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（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》

	2.编制《项目计划书》	《提供资料清单》
	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	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。	《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 ; 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;
	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	

	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	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 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 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 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
	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	

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。