

第三章 采购需求

海南省高级人民法院 2023 年至 2024 年信息化基础设施和网络安全

运维服务项目（A 包）

- 一、运维服务期限：合同签订之日起 2 年。
- 二、服务地点：用户指定地点。
- 三、交付方式：提供相应运维服务并出具相关报告。
- 四、采购资金的支付方式、时间、条件：运维服务费按年支付，每年度运维服务费用分两笔支付。
 - 4.1 年度运维服务开始之日起 30 天内，支付年度运维费用的 70%作为首付款。
 - 4.2 年度运维服务结束前 90 天内支付年度运维费的 30%作为第二笔费用。每年度在支付第二笔费用前进行考核，考核时扣除相应的款项后再予以支付剩余的运维费用。考核方式如下：

在运维过程中，如有部门书面投诉，每次扣款 2000 元；重大任务保障失误或造成恶劣影响，每次扣款 5000 元；管理的资产丢失不及时向采购单位报告，每次扣款 5000 元，同时扣除资产同等价值的款项。因工作过失造成采购单位资产损坏，要负责维修，并承担相关费用。
- 五、申请人的资格要求：见招标公告。
- 六、验收要求：按标书服务要求和国家行业标准进行验收。
- 七、本次采购标的对应中小企业划分标准所属行业为软件和信息技术服务业。

八、服务要求：

（一）项目概述

1、项目背景

在新时期信息化服务依法治国战略的职责更加重大，信息化服务法院司法改革的任务更加繁重，信息化服务人民群众司法需求的使命更加艰巨，信息化为法院科学发展提供的机遇更加难得。

人民法院信息化规划中提出了加强运维保障能力，全面提升运维质效的要求，要求参照相关运维标准，结合法院实际，建立质效型运维管理体系；改变以设备完好性为目标的应急式运维管理模式，通过建立质效运维体系实现故障预防和效能评估等功能，全面提升运维质效；建立信息系统应急处置平台和应急保障机制，提高处置突发事件的应急保障能力。

海南省高级人民法院根据法院信息化建设要求，并结合本省实际情况，组建专业的运维管理团队，通过运维服务外包的方式，建立质效型运维管理体系。针对运维对象开展信息化运维保障和服务，统一服务接口，规范管理体系，把控整体服务质量，提高工作效率，确保信息系统稳定运行，为法院业务提供全面有效支撑。

按照最高院《人民法院信息化建设五年发展规划（2021—2025）》（2022年修订版）的要求，参照《人民法院信息系统运行维护工作管理办法》（2016年修订版）、《人民法院信息系统运行维护工作规范》（2016年修订版）、《人民法院质效型运维标准规范》（2015年修订版）以及《海南省大数据管理局 海南省财政厅关于印发〈海南省政务信息化项目投资编制标准（试行）〉的通知》（琼数政〔2022〕28号）等标准规范，制定本需求。

2、项目目标

本项目旨在加强海南省高级人民法院正在使用的各类信息化基础设施运行监控、日常维护，加强网络安全运维，确保系统的正常运行，切实保障相关业务的正常开展。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。

(1) 在项目服务期内，保证各系统基础设施运行支撑水平满足日常业务需求，确保人民法院 IT 基础设施和应用系统正常、安全、高效、经济运行。

(2) 建立质效型运维服务体系，实现人员、技术和流程的标准化、规范化。通过该体系的建设和持续完善，促进运维工作实现标准化、规范化，满足信息运维工作集约化、精细化管理的要求，达到服务水平的持续提升。

(3) 建立信息系统运维评价体系。指标体系覆盖系统连续性服务能力、系统可用性、人员服务能力、项目管理等方面，通过服务指标监控和运行分析，实现对系统运行服务的集中、分级管理和监控，并能够及时调整运行维护策略。

(二) 建设依据与相关技术规范

1、政策文件

《人民法院信息化建设五年发展规划(2021—2025)》(2022 年修订版)

《人民法院信息系统运行维护工作管理办法》(2016 年修订版)

2、标准规范

《人民法院信息系统运行维护工作规范》(2016 年修订版)

《人民法院质效型运维标准规范》(2015 年修订版)

《智慧法院建设评价指标体系(2021)》

《关于加快建设可视化运维平台的通知》(法(信)明传(2017)53号)

《海南省大数据管理局 海南省财政厅关于印发〈海南省政务信息化项目投资编制标准(试行)〉的通知》(琼数政(2022)28号)

《质效型运维服务规范 第1部分：总则》FYB/T 59003.1-2020(2020年修订版)

《质效型运维服务规范 第2部分：基础设施运维》FYB/T 59003.2—2018

《质效型运维服务规范 第3部分：安全运维》FYB/T 59003.3—2018

《质效型运维服务规范 第4部分：应用运维》FYB/T 59003.4—2018

《质效型运维服务规范 第5部分：数据运维》FYB/T 59003.5—2018

《质效型运维服务规范 第6部分：应急处理》FYB/T 59003.6—2018

（三）运维服务内容

1、基础运维服务

基础运维服务主要负责对海南省高级人民法院信息化基础设施进行日常运维，保障信息系统的各类环境及设备的可靠、高效、持续、安全运行，包括机房环境、服务器存储设备、网络系统、计算机终端、大楼弱电系统和视频会议系统等（不含 2、重要设备及系统维保内容）。其中各类系统运行的网系由专网及互联网等网系组成。

提供基础运维服务需配备不少于十名驻场运维服务人员。

1.1 机房环境运维服务

负责对海南省高级人民法院信息化基础环境进行运维，包括电气系统、智能化系统、弱电系统等。具体工作包括对基础环境进行例行操作、响应支持、优化改善、调研评估等运维活动，从而保障机房辅助基础设备正常运行，不含设备维修和备品备件更换。

例行操作：主要包括对机房环境各系统进行监控、预防性检查、常规作业等运维活动。

响应支持：主要包括对机房环境各系统开展的事件驱动响应、服务请求响应、应急响应等运维活动。

优化改善：主要根据机房环境的特点和运行需求，对基础环境进行开展的适应性改进、增强性改进、预防性改进等运维活动。

质效分析：机房环境的质效分析时在例行操作、响应支持和优化改善工作基础上，提出机房环境质效改进建议和措施，不断提升机房基础环境运维的支撑质效。

1.2 服务器及存储运维服务

负责对海南省高级人民法院主八楼中心机房、南副楼四楼执行局机房及诉服大厅机房中的服务器、存储设备进行运维，不含设备维修和备品备件更换。

负责对服务器、存储状态等进行实时监控，包括服务器、存储设备 CPU 性能管理、内存使用情况、硬盘使用情况、系统进程管理、主机进程管理；监控记录磁盘阵列、磁带库等存储硬件故障提示和告警，并及时解决故障。

负责对服务器及存储进行例行操作、预防性检查，包括设备性能检测，运行状况观察、测试和分析、系统日志分析、应用程序备份、系统数据备份等。

1.3 网络运维服务

网络设备运维包含对海南省高级人民法院配备的交换机、路由器等网络设备的管理与维护，主要工作包括对交换机及路由器主动巡检、故障处理、应急响应、定期优化等内容，确保全省法院广域网线路、海南省高级人民法院到最高人民法院法院专网线路、互联网专线、干警办公终端网络等正常运行，不含设备维修和备品备件更换。

网络设备主要分布在主二楼、主四楼、主六楼、主八楼、北二楼、北四楼、北六楼、南三楼、南四楼、南六楼等弱电间。

1.4 计算机终端运维服务

主要工作包括对全院计算机终端设备（与海南法院智慧审判系统、海南法院智慧执行系统等信息系统相关的）运维，及时解决设备故障，保证其正常运行，不含设备维修和备品备件更换。

1.5 音视频运维服务

音视频运维服务主要负责对视频会议系统、有线电视、视频监控等音视频设备提供运维服务，确保音视频系统音响扩声、信号切换、集中控制、语音激励、信号显示、视频存储等能够正常使用，保障与高院相关的各类视频会议正常召开。主要工作内容包括主动巡检、应急响应、定期优化等工作内容，并在用户使用过程中提供技术支持和现场保障，不含设备维修和备品备件更换。

主动巡检：实时监控各个系统设备、软件运行状态；音视频矩阵、双机热备等定期进行切换和测试；对各类设备、软件进行日常巡检、定期巡检、专家巡检。

应急响应：各类设备故障及时响应与处置，主动向总服务台汇报处理进度和结果。

定期优化：定期调查音视频系统现状，制定信息系统服务计划和策略；定期进行系统优化和调整，如声音、图像清晰度优化；定期备份设备、系统日志、重要配置文件和脚本程序。

1.6 基础设施支撑系统成品软件运维服务

对海南省高级人民法院的基础设施支撑类信息系统关联的成品软件进行运维，如安防监控系统运维服务、非结构化数据综合管理系统运维服务等，包括例行操作、响应支持、优化改善、调研评估等运行维护活动。

1.6.1 安防监控系统运维服务

对海南省高级人民法院安防监控系统关联的成品软件（如安防综合管理平台、智能访客管理系统和 3D 导航系统等及配套的操作系统、数据库、中间件）进行运维，包括例行操作、响应支持、优化改善、调研评估等运行维护活动。

例行操作：实时监控系統运行状态；对设备、软件进行日常巡检、定期巡检、专家巡检。

响应支持：主要包括对安防监控系统开展的事件驱动响应、服务请求响应、应急响应等运维活动。

优化改善：主要包括对安防监控系统开展的适应性改进、增强性改进、预防性改进等运维活动。

调研评估：主要包括对安防监控系统开展的运行状态分析、评估、建议等运维活动。

1.6.2 非结构化数据综合管理系统运维服务

对海南省高级人民法院非结构化数据综合管理系统关联的成品软件（如 ORC 软件系统、云存储系统等及配套的操作系统、数据库、中间件）进行运维，包括例行操作、响应支持、优化改善、调研评估等运行维护活动。

例行操作：实时对非结构化数据综合管理系统运行状态；对设备、软件进行日常巡检、定期巡检、专家巡检。；

响应支持：主要包括对非结构化数据综合管理开展的事件驱动响应、服务请求响应、应急响应等运维活动。

优化改善：主要包括对非结构化数据综合管理开展的适应性改进、增强性改进、预防性改进等运维活动。

调研评估：主要包括对非结构化数据综合管理开展的运行状态分析、评估、建议等运维活动。

1.7 资产管理服务

负责海南省高级人民法院运维资产管理，建立和完善资产分类、资产命名、资产档案、资产保管、资产变更、资产核查等相关的资产管理制度、流程和规范。

资产保管：负责对本运维项目中涉及的资产进行管理，包括有效使用资产、合理调配资源、防止资产流失。

资产档案：负责对本运维项目中涉及的资产建立资产档案，包括资产大类、细类、名称、数量、用途、安装部位、所属系统、保修期限、SN号、原厂商、集成商、运维商、维修更换情况等。

资产标识：制作信息化资产标签，对资产实体进行标识。

资产核查：对所承担运维的信息化资产进行整理，并配合采购单位职能部门做好资产核查工作，将资产清单与资产实物进行一一核对，维护资产清单准确性。

资产变更：当资产发生变更时，及时更新资产标识、资产清单。所有变更资产需最高人民法院运维主管部门的签字认可。

1.8 质效型运维服务

按照中华人民共和国法院行业信息化建设标准《质效型运维服务规范 第1部分：总则》（以下称为“总则”）等质效型运维服务规范要求，建立质效型运维服务体系。需取得标准中涉及第6.2.3章节、第7.2.5章节中与一种法院业务应用系统的监测方法及装置（CN201710512518.7）相关授权的和正在申请的专利的使用。（详见附件4中华人民共和国法院行业标准《质效型运维服务规范 第1部分：总则》（FYB/T 59003.1—2020）（需在投标文件中提供获得相关授权的和正在申请的专利的使用的证明材料复印件加盖公章）

2、重要设备及系统维保

重要设备及系统主要采用原厂维保的方式，做到提前预防、快速响应、及时处理，确保其可靠、高效、持续、安全运行。

2.1 UPS 维保

对海南省高级人民法院主楼八楼中心机房、主楼负一楼机房和南副楼四楼执行局机房的UPS（不含电池组）与配电柜、列头柜等进行定期设备检测、清洁，保障UPS的正常运行。主要包括对UPS系统的巡检、维修、易损件更换等工作。

2.2 动力监控系统维保

主要负责机房动力监控系统故障诊断、修复、系统性能维护，保持系统稳定高效运行。

定期测试监测以及系统环境保障、故障处理、巡检、监控点位接入等常规工作，包括检查各个信号转换模块、通讯模块、系统主机工作情况，并以季度为单位总结运维工作并形成报告。

2.3 精密空调原厂维保

对海南省高级人民法院主八楼机房两台精密空调进行运维，包括设备日常检测、清洁室外机、常规维护、设备年检；易损零部件维修、更换；设备运行日志填写，并生成季度与年终巡检报告。

2.4 高清 MCU 原厂维保

针对华为视频会议高清 MCU 平台提供原厂维保，对设备进行巡检、维修、易损件更换以及重大会议时现场保障支持，保障设备的正常运行。

2.5 核心交换机原厂维保

对目前两台华为广域网核心交换机提供原厂维保，保障交换机的正常运行、巡检、维修、易损件更换等工作。

2.6 LED 大屏原厂维保

对海南省高级人民法院主三楼、主二楼、诉服中心、西大门等核心区域的大屏进行原厂维保，对大屏进行维修、易损件更换等工作，进一步保障大屏的正常运行。

2.7 网络安全设备原厂授权及升级服务

为海南省高级人民法院主楼八楼中心机房入侵防御及防毒墙提供 2 套病毒防护 1 年特征库升级服务和 2 套入侵防御特征库 1 年升级授权服务，从授权到期时间开始计算。

3、网络安全运维

网络安全运维包括提供渗透测试服务、漏洞扫描服务、流量监控及威胁分析服务、安全

设备运维及加固服务、应急响应服务、重大活动安全保障服务、安全事件运营服务、实战型应急演练服务以及网络安全态势感知平台服务等。

同时，协助完成网络安全管理工作、落地网络安全制度、网络安全规划优化、网络安全运维组织建设、流程规范管理编排、数据安全制度机制编排、网络安全意识宣贯等。

提供网络安全服务需配备不少于三名驻场网络安全服务人员。

3.1 渗透测试服务

每年选取不少于 5 个高院重要业务系统开展 1 次渗透测试。

采用人工黑盒的方式对海南省高级人民法院重要应用系统进行模拟攻击测试，并提出安全加固建议。主要测试方法包括：信息收集、端口扫描、远程溢出、口令猜测、本地溢出、客户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试等，服务包含一次安全整改指导以及一次复查测试。

3.2 漏洞扫描服务

每月不少于一次漏洞扫描服务，通过自动化扫描工具，对法院专网所有系统服务器、网络设备、安全设备等进行漏洞扫描、软件漏洞扫描、端口及服务探测、弱口令扫描等，排查检测系统可能存在的各类安全风险，并提供漏洞修复建议。

3.3 流量监控及威胁分析服务

对来自网络安全态势感知平台或其他流量分析设备对法院专网及互联网的威胁流量进行分析研判，找出确认或可能存在的攻击行为，对受害目标和攻击目标精准定位，攻击途径和攻击者背景通过与云端数据、威胁情报等结合溯源分析，帮助海南省高级人民法院发现和解决法院专网及互联网各层面的安全风险。每月提供一份流量监控及威胁分析报告。

3.4 安全设备运维及加固服务

主要工作包括主八楼中心机房及南副楼四楼执行局机房的光闸、防火墙、入侵防御等网络安全设备的日常运维，定期对安全设备、网络设备、主机、系统服务器等安全情况进行巡

查检测，并指导系统开发商完成安全加固，优化网络安全设备策略，定期进行策略配置变更，排查服务器用户最小化、服务启用最小化、访问最小化及端口最小化落实情况。安全加固指导类型包括主机加固、数据库加固、服务器加固、应用安全加固等。

3.5 应急响应服务

根据事件类别，提供应急响应服务，通过现场支持的形式，负责对客户遇到的突发性安全事件进行紧急分析和处理。主要工作内容包括：突发事件相关信息的收集、事件的分析溯源、报告提交、问题解决建议等。紧急事件主要包括：勒索病毒、病毒和蠕虫事件、黑客入侵事件、数据泄露、挖矿事件等。

3.6 重大活动安全保障服务

为确保海南省高级人民法院在重保期间业务系统持续、稳定的运行，确保重要业务操作行为的可审计，抵御黑客、恶意代码、病毒等对用户信息系统的攻击与破坏，防止对用户信息系统的非法、非授权访问、恶意篡改、挂马等等，在重大活动时期（如两会、国庆、“护网”等），开展安全检查、驻场保障以及应急值守等，对海南省高级人民法院重要系统进行安全保障。

3.7 安全事件运营服务

主要包括以下几个方面内容：

- (1) 配合用户督导各业务系统运维公司完成网络安全事件整改。
- (2) 配合用户完成网络安全检查迎检工作。
- (3) 配合用户对各业务系统运维人员进行安全培训与意识宣贯工作，提高整体安全认知。
- (4) 配合用户分析安全方面监管政策和要求，修改完善与信息安全管理体系相关的策略、制度、规范、标准和流程等。

3.8 实战型应急演练服务

每年开展一次实战型应急演练，由红队攻击小组，对用户目标系统进行攻击，防护工作小组完成防守方工作，实施对抗并进行安全防护，通过真实攻击对抗来检验和提高相关人员的临场组织指挥、队伍调动、应急处置技能和后勤保障等应急能力。

(1) 发现应急预案中可能存在的问题和不完善之处，使应急预案更为科学、有效的执行。

(2) 提高应急人员在紧急情况下妥善处置事故的能力。

(3) 完善应急管理相关部门人员的工作职责，提升协同作战处置能力。

(4) 通过应急演练，提高参演和观摩人员风险防范意识。

(5) 完善应急管理和应急处置技术，丰富应急经验和应急工具以应对不同场景的安全事件。

3.9 网络安全态势感知平台服务

在法院专网部署整套网络安全态势感知平台（含足够的流量探针），全方位监测专网办公区、专网服务器区及广域网区等区域的数据流量。平台通过采用先进的大数据分析技术架构和 AI 深度感知引擎，运用用户实体行为分析、安全编排与自动化响应、多维态势感知等技术，为海南省高级人民法院提供全局安全态势感知能力，保障其业务不间断稳定运行，且通过威胁发现、智能研判和自动化响应处置的流程，提高安全运维工作效率，构建智能安全运营体系，实现安全运营的闭环管理。

（四）运维服务要求

1、运维服务流程

运维服务流程符合海南省高级人民法院的实际需要，运维服务流程与服务需求结合合理，明确运维服务流程的实现方式。

2、运维服务工作计划

制定运维服务工作计划，按计划开展运维工作。

3、基础设施故障响应及修复

基础设施从出现故障到恢复的时间<30 分钟。

4、计算机终端故障响应

与信息系统相关的计算机终端出现故障后的响应时间<10 分钟。

5、运维资产管理

建立完备的资产管理体系，实时更新台账；资产实物与账目 100%一致；实物资产的硬件配置 100%完整；资产标识覆盖率和准确率 100%；定期清洁设备资产环境 6 次/年。

6、机房环境管理

巡检次数不少于 1 次/天；温湿度、UPS 负载情况监控覆盖率 100%。

7、重大责任安全事故次数

因运维失误导致信息失窃或泄密、黑客入侵、全网病毒爆发等信息安全事故的次数=0 次。

8、运维响应时限要求

运行维护 级别	可用性	持续性	安全性	响应速 度
一级（非常 重要）	连续正常运行 时间 >95%；故	系统非计划停机 时间少于 3 天/	严格杜绝特别重大安全事故， 尽可能避免重大安全事故，较	即时

	障次数<3 次/月	季度, 平均故障解决时间小于 5 小时/次。	大安全事故控制在 1 次/年以下, 一般安全事故控制在 3 次/年以下。	
二级 (重要)	连续正常运行时间>90%; 故障次数<5 次/月	系统非计划停机时间少于 5 天/季度, 平均故障解决时间小于 8 小时/次。	严格杜绝特别重大安全事故, 尽可能避免重大安全事故, 较大安全事故控制在 2 次/年以下, 一般安全事故控制在 5 次/年以下。	响应时间 <10 分钟
三级 (较重)	连续正常运行时间>80%; 故障次数<5 次/月	系统非计划停机时间少于 8 天/季度, 平均故障解决时间小于 24 小时/次	严格杜绝特别重大安全事故, 尽可能避免重大安全事故, 较大安全事故控制在 3 次/年以下, 一般安全事故控制在 8 次/年以下	响应时间 <20 分钟
四级 (一般)	连续正常运行时间>70%; 故障次数<8 次/月	系统非计划停机时间少于 15 天/季度, 平均故障解决时间小于 72 小时每次	严格杜绝特别重大安全事故, 尽可能避免重大安全事故, 较大安全事故控制在 3 次/年以下, 一般安全事故控制在 10 次/年以下。	响应时间 <30 分钟

9、信息安全保密要求

运维服务商所有运维人员必须遵守海南省高级人民法院对信息安全保密的各项管理规定和要求, 公司签署信息安全保密协议, 个人签署信息安全保密承诺书, 采取切实可行的措施保障本项目的网络与信息安全。

10、服务文档管理要求

运维服务商应编制、维护和保管各类运维过程文档和系统文档资料; 运维服务商应保存好运维服务过程中各种记录和文档; 运维服务商应以月为单位总结日常运维服务工作; 运维服务商应当规范管理运维服务过程中的各种专项报告。

11、质效型运维体系建设

参照中华人民共和国法院行业信息化建设标准《质效型运维服务规范 第1部分：总则》（FYB/T 59003.1-2020）（2020年修订版）、《质效型运维服务规范 第2部分：基础设施运维》（FYB/T 59003.2-2018）、《质效型运维服务规范 第3部分：安全运维》（FYB/T 59003.3-2018）等质效型运维服务规范要求，进行质效型运维体系建设。（详见附件4、5、6）

质效型运维服务体系以基础设施、应用系统、数据和安全为运维对象，以运行对象的关键指标为核心，以人员管理、资源管理、过程管理为保障，通过服务策划、服务实施、服务检查和服务改进，不断提升服务质量和应用成效。本项目主要涉及基础设施和安全运维。

基础设施运维的关键指标主要包括设备故障率、CPU资源利用率、内存资源占有率、磁盘读取速度、磁盘写入速度、网络中断次数、网络延迟、带宽利用率、网络性能、存储空间占有量（率）、存储性能等。

基础设施运维的关键指标是评估人民法院基础设施质效的基础，要在日常运维过程中不断优化完善关键指标并实施监控，以充分掌握基础设施质效，为质效提升提供依据。

安全运维的关键指标包括网络被攻击次数、有害程序事件数、终端漏洞数、服务器漏洞数、安全设备运行状态、网络防护能力、主机/终端防护能力、应用防护能力、数据防护能力等。

安全运维的关键指标是评估人民法院信息系统安全质效的基础，要在日常运维过程中不断优化完善关键指标并实施监控，以充分掌握信息安全质效，为质效提升提供依据。

11.1 人员管理应明确组织架构，岗位职责并制定相应的人员储备，人员培训和人员考核制度。

本项目要求派驻人员岗位职责如下（共13人）：

序号	岗位	职责
1	机房环境运维服务人员	投标人拟派驻的驻场服务人员不能少于1人，负责对主八楼中心机房、负一楼机房、南副楼四楼执行局机房环境进行维护，保证机房辅助基础设备正常运行。
2	服务器及存储运维服务人员	投标人拟派的驻场服务人员不能少于1人，负责海南省高级人民法院机房环境运维服务及对高院的云平台、X86服务器、Unix服务器、虚拟化平台等软件和硬件进行维护。并对相应应用系

		统的例行操作、监控、预防性检查和常规操作，包括系统栏目更新、系统日志分析、应用程序备份等。
3	网络运维服务人员	投标人拟派的驻场服务人员不能少于1人，负责对高院专网、互联网、涉密内网、移动专网、外部专网五大网络系统及其内部的交换机、路由器等设备进行维护。
4	计算机终端服务人员	投标人拟派的驻场服务人员不能少于2人，负责对办公办案人员使用的PC、打印机、复印机、传真机、操作系统、网络接入、办公软件等进行日常维护。
5	音视频管理服务人员	投标人拟派的驻场服务人员不能少于2人，负责对高院视频会议系统、远程接访、有线电视、视频监控等设备进行维护，重大会议、接访及活动进行保障。
6	基础设施支撑系统成品软件运维人员	对海南省高级人民法院的基础设施支撑类信息系统关联的成品软件进行运维，如安防监控系统运维服务、非结构化数据综合管理系统运维服务等，包括例行操作、响应支持、优化改善、调研评估等运行维护活动。
7	资产管理服务人员	投标人拟派的驻场服务人员不能少于1人，负责海南省高级人民法院运维资产进行管理。建立和完善资产分类、资产命名、资产档案、资产保管、资产变更、资产核查等相关的资产管理制度、流程和规范。
8	质效型运维服务人员	投标人拟派的驻场服务人员不能少于2人，其中项目经理1名，质效运维服务台人员1名。负责对派驻人员的全面管理、组织领导完成所承担的各项运维工作任务，负责与运维主管部门之间的日常沟通、协调，按时向运维主管部门交付各种维护文档和记录。
9	安全服务人员	投标人拟派的驻场安全服务人员不能少于3人，提供渗透测试、漏洞扫描、流量监控及威胁分析、安全设备运维及加固、应急响应、重大活动安全保障、安全事件运营、实战型应急演练等运维服务，确保数据和信息系统的安全。

11.2 资源管理是运维服务的重要辅助手段，主要包括服务台、知识库、运维工具等。通过运维资源的使用，可以提高运维服务的效率、提高发现问题解决问题的能力及系统故障时的快速恢复能力。

服务台：为进一步保障日常计算机终端运维工作，设立统一需求受理服务台，利用电话、网络等方式提供技术支持和服务，包括故障响应、诊断与解决，对所有的服务请求进行受理、记录、分发、跟踪和反馈，整理归档各类服务文档等。

知识库：建立故障处理资料库。根据运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。

运维监控工具：通过运维监控工具，实现对基础设施、网络设备、安全设备等进行监控或管理。

11.3 过程管理是人民法院实施质效型运维的重要保障，通过制定相应的管理制度和服务流程，使得运维过程和结果可控，确保达到预期效果。

具体内容包括：

(1) 运维流程管理：主要包括服务台服务流程、问题处理流程、巡检流程、资产管理流程、应急响应流程。

(2) 运维制度规范：主要包括运维职责、环境管理、节假日管理、安全管理、文档管理等，以及巡检、终端现场服务、公共信息发布、用户权限变更、视频会议等制度和规范。

(3) 运维绩效管理：对运维工作的相关数据进行收集、归类 and 统计，生成相关报表，以真实数据客观反映运维工作的成效。

(4) 其他管理服务：主要包括特殊时期值守、项目协助配合、其他交办任务等。针对特殊时期的信息网络系统运维需求提供保障服务，确保信息网络系统的安全稳定；配合其他信息化项目的开展，按照采购单位具体要求，为在海南省高级人民法院进行的其他信息化项目提供相关信息或资料、配合调试、安排人员值守、临时保管设备等；及时响应和完成采购单位交办的各项临时任务，提供优质的服务。

(五) 运维采购明细表

本项目 A 包采购预算（最高限价）为：627.3 万元人民币，报价不得超过采购预算（最高限价），否则视为无效投标。每年度采购预算详见表 5.1 《项目采购预算表》。

投标人除提供本项目 A 包总体报价外，还需按年分别提供每年度的运维服务报价（每年度报价不得超过每年度采购预算，否则视为无效投标）。

表 5.1 项目采购预算表

2023 年费用 (万元)	2024 年费用 (万元)	总费用 (万元)	服务期限	备注
308.8	318.5	627.3	2 年	

表 5.2 2023 年项目采购明细表

序号	运维项	运维服务内容		服务期限	备注
1	基础运维服务	机房环境运维服务		合同签订之日起 1 年	配备不少于十名驻场运维服务人员
		服务器及存储运维服务			
		网络运维服务			
		计算机终端运维服务			
		音视频运维服务			
		基础设施支撑系统成品软件运维服务			
		资产管理服务			
		质效型运维服务			
2	重要设备及系统维保	设备维保	UPS 维保	合同签订之日起 1 年	
			动力监控系统维保	合同签订之日起 1 年	
		原厂维保	精密空调原厂维保	2023 年 9 月 15 日至第 1 年度运维截止日期	
			高清 MCU 原厂维保	2023 年 10 月 22 日至第 1 年度运维截止日期	
			核心交换机原厂维保	合同签订之日起 1 年	
			LED 大屏原厂维保	合同签订之日起 1 年	
		合同签订之日起至			

				第1年度运维截止日期	
				2023年 12月25日 至 第1年度运维截止日期	
3	网络安全 运维	基础安全服务	渗透测试服务	合同签订之日起1年	配备不少于三名驻场安全运维服务人员
			漏洞扫描服务		
			流量监控及威胁分析服务		
			安全设备运维及加固服务		
			应急响应服务		
			重大活动安全保障服务		
		安全事件运营服务			
应急演练服务	实战型应急演练服务				
网络流量安全分析平台租赁服务	网络安全态势感知平台服务				
4	专利费	按照中华人民共和国法院行业信息化建设标准《质效型运维服务规范 第一部分：总则》（以下简称“总则”）等质效型运维服务规范要求，建立质效型运维服务体系。需取得标准中涉及第6.2.3章节、第7.2.5章节中与一种法院业务应用系统的监测方法及装置(CN201710512518.7)相关授权的和正在申请的专利的使用。		第1年度	

表 5.3 2024 年项目采购明细表

序号	运维项	运维服务内容		服务期限	备注
1	基础运维服务	机房环境运维服务		第 2 年度	配备不少于十名驻场运维服务人员
		服务器及存储运维服务			
		网络运维服务			
		计算机终端运维服务			
		音视频运维服务			
		基础设施支撑系统成品软件运维服务			
		资产管理服务			
		质效型运维服务			
2	重要设备及系统维保	设备维保	UPS 维保	第 2 年度	
			动力监控系统维保		
		原厂维保	精密空调原厂维保		
			高清 MCU 原厂维保		
			核心交换机原厂维保		
			LED 大屏原厂维保		
			网络安全设备原厂授权及升级服务		
3	网络安全运维	基础安全服务	渗透测试服务	第 2 年度	配备不少于三名驻场安全运维服务人员
			漏洞扫描服务		
			流量监控及威胁分析服务		
			安全设备运维及加固服务		
			应急响应服务		
			重大活动安全保障服务		
			安全事件运营服务		
		应急演练服务	实战型应急演练服务		

		网络流量安全分析平台 租赁服务	网络安全态势感知平台服务		
4	专利费	按照中华人民共和国法院行业信息化建设标准《质效型运维服务规范 第一部分：总则》（以下称为“总则”）等质效型运维服务规范要求，建立质效型运维服务体系。需取得标准中涉及第6.2.3章节、第7.2.5章节中与一种法院业务应用系统的监测方法及装置(CN201710512518.7)相关授权的和正在申请的专利的使用。		第2年度	

附表：海南省高级人民法院设备清单

序号	名称	品牌	技术参数	数量	型号	备注
一、基础环境						
1	动力监控系统		供配电监测及UPS监控系统等	1套	研华科技610L	含维保
2	精密空调	佳力图	60KW	2台	MEAD602	含原厂维保
3	UPS系统	科华		3套	KR3340	含维保
二、硬件设备						
1	服务器	华为		31台	2288H V5 (1台) DAE52435U4 (1台) H22H-05 (3台) RH2288H V2(1台) SPE62C0300 (1台) DAE22435U4 (3台) DEA12435U4 (

					3 台) netengine 8000 m8 (1 台) RH2288 V3 /H22M-03 (5 台) OceanStor 5300 V3 磁盘 (1 台) RH5885 V3/H58M-03 (11 台)	
2	服务器	浪潮		28 台	NF5245M3 (1 台) MF5240M3 (2 台) MF8460M3 (1 台) NF5280M5 (8 台) NF5280M4 (1 台) NF8460M3 (15 台)	
3	服务器	IBM		5 台	X3650 M4 (3 台) X3750 M4 (1 台) XSERIES 346 (1 台)	

4	服务器	海康威视		13 台	安防 /IS-VSE2326 B-BBC (1 台) /DS-VE22S-B (2 台) /DS-VR1104C -BAC (1 台) /IS-VSE2326 C-DDA (1 台) /DS-AB1016S (1 台) /IS-VSE2326 (2 台) DS-A80636S/ XG (4 台) ids-9608NX- 18/X (1 台)	安防
5	服务器	科达		2 台	KDM2801H	监控平 台
6	服务器	长城		10 台	擎天 CF520	2019 项目
7	服务器	惠普		1 台	DL380G6	
8	存储服务器	macrosanms 3000		1 台	Ms3000	
9	负载均衡	天融信负载 均衡		1 台	天融信负载 均衡 V3	2019 项目
10	磁盘阵列	宏杉		1 台	MS3000G2	
11	磁盘阵列	科达		4 台	VS200C-4	
12	备份系统一体机	鼎甲		1 台	鼎甲	2019 项目
13	光盘库	北丞		1 台	蓝光	
三、网络设备						
1	交换机	思科		30 台	WS-S2960	
2	核心交换机	思科		4 台	SISCO4507R+ E	

3	广域网交换机	思科		6 台	WS-S2918	
4	交换机	H3C		6 台	S51110V4-SI (3 台) S5130 (2 台) S1224R (1 台)	
5	交换机	华为		8 台	S2326TP (5 台) S2309TP (3 台)	
6	核心交换机	华为		2 台	s9303 (1 台) S5720 (1 台)	
7	广域网交换机	华为		2 台	S9706, 含原 厂维保	含原厂 维保
8	广域网路由器	思科		2 台	ASR1004	
四、安全设备						
1	防火墙	天融信		1 台	TopSEC-CARD -4S4A-n	
2	防火墙	华为		2 台	USG6650E-AC	
3	广域网防火墙	华为		1 台	S2700(财 政 专网)	
4	入侵防御	网神		2 台	P9000-TG63M	
5	广域网入侵防御	网神		1 台	P5000-TG13P (执行单兵)	
6	防毒墙	网神		2 台	NSG7000-TX2 5	
五、终端设备						
1	摄像机	sony		4 个	Pxw z150 (1 台) Hvr-s270c (1 台) FDR-AX30 (1 台) MODELEVI-HD 1 (1 台)	
2	摄像机	海康威视		216 个	DS-2CD2GYWD A (98 个)	

					DA-2CD272GY WDA (109 个) IDS-2DF82GY MH (9 个)	
3	监控摄像头	科达		57 个	IPC112E-P (57 台)	
4	拾音器	国产		21 台		安防监控系统
5	报警设备	海康威视		1 台	ivms-A200	
6	门禁一体机	海康威视		80 台	DS-K5604A-3 XF (10 台) DS-K1T671TM F (3 台) DS-K1T6ZXZT MF (41 台) DS-K5604LCF (18 台) DS-K1T607M (8 台)	
7	人证核验终端	海康威视		1 台	MD2012	
8	人脸识别闸机	华宇		4 台	IFB-A4-10-N	
9	电子锁	国产		11 把	JDY-002	门禁系统
10	取号机	金雀		1 台	KLS-P430DR	
11	高清视讯互联主机	华宇		1 台	EDS-500N	
12	实体云柜	炫盈		9 台	ccp-zg201 (2 台) ccp-fg201 (7 台)	
13	监控摄像头	炫盈		4 个	WZM-JK100	
14	二维码扫描枪	炫盈		5 个	WZM-SB100	
15	大屏控制电脑	联想		1 台	M4000S	
16	大屏配电系统	海康威视		2 套	定制	

17	窗口显示条屏	金雀		2 套	定制	
18	音视频呼叫器	金雀		11 套	JQ-CTL-1	
19	触摸评价器	金雀		11 台	JA100-PV0	
20	无线麦克风	ITC		9 台	T-5Z10H (2 个) 鹅颈无线麦 TL-W102A (7 个)	
21	6 路调音台	ITC		1 台	TS-6P	
22	音频处理器	ITC		1 台	TS-108R	
23	吸顶音箱	ITC		16 台	TS-108R	
24	功放	SONDANA		7 台	X-600II (2 台) X-400II (2 台) X-800II (2 台) X-1500II (1 台)	
25	功放	ITC		4 台	TS-200PI	
26	SDI 分配器	视麦特		1 台	SDI-14	
27	HDMI 分配器	视麦特		1 台	HS-2314FS	
28	大屏显示器	海信	55 英寸 LED 超高清 4K 无边框液晶电视, HDMI 输入	3 台	HZ55E5A	
29	音频采集主机	华宇		1 套	VAS-800	
30	电容话筒	华宇		1 台	CDST-005	
31	智能混音器	ITC		1 台	TS-P880	
32	数字音频处理器	ITC		1 台	TS-0812	
33	专业功放	ITC		1 台	TS-200PL	
34	扩声音箱	ITC		2 台	TS-605H	
35	时序电源控制器	华宇		1 台	TPS-1008-1	

36	功率放大器	PSS		2 台	DX5.2	
37	4*两分频同轴天花扬声器	PSS		8 个	QT-809	
38	数字音频处理器	PSS		1 台	PA260P	
39	中央控主机	CREATOR		1 台	CR-PGM	
40	无线接收器	CREATOR		1 个	CRRFA	
41	8 路电源控制器	CREATOR		1 台	ITC-TS-820	
42	主会场终端	华为		1 套	HUAWEI TE50	
43	全数字会议系统主机	CREATOR		1 套	CR-DIG5201-A	
44	会议系统连接盒	CREATOR		5 台	CR-DIG52032 2BOX	
45	会议延长线	CREATOR		2 条		
46	北京威泰二套设备	威泰视信		1 台	VEXTRA960-S	
47	一体化支架	定制		10.1 平方米		
48	大屏控制器	海康威视		1 台	DS-D40C04	
49	视频综合平台	海康威视		1 台	DS-B20-08V-16HU	
50	大屏专用线缆	定制		1 套		
51	VGA 分配器	海康威视		2 个	DS-C50V0102 P	
52	84 寸信息发布屏	海康		1 套	DS-D5084TL/ P	
53	84 寸信息发布屏支架	定制		1 套		
54	升降器	定制		11 个		
55	全省会议终端	华为		1 台	Hauwei TE50	
56	采集盒	itc		29 个	TV-711H4K	
57	4k 输出盒	itc		9 个	TV-712AK	
58	LED 控制卡	海康		6 台	DS-D40C04-H	
59	多屏控制器	海康		1 台	DS-C10S	

60	大屏控制输入板	海康		2 块	DS-C10S-DI4 T	
61	大屏控制输出板	海康		1 块	DS-C10S-DI4 T	
62	华为摄像头	华为		1 台	Camera 200	
63	执行局机房瘦客 户机	联想		11 台	L1913PA	
64	执行局机房 19 寸 方形液晶显示器	联想		11 台	LT913PA	
65	执行局机房大屏 控制电脑（含叶晶 晶显示器）	联想		1 台	M8500T-N000	
66	执行局机房灯光 控制平板	iPhone		1 个	A1489	
67	主二楼会议室控 制台台式电脑	联想		1 台	M425	
68	诉服大厅扫描中 心打印机	理光		1 台	MP6055SP	
69	诉服大大厅律师 工作室打印机	理光		1 台	HPM132A	
70	书写台一体机	联想		8 台	AI052523 IKV	
71	3D 导航一体机	华宇		1 台	ALM-400-F-B I	
72	虚拟导诉一体机	华宇		1 台	ALM-400-F-B I	
73	智能服务机器人	定制		1 台	TH-M4H5	
74	投影机	NEC		1 台	P525UL	
75	移动投影幕	美视		1 套	DI-MI100W	
76	投影仪电动吊架	美视		1 台	PR2215-A	
77	高性能底图机	定制		1 台	M4000S	
78	智能高拍仪	良田		2 台	S520R	
79	书记员桌面电脑	联想		1 台	MOB-WAH9P	
80	法官桌面电脑	联想		1 台	NOB-WAH9P	
81	打印机	联想		1 台	HP M254DW	
82	19 寸安卓一体机 及媒体显示端软	博衍思创		13 台	SC-19-X&Med iaScape-Cli	

	件				ent	
83	窗口电脑	联想		25 台	M4000s	
84	窗口业务人员显示器	LG		25 台	Z9WK600	
85	打印机	惠普		17 台	M132A	
86	一楼立案大厅扫描仪	方正		1 台	Z30D	
87	二代身份证读卡器	华旭金卡		17 台	HX-FOX5	
88	自助诉讼工作台	华宇		2 套	ALM-400-M-A 3	
89	法官留言一体机	华宇		1 套	ALM-400-F-A 6	
90	高清 MCU 平台	华为		1 台	含原厂维保 HUAWEI VP9650	含原厂 维保
91	全彩 LED 屏	ITC	55.479 平方米	4 块	C1.579	含原厂 维保
92	LED 显示屏	海康威视	35.04 平方米	4 块	P1.5 全彩	含原厂 维保
93	电视显示器	海尔		2 台	LS65AL88A81	
94	电视显示器	海信		4 台	LED55K310X3 D	
95	摄像机	华为		2 个	CAMERA 200	
96	会议终端	华为		1 台	Box 600	
97	视联网终端	视联动力		1 台	VT-AUROR3	
98	4K 输出盒	ITC		16 台	TV-712A (6 台) TV-712A4K (10 台)	
99	多画面处理器	威泰视信		1 台	MVP400	
100	视频会议终端	威泰		1 台	VEXTRA 980	
101	拼接中控	ITC		1 台	GY-715	
102	反馈抑制器	ITC		1 台	TL-224	
103	反馈抑制器	Advanced Feedback		1 台	AFS224	

104	时序电源	SONDANA		1 台	HT-808	
105	会议系统主机	ITC		1 台	TL-W100	
106	电源控制器	ITC		1 台	GY-9101	
107	LED 控制卡	海康		6 张	DS-D40C04-H	
108	会议终端电脑	联想		2 台	M425	
109	调音台	雅马哈		1 台	MG166C	
110	华为平板	华为		1 台	MRX-W29	
111	控制台台式电脑	联想		1 台	M415-D075	
112	笔记本电脑	联想		1 台	K42-80	
113	会议触控屏	华为		1 台	Huawei touch	
114	会议电视终端	华为		1 台	Box 600	
115	视联网高清视频会议系统	统一视频		1 台	A2-32-CC-BR	
116	会议主机	纬志 ITAV		1 台	ITAVNT 8000	
117	音频处理中心	UAP		1 台	E341234 4BS6	
118	返听均衡器	SONDANA		1 台	EQ1231	
119	电源时序器	SONDANA		1 台	AC-2216	
120	无线会议主机	ITC		1 台	TS-W100	
121	分布式平台	ITC		2 台	GY-713A	
122	控制器	ITC		3 台	TS-9101	
123	拼接中控	ITC		1 台	TV-715	
124	调音台	ITC		1 台	TS-24PFX-4	
125	西大门大屏电脑	联想		1 台	510S-071MB	
126	机柜	金盾		1 台	42U	
127	分屏器	绿联		7 台	40201	
128	发送卡	ITC		11 张	TV-81S6F	

129	电视机	海信		5 台	LED55K310X3 D	三楼会 议室
130	摄像机	SONY		1 台	PXW-X280	

备注：运维保障设备包含但不限于以上设备清单的内容。

海南省高级人民法院2023年至2024年信息化基础设施和网络安全运维服务项目（B包）-信息系统网络安全等级保护测评

一、服务期限：合同签订之日起2年，每年1次（每年度合同签订生效后5个月内，完成等级保护测评对象网络安全等级保护测评工作，并出具网络安全等级保护等级测评报告）。

二、服务地点：用户指定地点。

三、交付方式：提供相应等保测评服务并出具相关报告。

四、采购资金的支付方式、时间、条件：服务费按年支付，每年度服务费用分两笔支付。

1. 签订合同之日起30个工作日内，支付年度服务费用的70%作为首付款。

2. 每年度进行一次信息系统等级保护测评服务验收，验收通过后支付该年度服务费用的30%作为尾款。

五、申请人的资格要求：见招标公告。

六、验收要求：

1. 按标书服务要求和国家行业标准进行验收。

2. 验收标准：每年度按系统提交《网络安全等级保护等级测评报告》（第一年提供7个三级测评报告和1个二级测评报告，第二年提供7个三级测评报告）。

七、本次采购标的对应中小企业划分标准所属行业为软件和信息技术服务业。

八、服务要求：

（一）项目服务背景

为了进一步贯彻落实国家网络安全等级保护制度，推进海南省高级人民法院的网络安全等级保护工作，提高海南省高级人民法院等级保护对象的安全保障能力和防护水平，更好地提升海南省高级人民法院网络安全管理的整体水平，根据《中华人民共和国网络安全法》、《中共中央国务院关于支持海南全面深化改革开放的指导意见》、《信息安全等级保护管理办法》（公通字〔2007〕43号）、《海南省政务信息化项目建设管理实施细则（暂行）》（琼数组办〔2022〕5号）和《海南省进一步贯彻落实网络安全等级保护制度实施方案》的通知（琼公通〔2022〕14号）等相关规定和要求，采购人将委托具有公安部第三研究所颁发的网络安全等级测评与检测评估机构服务认证证书的供应商，开展海南省高级人民法院2023年至2024年信息系统网络安全等级保护测评，以全面提高网络安全保障能力和水平，为切实做好等级保护对象的网络安全等级保护的各项工作夯实基础，等级测评结束后，出具《网络安全等级保护等级测评报告》，并针对等级保护对象安全建设提出具有针对性的整改建议。

（二）项目服务范围

本项目B包采购预算（最高限价）为：117万元人民币，报价不得超过采购预算（最高限价），否则视为无效投标。每年度采购预算详见表《项目采购预算表》。

投标人除提供本项目B包总体报价外，还需按年分别提供每年度的等保测评服务报价（每年度报价不得超过每年度采购预算，否则视为无效投标）。

项目采购预算表

2023年费用 (万元)	2024年费用 (万元)	总费用 (万元)	服务期限	备注
61	56	117	2年	

本次项目所涉及的等级保护对象服务范围如下：

2023 年度等级保护测评服务范围

服务内容	系统名称及级别		服务期限	备注
2023 年度 信息系统 等保测评	海南法院智慧审判系统	三级 (S3A3G3)	2023 年等保 测评 1 年 1 次	
	海南法院智慧诉讼服务系统	三级 (S3A3G3)		
	海南法院智慧执行系统	三级 (S3A3G3)		
	海南省高级人民法院信息基础设施支撑系统	三级 (S3A3G3)		
	海南法院智慧管理系统	三级 (S3A3G3)		
	海南法院门户网站群	三级 (S3A3G3)		
	海南省高级人民法院安全和运维保障系统	三级 (S3A3G3)		
	海南省高级人民法院综合辅助系统	二级 (S2A2G2)	2023 年至 2024 年等保 测评 2 年 1 次	

2024 年度等级保护测评服务范围

服务内容	系统名称及级别		服务期限	备注
2024 年度 信息系统等 保测评	海南法院智慧审判系统	三级 (S3A3G3)	2024 年等 保测评 1 年 1 次	
	海南法院智慧诉讼服务系统	三级 (S3A3G3)		
	海南法院智慧执行系统	三级 (S3A3G3)		
	海南省高级人民法院信息基础设施支撑系统	三级 (S3A3G3)		
	海南法院智慧管理系统	三级 (S3A3G3)		
	海南法院门户网站群	三级 (S3A3G3)		
	海南省高级人民法院安全和运维保障系统	三级 (S3A3G3)		

(三) 项目服务内容及技术要求

1、等保咨询服务

1.1 等级保护政策/标准咨询

随着国家信息安全等级保护的推进工作，信息安全等级保护政策、法律法规和标准体系也会相应的发布和更新，供应商应针对本项目设立信息安全等级保护咨询平台，明确较为固定的咨询服务人员，并根据咨询要求提供正式的答复资料

和文档。咨询内容包括但不限于信息安全等级保护国内外发展动态、等级保护政策、法律法规和标准体系咨询服务。

1.2 信息系统等级变更咨询

在信息系统出现等级变更时，供应商须协助采购单位对信息系统进行分析，明确信息系统边界和定级对象，对信息系统的子系统进行划分，确定信息系统以及子系统的安全等级。

1.3 等级保护建设指导

按照信息系统安全总体方案，供应商须结合信息系统安全现状及规划，根据信息安全等级保护相关标准和规定，对采购单位等级保护建设工作提供全面的安全方案设计咨询，协助采购单位落实安全技术与管理措施，并根据预期实现的安全目标，全程指导信息系统的测评、验收工作，满足等保测评要求。

1.4 等级保护整改及复核验证服务

根据信息系统测评报告要求，供应商须结合采购单位信息系统安全现状及规划，提供可落地的整改建议方案和实施计划，整改建议方案应明确设计依据、整改内容、整改建议等，基于系统现状指导采购单位开展信息系统测评整改工作，并在采购单位完成整改后提供整改复核服务，验证整改情况是否满足相关测评规范和主管单位文件要求。

1.5 信息系统安全检查咨询

在采购单位开展信息系统安全检查时，供应商全程提供现场咨询服务，包括检查范围、检查方法、检查结果分析以及整改措施制定等。

2、网络安全等级保护测评服务

供应商应依据国家网络安全等级保护管理规定，按照《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术网络安全等级保护测评过程指南》(GB/T28449-2018)有关管理规范和技术标准，在海南省高级人民

法院各分散的业务信息系统整合完成的基础上，2023-2024 年每年度对整合后的各业务信息系统进行网络安全等级保护测评，测评工作完成后，针对各业务信息系统测评的情况，出具《网络安全等级保护等级测评报告》，并针对各业务信息系统安全建设提出具有针对性的整改建议。

2.1 测评实施内容

供应商应针对等级保护对象完成等级保护对象要素进行确认、分析和梳理，提出详细的等级测评方案。对等级保护对象的整体保护状况和等级保护对象组件，逐一进行网络安全等级保护等级测评，等级测评的内容包括以下内容：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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理十个层面的安全测评；完成测评工作后，出具《网络安全等级保护等级测评报告》，并针对等级保护对象安全建设提出具有针对性的整改建议。

2.2 测评实施过程

供应商在测评过程中，按照《信息安全技术 网络安全等级保护测评过程指南》等标准开展测评实施工作，等级测评过程分为四个基本测评活动：测评准备活动、方案编制活动、现场测评活动、报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

2.2.1 测评准备活动

测评准备活动的目标是顺利启动测评项目，收集定级对象相关资料，准备测评所需资料，为编制测评方案打下良好的基础。

测评准备工作应包括工作启动、信息收集和分析、工具和表单准备。

详细要求见下表：

项目内容	工作内容	成果输出
项目启动	1. 组建测评项目组	向用户提交《项目计划书》 《提供资料清单》
	2. 编制《项目计划书》	

	3. 确定测评委托单位应提供的资料	
信息收集 分析	1. 整理调查表单	《等级保护对象调查表》
	2. 发放调查表单给测评委托单位	
	3. 协助测评委托单位填写调查表	
	4. 收回调查结果	
	5. 分析调查结查	
工具和表 单准备	1. 调试测评工具	确定测评工具(测评工具清单)《现场测评授权书》打印各类表单:风险告知书、文档交接单、会议记录表单、会议签到表单
	2. 模拟被测定级对象架构,熟悉被测定级对象	
	3. 准备和打印各类表单	

2.2.2 方案编制活动

方案编制活动的目标是整理测评准备活动中获取的定级对象相关资料,为现场测评活动提供最基本的文档和指导方案。

方案编制活动应包括测评对象确定、测评指标确定、测评内容确定、工具测试方法确定、测评指导书开发及测评方案编制等六项主要任务。

详细要求见下表:

工作内容	工作详细任务	输出成果
一、测评对象确认	分析并确定被测定级对象 识别并描述被测定级对象的整体结构 识别并描述被测定级对象的边界 识别并描述被测定级对象的网络区域 识别并描述被测定级对象的主要设备 确定测评对象 描述测评对象	《测评方案》的测评对象部分
二、测评指标确定	确定被测定级对象业务信息和系统服务安全保护等级	《测评方案》的测评指标部分
	根据被测定级对象的 A 类、S 类及 G 类基本安全要求的组合情况,从 GB/T22239、行业规范中选择相应等级的基本安全要求作为基本测评指标	
	根据测评委托单位及被测定级对象业务自身需求,确定特殊测评指标。	
	根据测评委托单位及被测定级对象业务自身	

	需求, 确定特殊测评指标。	
	对确定基本测评指标和特殊测评指标进行描述, 并分析给出指标不适用的原因	
三、测评内容确定	确定每个测评对象对应的每个测评指标的测评方法	《测评方案》的 单项测评实施 部分
	确定实施测评的单项测评内容	
四、工具测试点确定	<p>确定工具测试环境 确定工具测试工具 确定工具测试的测评对象 选择测试路径 确定测试工具的接入点 本次项目测评需要使用到如下工具: 漏洞扫描工具; Windows 主机安全配置检查工具; Linux 主机配置检查工具; 网络及安全设备配置检查工具; 病毒检查工具; 木马检查工具; 网站恶意代码检查工具; 在线检查工具(网站安全检查工具); 终端安全检查工具; 口令破解工具; 渗透测试工具; SQL 注入验证检查工具; 在线数据库安全检查工具。</p>	《测评方案》的 的工具测试方 法及内容部分
五、测评指导书开发	确定单个测评对象, 内容包含测评对象的名称、位置信息、用途、管理人员等信息	测评指导书、测 评结果记录表 格
	确定单项测评实施活动, 包括测评项、测评方法、操作步骤和预期结果等四部分	
	确定单项测评、整体测评表述形式	
	根据测评指导书, 形成测评结果记录表格	
六、测评方案编制	明确项目整体情况和测评活动依据	向用户提交经 过评审和确认 的《测评方案》、 《风险规避实 施方案》
	根据测评协议书和被测定级对象情况, 估算现场测 评工作量	
	根据测评项目组成员安排, 编制工作安排情况	
	根据以往测评经验以及被测定级对象规模, 编制具体测评计划, 包括现场工作人员的分工和 时间安排	
	汇总上述内容及方案编制活动的其他任务获 取的	
	内容形成测评方案文稿	
	评审和提交测评方案	
	根据测评方案制定风险规避实施方案	

2.2.3 现场测评活动

现场测评活动通过与测评委托单位进行沟通和协调,为现场测评的顺利开展打下良好基础,依据测评方案实施现场测评工作,将测评方案和测评方法等内容具体落实到现场测评活动中。现场测评工作主要取得报告编制活动所需的、足够的证据和资料。

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

详细要求见下表:

工作内容	工作详细任务	输出
1. 现场测评准备	测评委托单位对风险告知书签字确认	会议记录,风险告知书,测评方案和现场测评工作计划,现场测评授权书
	测评委托单位协助测评机构签署现场测评授权书	
	召开现场测评首次会	
	双方确认测评计划和测评方案	
	双方确认配合人员、测评环境等各种现场测评需要的资源	
2. 现场测评和结果记录	确认测评对象的关键数据已经进行了备份	《各类测评结果记录/测评证据和证据源记录/文档交接/规划记录单》 访谈结果: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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理安全测评的测评结果记录或录音;
	确认具备测评工作开展的条件,测评对象工作正常,系统处于一个相对良好的状况	
	根据测评指导书实施现场测评,获取相关证据和信息	
	测评结束后,双方确认测评工作是否对测评对象造成不良影响,测评对象及系统是否工作正常	
3. 结果确认和资料归还	汇总测评记录,对漏掉和需要进一步验证的内容实施补充测评	文档审查结果:安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评的测评结果记录;

	<p>召开现场测评结束会，测评双方对测评过程中得到的证据源记录进行确认</p>	<p>配置核查结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录表格</p> <p>工具测试结果:安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心测评结果记录,工具测试完成后的电子输出记录,备份的测试结果文件</p>
	<p>测评人员归还借阅的所有文档资料,并由测评委托单位文档资料提供者签字确认</p>	<p>实地察看结果: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、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理测评结果记录</p> <p>测评结果确认:现场核查中发现的问题汇总、测评证据和证据源记录、测评委托单位的书面认可文件</p>

2.2.4 报告编制活动

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

测评人员在初步判定单项测评结果后,还需进行单元测评结果判定、整体测评、系统安全保障评估,经过整体测评后,有的单项测评结果可能会有所变化,需进一步修订单项测评结果,而后针对安全问题进行风险评估,形成等级测评结论。报告编制活动应包括单项测评结果判定、单元测评结果判定、整体测评、系统安全保障评估、安全问题风险分析、等级测评结论形成及测评报告编制七项主要任务。

详细要求见下表:

工作内容	工作详细任务	工作依据(模版)
1. 单项测评结果判定	分析测评项所对抗威胁的存在情况	测评报告的等级测评结果记录部分
	分析单项测评项的测评证据,并与要	

	求内容的预期测评结果相比较, 给出 单项测评 结果和符合程度得分	
	综合判定单项测评项的测评结果	
2. 单元测评 结果判定	汇总不同测评对象对应测评指标的单项 测评结果情况	测评报告的单元测评 小结部分
	判定每个测评对象的单元测评结果	
3. 整体测评	分析不符合和部分符合的测评项与其他 测评项(包括安全控制点、安全控制 点间、区域间)之间的关联关系及对结 果的影响情况	测评报告的整体测评 部分
	根据整体测评分析情况, 修正单项测 评结果符合程度得分和问题严重程度 值	
4. 系统安全 保障评估	根据整体测评结果, 计算修正后的每个 测评对象的单项测评结果和符合程 度得分	测评报告的系统安全 保障评估部分
	根据各对象的单项符合程度得分, 计 算安全控制点得分	
	根据安全控制点得分, 计算安全层面 得分	
	根据安全控制点得分和安全层面得 分, 总体评价被测定级对象已采取的 有效保护措施和存在的主要安全问题 情况	
5. 安全问题 风险分析	针对整体测评后的单项测评结果中部分 符合项或不符合项所产生的安全问 题, 结合关联测评 对象和威胁, 分析 可能对定级对象、单位、社会及国家 造成的安全危害	测评报告的安全问题 风险分析部分
	结合安全问题所影响业务的重要程 度、 相关系统组件的重要程度、安全 问题严重程度以及安全事件影响范围 等综合分析可能造成的安全危害中的 最大安全危 害(损失)结果	
	根据最大安全危害严重程度进一步确 定定级对象面临的风险等级, 结果为 “高” “中” 或 “低”	
6. 等级测评 结论形成	统计再次汇总后的单项测评结果为部 分符合和不符合项的项数	等级测评报告的等级 测评结论部分
	计算定级对象综合得分, 形成等级测 评结论, 形成等级测评结论	
7. 测评报告 编制	概述测评项目情况, 整理前面几项任 务的输出/产品	经过评审和确认的被 测定级对象等级测评 报告
	针对被测定级对象存在的安全隐患,	

	提出处置建议	
	根据测评协议书、测评委托单位提交的相关文档、测评原始记录和其他辅助信息,对测评报告进行评审	
	评审通过后,由项目负责人签字确认并提交给测评委托单位	

2.2.5 测评实施活动文档

测评机构在上述各阶段活动的测评实施服务过程中,根据服务规范和采购人要求,提供系统、完整、清晰的服务日常报告。

提供的服务文档应至少但不限于如下文档:

测评准备活动阶段:

- 《项目计划书》;
- 《等级保护对象调查表》;
- 《会议记录表》;

方案编制活动阶段:

- 《网络安全等级保护测评方案》;
- 《测评指导书》;
- 《风险规避实施方案》;

现场测评活动阶段:

- 《现场测评授权书》;
- 《文档交接单》;
- 《会议记录》;

报告编制活动阶段:

按信息系统提交《网络安全等级保护等级测评报告》,并针对该信息系统提出安全整改建议。

(四) 项目服务要求

1、工作要求

供应商须给出采购单位在进行调查和评估时所需要提供的信息列表,并经采购单位确认。采购单位有权利不提供信息列表以外的任何信息。

安全评估必须按照分层的原则，包括但不限于以下对象：物理环境、网络结构、网络服务、主机系统、数据、应用系统、安全系统、安全相关人员、处理流程、安全管理制度、安全策略等。

供应商应详细描述安全调查和评估的组织方式，包括组成的人员及分工、评估的过程组织、实施时间安排、评估方式所遵循的标准等。供应商需要描述调查和评估过程的步骤，每一步骤的具体内容、时间安排、详细实施过程、可能对网络及主机造成的影响等等。

安全调查和评估的过程中，供应商如需采购单位配合，供应商需要详细描述需要配合的内容。如需要采购单位协助完成各种表单，需要详细描述表单的名称、功能及主要表项等等，并由供应商给出具体示例。采购单位有权利拒绝提供任何未事先提出的配合要求，由此产生的损失由供应商负完全责任。

安全调查和评估过程中，如需使用安全工具，请详细描述所使用的安全工具（软硬件型号、功能和性能描述）、使用的方式和时间、对环境和平台的要求等。

供应商应向采购单位提供详细的评估的原始材料、各种表单及结果报告。

供应商需要详细描述本次评估采用的评估方式及标准。

2、项目组人员要求

2.1 供应商须根据项目特点和实际情况，提出项目团队配置方案，包括团队成员、组织架构和分组分工等，满足项目实施建设的需要。

2.2 **驻场服务要求：**合同签订后，每年度开展信息系统网络安全等级保护测评工作期间，必须选派具有相关资历的人员到本地（海南省高级人民法院）驻场开展服务直至所有成果报告编写完成。本地驻点人员还需现场提供等级保护政策/标准咨询、等级保护建设整改指导、整改情况复核验证、信息系统安全检查咨询、网络系统安全方案设计等服务。实际提供的项目团队必须与投标提供的团队名单材料一致，如不符将视为虚假应标。若采购单位认为项目负责人或者技术人员能力与工作所要求的能力不相称而提出更换时，测评机构必须予以更换，人员更换不得影响测评成果交付时间；供应商单方面更换项目负责人或技术员（工程师）必须经采购单位书面同意，否则按违约处理直至合同中止。

2.3 按照公安部对测评机构管理的规定和要求，测评项目现场实施的人员必须是本机构的持证测评师，而且测评项目不允许分包或转包，中标人一旦出现上

述违规情况采购人有权解除合同。

2.4 项目团队实施中提供 7×8 小时现场咨询服务。项目验收后提供 1 年的跟踪咨询服务，自项目验收通过之日起计算。在采购单位提出服务请求时，项目团队应在 30 分钟内响应，如紧急或特殊情况需要 2 小时内到达采购人现场，在 24 个小时内提供解决方案。

3、数据安全及应急响应处置要求

供应商在开展信息系统网络安全等级保护测评前，必须向采购单位提供信息系统数据备份建议，指导采购单位或第三方完成信息系统数据备份，并在项目实施过程中自觉遵守国家有关信息安全的法律法规、行政规定、方针政策等规定，严格按照国家相关标准和规范开展测评工作，对开展工作过程中所获悉采购单位的数据信息，应实施有效保护和管理，加强数据安全使用管控，避免造成信息泄露。

当信息系统发生紧急安全事件等突发情况时，提供现场的应急响应服务，协助采购单位和第三方对突发情况进行应急处置，协助和指导采购单位和第三方解决安全故障、修复系统，最大限度的保护服务器和数据安全，最快的速度恢复访问和网络畅通，使信息系统恢复正常工作，尽可能挽回或减少损失。

4、安全保密要求

要求供应商制定等保测评服务安全保密制度，确定项目保密责任人，同时要求供应商：

4.1 按照国家和海南省有关保密规定，与采购单位签订保密协议，参与测评或评估的工作人员签订保密承诺函；

4.2 严格履行保密职责，按照保密规定开展等保测评工作。