、支持 SM2、SM3、SM4 国产密码算法； 3、采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数，生成 RSA 算法 1024/2048/3072/4096 密钥对，生成 SM 系统国产算法的 1024、2048、4096 位 SM2 密钥对； 4、密钥的安全存储:设备内可存储 50 对 SM2 密钥对，并且私钥部分受系统保护密钥的加密保护，持做双机热备或多机集群满足重要业务系统高可用性； 5、产品经国家密码管理局审批鉴定，具有商用密码产品认证证书； 6、含 400 个 SSL VPN 的客户端许可；IPSEC 吞吐率：2.5Gbps，IPSEC VPN 隧道数：20000；SSL 吞吐率：2.5Gbps，SSL 并发用户数：12000，管理用户数：30000。	台	15	BHF 网络/数据加密机部署在 15 个中心，每个中心 1 台，起到了服务器密码机和 SSL VPN 安全网关的作用，负责对重要数据的加密以及构建加密传输通道

成品软件购置

序号	名 称	技术参数	单位	数量	备注
一	等级保护				

	建设				
1	服务器防病毒	1 个 WindowsServer 客户端防病毒功能授权,含 3 年升级许可,按点数销售。针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。	套	60	服务器防病毒部署在各中心的核心服务器上，每个中心部署四套，用于保护核心服务器，支持 WindowsServer 客户端
2	终端防病毒服务端	用于对终端防病毒客户端进行安全策略、补丁下发的集中管理	套	1	终端防病毒服务端部署在省中心的数据处理服务器中，可以实现对各分中心 PC 终端部署的终端防病毒客户端进行统一管理
3	终端防病毒客户端	1、防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能； 2、客户端系统支持 Windows XP/VISTA/WIN7/WIN8/WIN10； 3、服务端支持采用 Docker 部署方式，能够快速恢复，横向扩展，可移植性强。	个	110	终端防病毒客户端部署在各中心的 PC 终端上,14 个分中心里每个分中心有 6 台终端，部署 6 个客户端，省中心有 20 台终端，部署 20 个服客户端，共部署 104 个终端防病毒客户端，6 个冗余终端防病毒客户端可按需分配
二	密码应用建设				
1	业务系统身份证书	代表业务系统身份，存放在签名验签服务器中，长期有效。	张	1	业务系统身份证书存放在签名验签服务器中，用身份证书中的公钥对签名进行验证

2	国密浏览器	1、客户端、管理平台支持主流国产 CPU，包括鲲鹏、龙芯、飞腾、兆芯；支持主流国产操作系统，包括中标麒麟、银河麒麟等； 2、支持地址栏、标签栏、收藏管理、数据清理、下载管理、插件、扩展、快捷键、鼠标手势功能； 3、支持 HTTP/1.1 HTTP/2.0 协议，支持 HTML5 最新标准，支持 WebGL(Web 图形库)，支持 MathML，支持 Web Workers； 4、支持证书配置管理功能，通过配置界面将需要内置的国密证书导入到浏览器的信任列表中，便于访问国密加密站点； 5、支持自动获取管理员针对特定网站配置的访问控制策略； 6、支持基于国密 https 站点和国际算法 https 站点的智能探测，自动切换通信协议； 7、支持本地数据的安全防护，对 cookie、历史记录数据进行加密保护； 8、支持弹出窗口的自动拦截，支持针对内部合规应用弹出窗口的统一可配置例外处理； 9、支持国密 USB Key 的驱动管理功能，在管理界面中进行 USB Key 的驱动文件的配置，便于浏览器启动后能够正常识别设备驱动； 10、具备商用密码产品认证证书。	个	110	国密浏览器部署在各中心的 PC 终端上，各分中心里每个分中心有 6 台终端，部署 6 个国密浏览器，省中心有 20 台终端，部署 20 个国密浏览器，共部署 104 个国密浏览器，6 个冗余国密浏览器可按需分配

系统集成实施

序号	名称	单位	数量
1	系统集成实施	项	1

核心产品：数据库审计

二、商务要求

2.1项目工期要求

★2.1.1 合同履行期限/工期：A 包：本项目总建设周期为 6 个月，第一阶段工期为 3 个月，第二阶段工期为 3 个月

2.1.2 建设地点：用户指定地点

2.2实施要求

2.2.1 投标人必须成立合理的组织机构，建立健全保障设计、开发工作顺利实施各项管理制度和质量保证体系，安排好足够的高技术人才参加本项目工作。

2.2.2 在组织机构中应明确各岗位的职责、任职资格及成果，确保项目顺利实施，应分别配备有项目经理、技术负责人承担本项目工作。投标人应确保服务于本项目的核心技术人员及主要团队人员稳定，未经采购人允许不得调整团队成员，采购人有权要求更换投标人项目团队不合格成员。

2.2.3 投标人必须针对本项目提供完善的项目管理实施方案（包括项目组团队的组建方案）和项目进度计划表。

2.3安装调试要求

2.3.1 投标人负责合同规定的相关设备、应用软件的现场安装、集成和联调。安装调试时所用的工具、设备由投标人负责。

2.3.2 投标人在安装调试阶段，保证不影响现有业务系统的正常运行。

2.4★验收要求（实质性条款）

项目完工后经采购人委托的第三方机构测评，海南省 HF 监控系统整体通过网络安全等级保护测评（三级测评结果达到“良”）及通过商用密码应用安全性评估，

设备、系统整体功能交付达到了全部规定要求，系统上线后稳定试运行 3 个月后，通过项目监理方认可，且在提交全部相关文档、报告、源代码（如有）等交付物的前提下，由中标方向采购方提出项目竣工验收申请，采购人按照国家、海南省信息化项目管理办法进行验收。

2.5售后服务

★2.5.1 整体项目提供不少于三年的免费维护，从项目通过竣工验收起算，中标单位应免费提供主要设备产品的 3 年质保。具体以签订的合同为准。

★2.5.2 软件部分由中标单位免费提供 3 年软件更新维护服务，包括但不限于：软件系统平台版本升级、数据包升级、BUG 修复、内核优化及功能优化等。

2.5.3 软件开发商和项目中标集成商应积极与项目建设单位对接需求，当项目建设单位提出新的需求需要修改软件系统时，开发商应当提供优惠的报价和完备的软件功能开发解决方案。

2.5.4 免费质保期过后，软件开发商和项目中标集成商应定期巡检，对已知故障汇报项目建设单位项目负责人，根据项目建设单位决策是否实施有偿升级维护。质保期后的维护费用应当符合市场主流报价并有一定的优惠。

2.5.5 运维管理单位职责包括以下部分：

2.5.5.1 对系统用到的硬件、软件做定期的检查。当出现人为或意外故障时，让系统及时恢复数据，保证系统正常运行（简单故障 8 小时内处理，复杂故障 48 小时内处理）；

2.5.5.2 对系统用到的硬件、软件做定期的升级，完善系统功能，满足用户合理的需求变动；

2.5.5.3 提供现场故障排除服务，并及时解决突发事件，减少故障损失；

2.5.5.4 协助建设方工作人员，接待领导对本项目运行情况的工作视察。

2.6运维服务内容

2.6.1 运维服务目标：保障系统 7*24 小时运行，业务不中断。

2.6.2 运维服务内容：本项目设备及系统软件部署及安装；运行期间预防巡检、出现问题的排查以及技术支持等。对系统相关的主机设备、操作系统、数据库和存储设备的运行维护服务，可以保证现有的系统的正常运行，降低整体管理成本，提高网络信息系统的整体服务水平。同时根据日常维护的数据和记录，提供信息系统的整体建设规划和建议，更好的为项目建设单位的信息化发展提供有力的保障。

2.6.3 由于信息化建设的特点及较高的专业化知识的要求，为保证本次项目的正常运行，主设备与系统的运行维护由设备供应商负责，辅助设备的运行维护

由系统集成商负责，质保期后系统日常的运行管理、使用维护由项目建设单位负责。

2.6.12 运维服务工作要求

2.6.12.1 本项目质保期三年

2.6.12.2 根据运维服务质量要求，运维人员须满足中级工程师和高级工程师的要求。

表 5- 67 运维服务工作量估算表

序号	分配职位	数量（人）	工作量	备注
1	运维负责人	1	320 天	长期负责运维团队的运行
2	驻点服务工程师	3	365 天	驻点工程师轮值驻场，保证现场长期有人驻守
3	技术支持工程师	5	120 天	随时准备应急技术支撑或重大活动现场服务保障

2.7运维服务提供方式

2.7.1 由运维管理单位确定具体的系统运维单位，运维单位有驻场运维和远程运维两种方式。建立运维管理制度和运维管理流程，搭建运维管理队伍，运维管理单位负责对日常运维工作进行管理、监督和绩效考核。

2.7.2 根据本项目需求，本项目的运维服务提供方式为现场值守、远程维护和定期巡检。

2.7.3 现场值守

2.7.3.1 现场运维值班由驻点服务工程师提供驻场服务，值守人员需要熟悉 BHF 控业务管理与处置流程，具备一定的 BHF 管控事务协调沟通能力，具备一定的网络故障维护能力、安全防护保障能力、视频服务管理能力，熟悉各项系统的操作维护，如涉海视频监控系统、军警民联防通信指挥调度系统、数据中心基础配套设备、多功能指挥大厅配套设备等日常操作及简单的故障修复。

2.7.3.2 现场值守分为日常维护和重大活动保障两个部分，提供 7*24 小时现场驻点值守服务。其中日常维护提供不少于 3 名技术人员驻场运维保障；重大活动保障提供不少于 3 名技术人员进行现场保障。

2.7.4 远程维护

2.7.4.1 远程维护服务主要由技术支持工程师提供，通过网络、电话、电子邮件、即时通信、远程协助等方式提供技术支持，提供全年 7*24 小时在线电话及传真服务，技术支持工程师在接收到通报故障的电话、传真或电子邮件后半小时之内将通过电话、传真或电子邮件等方式解决相关工作人员在使用过程中遇到的有关系统、服务器和网络的日常操作等方面的问题，并按规范记录存档。对于重大故障及疑难问题，需要在接到故障电话后及时到达现场排除故障远程进行系统故障的修复处理。

2.7.5 定期巡检

2.7.5.1 巡检内容包括由专业工程师按周期对系统的使用情况进行了解并进行常规性检查、调试和清理工作，记录系统的运行情况，包括检查各设备的工作状态，查看各设备的运行状态信息、报警故障信息等；检查系统配置，核实系统软件配置及对应版本；检查各中心的操作和管理软件使用情况；检查软件系统运行环境，检查网络操作系统软件、操作系统软件、数据库系统软件等稳定性。

2.7.5.2 每次巡检完成后以书面形式提交例行检查报告，包括检查发现的问题、系统现状评价、改进建议等。对例检发现的问题将在 1 个工作日内解决相关问题，并同时提交故障修复报告供存档，每年定期对系统提供以下服务：

2.8培训

2.8.1 投标人在项目建设过程中需对相关人员进行技术培训，在以后系统运行过程中亦需根据具体情况进行相应内容的培训，以保证系统的管理人员、技术人员和应用人员能够及时、准确地了解和熟练地运行系统。综合考虑本项目建设规模和业务应用系统情况，人员培训应分为两个方面进行：

2.8.2 对系统应用人员的培训

2.8.2.1 使之能够了解信息系统的建设思想、主要功能和操作规程，能够熟练应用这一系统辅助开展工作，并能结合实际工作需要提出各种改进意见。根据人员对系统的使用特点不同，对应用人员的培训分为两个层次：

2.8.2.2 对领导培训的主要目的是使有关主管领导对系统有一定的了解，同时能够应用系统进行决策、指挥工作。

2.8.2.3 对其他应用人员的培训，主要使他们在各业务环境下能够很好地利

用系统完成相应的专业工作，提高工作效率，提高信息的准确性和全面性。

2.8.3 系统运行维护人员的培训

2.8.3.1 运维人员培训主要包括以下几个方面：系统整体知识培训、业务系统培训、信息系统安全分级保护培训、安全事件应急处置培训等。通过培训使项目运维队伍能够充分掌握业务运营技术和维护经验，从技术上和管理上保证信息系统能正常运行。为了保障系统的安全稳定运行，还应对系统运行维护人员进行设备特性、系统功能、故障诊断、安全技术、规范操作、系统备份、系统恢复以及管理制度等方面的培训。

2.9付款时间、方式及条件：（以实际签署合同为准）

（1）合同签订之日起 20 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 25%；（2）所有设备到货并经过点验确认，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 25%；（3）项目初验合格并上线试运行后，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 20%；（4）项目通过整体竣工验收和第三方公司的结算审计后，乙方开具的正式有效发票和履约保证金保函(合同价的 5%)，甲方按审计金额支付剩余尾款。

（付款前提：甲方收到正规发票后，在财政资金拨款到位的前提下，20 个工作日完成支付。）

2.10知识产权要及其他要求：

2.10.1 知识产权归属中共海南省委军民融合发展委员会所有。

2.10.2 供应商保证对其销售的产品/服务拥有完全的所有权/处置权或已取得相关授权，不侵犯任何第三方专利、商标、著作权和其他合法权利，如因专利、商标权或其它知识产权而引起法律和经济纠纷，由供应商承担所有相关责任的同时不得耽误本项目进度。

2.10.3 供应商保证其提供的软件及服务不含有任何旨在破坏最终用户计算机信息系统和获取最终用户隐私信息的恶意代码。

2.10.4 投标技术文档需根据项目需求，编制包括但不限于总体设计、项目

实施方案、安全保密措施方案、售后服务方案、培训方案等内容。

2.10.5 招标人保留进一步核实投标人所提供证明材料真实性的权利，如经核实投标人所提供证明材料有虚假，保留提请省级主管部门将其列入不良企业黑名单的权利；如因此给招标人造成损失的，赔偿损失并将其列入不良企业黑名单。

B包采购需求

一、监理内容

监理内容为海南省海防监控系统安全达标升级改造项目的全部建设内容监理服务。

二、监理技术要求

（一）监理服务周期

本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。

（二）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、软件及应用技术培训、试运行、测试、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的工程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，最终实现工程监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程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。

（三）监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.6《信息化工程监理规范》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，对工程全过程进行监督、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工程合同中规定的功能、技术参数等目标。

确保工程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》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、部署、培训和运行；系统集成和软件服务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。

要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。

投标人应针对本项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件服务、工程培训等提出工程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、有代表性的信息工程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

协助建设方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。

4、 监理项目变更控制

协助用户对本项目的整体进行工期进度、投资、技术等方面进行变更管理、审核。以项目建设方和承建单位的可研、招投标文件，以及签订的合同建设内容为监理依据，确保项目实施控制在规定的范围内没有遗漏，如有则需进行变更流程。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。

（四）工程监理重点难点分析

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建设工程的监理服务工作。

1、 项目组织及总体技术方案的质量控制

（1） 协助审查项目承建方的合同及实施方案；

（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工程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，参与制定系统验收大纲，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：监督审查承建方提供的软件开发、测试、部署相关文件的标准性和规范化，在各项目验收时，应监督项目承建方提交符合规定的成套资料，包括纸质版和电子版。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、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） 审查各子系统承建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工程量完成情况进行审查，对为完成系统建设进度计划所采取的措施是否恰当，管理

上有无缺陷进行审查。要根据承建方所能提供的人员及产品性能复核、人员安排是否满足要求等，分析判断计划是否能落实，审查承建方提出的进度计划能否落实。如发现未落实，应及时报告采购人，要求承建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，在工程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，不影响后续工程的进行。

（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，向承建方提出要求和修改计划的指令。

4、 投资控制

（1） 审查设计图纸和文件。审查承建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。

（2） 严格督促承建方按合同实施，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，可以督促承建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，确保项目承建方按时履约。

（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，审核项目承建方的支付申请。

（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、 信息、工程文档管理

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、承建方的文件、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工程监理日记和工程大事记。

（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工程的成套资料，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，成立项目监理部，按工程需要派驻相应的专业人员进行项目现场监理，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） 制定工程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，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，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。

（五）工程各阶段的监理规划、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工程监理的工作流程，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开施工阶段、验收阶段、质保期阶段等。

1、 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） 了解施工条件准备情况；

3） 了解承建方实施前期的人员组织、施工设备到位情况；

4） 编制各个子项目监理细则；

5） 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）促使项目中所使用产品和服务符合合同及国家相关法律法规和标准；

4） 审核项目各个阶段进度计划；

5） 督促、检查承建单位进度执行情况；

6） 审查项目变更，提出监理意见；

7） 审查承建单位阶段款支付申请，提出监理意见；

8） 按周（月、旬）定期报告项目情况；

9） 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；

3） 进行试运行期系统测试，做出测试报告；

4） 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；

5） 进行试运行时间核算；

6） 协助建设方确认试运行通过。

2、 验收阶段监理

（1） 验收阶段

1）依照国家信息化管理细则，国家验收管理办法约定执行。

2）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；

3）监督检查承建单位作好用户培训工作，检查用户文档；

4）组织系统初步验收；

5）审查承建单位提交的竣工文档；

6）参与项目竣工验收；

7）竣工资料收集整理齐全并装订，签署验收报告；

8）审核项目结算；

9）审查承建单位阶段款支付申请，提出监理意见；

10） 向建设单位提交监理工作总结；

11） 将所有的监理材料汇总，编制监理业务手册，提交采购人；

12） 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）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。

3、 质保期阶段监理

监理单位承诺依据委托监理合同约定的工程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。

（六）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。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保证至少三名监理工程师在甲方现场进行监理协调调度。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。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

工程监理组织形式应根据工程项目的特点、工程项目承包模式、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工程监理的各项运作，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） 做好监理日记及工程大事记；

（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。

4、 监理合同管理要求

本项目建设过程中会与承建单位签订合同或协议，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；

（6） 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。

三、监理服务准则

遵照国家 GB/T19668.1-19668.6《信息化工程监理规范》，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。

四、监理依据

（1） 国家 GB/T19668.1-19668.6《信息化工程监理规范》和国家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承包工程合同

（3） 建设单位与监理单位签订的委托监理合同

（4） 本工程招标书、招标过程文件、各中标单位的投标书

（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） 与工程相关的技术资料

（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

五、安全保密要求

本项目要求投标人制定一整套工程监理安全保密制度，确定工程保密责任人，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。

六、监理验收要求

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。

监理工作的最终验收由主管部门组织，项目通过验收即为验收通过。

七、其它要求

总监理工程师、总监理工程师代表及专业监理工程师均需对应行业标准要求设定。

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。

八、商务要求

1.服务期限、服务地点和服务方式（履约时间、地点和方式）：

1.1 服务期限（履约时间）：自签订合同之日起，至建设项目完成竣工验收

1.2 服务地点（履约地点）：用户指定地点

1.3 服务方式（履约方式）：按本招标文件要求和中标人投标文件的规定

2.付款时间、方式及条件：

（1）合同签订之日起 20 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 40%；（2）项目初验合格并上线试运行后 20 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 30%；（3）项目通过整体竣工验收完成后 20 个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同总金额的 30%。

（付款前提：甲方收到正规发票后，在财政资金拨款到位的前提下，20 个工作日完成支付。）

3.知识产权要求：

投标人应保证在本项目使用的任何产品和服务（包括部分使用）时，不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其他知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。

4.其他：

4.1 项目的实质性要求：按本招标文件要求和中标人投标文件的规定。