合同号:HKHSFY2025-7-3

海口海事法院信息化基础设施建设项目
网络安全等级保护测评服务合同

甲方：海口海事法院

乙方：海南正邦信息科技有限公司

签订日期：2025年 7月 8日

甲方:海口海事法院

乙方:海南正邦信息科技有限公司

甲乙双方根据 2025 年 6 月 16 日 海口海事法院信息化基础设施建设项目 （项目编号：HZ2025-154）竞争性磋商结果及磋商文件的要求，经协商一致,按照《中华人民共和国政府采购法》、《中华人民共和国民法典》规定，经双方协商,本着平等互利和诚实信用的原则，一致同意签订本合同。

一、合同标的及金额等

序号	项目名称及包号	金额（元）	合同履行期限
1	海口海事法院信息化基础设施建设项目、采购包 3	79,200.00	合同签订生效且达到进场条件后 60 个工作日内完成网络安全等级保护等级测评服务、整改指导服务，并按要求出具相关服务成果及报告。
	合　计	￥79,200.00 元 （包含税费等乙方完成服务所需所有费用，除另有约定，甲方无需向乙方另行支付其他任何费用。）	
项目地点：采购人指定地点 **投标报价总计：￥79,200.00 元** **人民币（大写）人民币柒万玖仟贰佰元整**			

二、服务期

合同签订生效且达到进场条件后60个工作日内完成网络安全等级保护等级测评服务、整改指导服务，并按要求出具相关服务成果及报告。

三、项目服务内容

通过委托专业信息安全等级测评服务机构，根据网络安全等级保护2.0标准等相关文件及标准要求，针对甲方单位系统状态为新建的核心网络实施网络安全等级保护测评，明细如下：

序号	信息系统/服务项目		级别
1	核心网络（以最终采购人确认名称为准） 测评		三级
2	整改指导	测评前中后各时间段，按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，向用户进行报告解读，并将技术措施和管理措施有机结合，建立信息系统综合防护体系，提供整改方案，指导用户进行整改，以达到提高信息系统整体安全保护能力。	
3	测评实施过程及结果输出	实施过程：依据《网络安全等级保护基本要求 GB/T22239-2019》和《网络安全等级保护测评要求 GB/T28448-2019》等相关文件及标准要求，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、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、安全运维管理等十个方面，按	

		照网络安全保护等级的基本要求进行测评。 结果输出:《网络安全等级保护测评报告》及提出具有针对性的整改方案。

（一）服务实施

1、服务目标

通过网络安全等级保护测评服务，对甲方单位系统状态为新建的核心网络开展符合性测评，衡量信息系统的安全保护管理措施和技术防护措施是否符合等级保护基本要求，是否具备了相应的安全保护能力。找出问题，针对性的制定整改措施，推进信息安全防护体系不断完善。

2、测评依据

项目主要依据但不限于以下相关的法规政策、标准及规范：

- 《中华人民共和国网络安全法》（第十二届全国人大常委会2016年11月7日通过，自2017年6月1日起施行。）
- 《海南省信息化管理条例》（海南省第五届人大常委会2013年9月25日通过，自2013年11月1日起施行。）
- 《计算机信息系统安全保护等级划分准则》（GB 17859-1999）
- 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
- 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
- 《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/T 28449-2018）
- 《信息技术 安全技术 信息技术安全评估准则》（GB/T 18336.2-2015）
- 《信息安全技术 信息安全风险评估规范》(GB/T 20984-2007)
- 《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）
- 《信息安全技术 信息安全风险管理指南》(GB/Z 24364-2009)
- ……

（二）服务内容

服务期内，乙方须向甲方提供以下服务。

1、等级保护测评服务

依据网络安全等级保护2.0标准等相关文件及标准要求，对甲方各信息系统的安全技术体系和安全管理体系等进行合规性检查，出具《网络安全等级保护测评报告》，并提出具有针对性的整改建议。

1）测评内容

（1）对甲方单位已备案信息系统进行摸底、分析和梳理，提出详细的等保测评方案。

（2）逐一对信息系统进行安全等级保护测评，测评的内容包括但不限于以下内容：

① 安全技术测评：包括安全物理环境、安全通信网络、安全区域边界、 安全计算环境、安全管理中心五个方面的安全测评；

② 安全管理测评：安全管理机构、安全管理制度、安全管理人员、安全建设管理和安全运维管理五个方面的安全测评。

（3）完成测评工作后，提出整改建议；最后出具符合公安部门要求的信息系统安全保护等级测评报告，并在后期整改实施过程中提供全程咨询服务。

2）测评实施

测评项目过程需按照《网络安全等级保护测评过程指南》开展工作，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、分析及报告编制活动。测评双方之间的沟通与洽谈应贯穿整个等级测评过程。

（1）测评准备活动

测评准备工作包括编制项目启动、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.确定招标人应提供的资料	
信息收集分析	定级报告及整改方案分析	《系统基本情况分析报告》
	1.整理调查表单	
	2.发放调查表单给甲方	
	3.协助甲方填写调查表	
	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》《测评结果记录表》《文档交接单》
	2.模拟被测系统搭建测评环境	
	3.模拟测评	
	4.准备打印表单	

（2）方案编制活动

方案编制活动包括测评对象确定、测评指标确定、测试工具接入点确定、测评内容确定、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	识别被测系统等级 识别被测系统的整体结构 识别被测系统的边界 识别被测系统的网络区域 识别被测系统的重要节点和业务应用 确定测评对象	《测评方案》的测评对象部分
二、测评指标确定	识别被测系统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
	选择对应等级的ASG三类安全要求作为测评指标	
	就高原则调整多个定级对象共用的某些物理安全或管理安全测评指标	
三、工具测试点确定	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	《测评方案》的测试工具接入点部分
四、测试内容确定	识别每个测评对象对象的测评指标	《测评方案》的单项测评实施和系统测评实施部分
	识别每个测评对象对应的每个测试指标的测试方法	
五、测评指导书开发	从已有的测评指导书中选择与测评对象对应的手册	《测评方案》的测评实施手册部分
	针对没有现成测评指导书的测评对象，开发新的测评指导书	
六、测评方案编制	描述测评项目基本情况和工作依据	向用户提交《测评方案》
	描述被测系统的整体结构、边界和网络区域	
	描述被测系统的重要节点和业务应用	
	描述测评指标	
	描述测评对象	
	描述测评内容和方法	

（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，然后依据测评方案实施现场测评工作，将测评方案和测评工具等具体落实到现场测评活动中。现场测评工作应取得分析与报告编制活动所需的、足够的证据和资料。

现场测评活动包括现场测评准备、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	现场测评授权书签署	会议记录、确认的授权委托书、更新后的测评计划和测评方案
	召开现场测评启动会	
	双方确认测评方案	
	双方确认配合人员、环境等资源	
	确认信息系统已经备份	
	测评方案、结构记录表格等资料更新	
2.现场测评和结构记录	依据测评指导书实施测评	访谈结果：技术安全和管理安全测评的测评结果记录或录音 文档审查结果： 管理安全测评的测评结果记录 配置检查结果：技术安全测评的网络、主机、应用测评结果记录表格 工具测试结果： 技术安全测评的网络、主机、应用测评结果记录，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：技术安全测评的物理安全和管理安全测评结果记录 测评结果确认：现场核查中发现的问题汇总、证据和证据源记录、被测单位的书面认可文件
	记录测评获取的证据、资料等信息	
	汇总测评记录，如果需要，实施补充测评	
3.结果确认和资料归还	召开现场测评结束会	
	测评委托单位确认测评过程中获取的证据和资料的正确性，并签字认可	
	测评人员归还借阅的各种资料	

4）报告分析及编制活动

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元测评结果后，还需进行整体测评，经过整体测评后，有的单元测评结果可能会有所变化，需进一步修订单元测评结果，而后进行风险分析和评价，形成等级测评结论。分析与

报告编制活动包括单项测评结果判定、单元测评结果判定、整体测评、风险分析、等级测评结论形成及测评报告编制六项主要任务。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	等级测评报告的单项测评结果部分
	分析单个测评项是否有多方面的要求内容，依据“优势证据”法选择优势证据，并将优势证据与预期测评结果相比较	
	综合判定单个测评项的测评结果	
2.单元测评结果判定	汇总每个测评对象在每个测评单元的单项测评结果	等级测评报告的单项测评结果汇总分析部分
	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（包括单元内、层面间、区域间）之间的关联关系及对结果的影响情况	等级测评报告的系统整体测评分析部分
	分析被测系统整体结构的安全性对结果的影响情况	
4.风险分析	整体测评后的单项测评结果再次汇总	等级测评报告的风险分析部分
	分析部分符合项或不符合项所产生的安全问题被威胁利用的可能性	
	分析威胁利用安全问题后造成的影响程度	
	为被测系统面临的风险进行赋值	
	评价风险分析结果	
5.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
	形成等级测评结论	
6.测评报告编制	概述测评项目情况	等级测评报告 提交用户
	描述被测系统情况	
	描述测评范围和方法	
	描述整体测评情况	
	汇总测评结果	
	描述风险情况	
	给出等级测评结论和整改建议	

2、整改指导服务

乙方根据测评结果，应针对性的提出整改建议方案。整改建议方案应具有可操作性，符合甲方实际情况，且能够切实解决问题。整改建议方案应明确设计依据、整改内容、整改方案、能够解决的问题、投资概算以及风险评估。在整改实施过程中，乙方全力支持，负责技术把关、整改验收以及其他咨询工作。

3、等级保护咨询服务

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，乙方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。

2）信息系统等级变更咨询

在信息系统出现等级变更时，乙方协助甲方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。

3）等级保护建设整改咨询

按照信息系统安全总体方案要求，乙方结合信息系统安全建设项目计划，根据信息安全等级保护相关标准和规定，对甲方等级保护建设整改工作提供全面的安全方案的详细设计咨询，结合甲方的实际情况，协助甲方进行分布或分期地落实安全技术与管理措施，并根据预期实现的安全目标，全程提供在建安全设备和系统的测试、验收工作等咨询服务。

4）信息系统安全检查咨询

在甲方开展信息系统安全检查时，全程提供咨询服务，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。

5）等级保护测评咨询

测评过程中，乙方协助用户单位参照《网络安全等级保护测评要求》中评估内容和方法，对测评过程中所涉及到的评估项及测评过程中所编制相关表格、填写项提供全程咨询服务，确保测评工作的顺利开展。

（三）验收标准

乙方完成了采购需求的所有服务内容，并提交以下服务成果：

- 《网络安全等级保护测评报告》；
- 《网络安全整改建议方案》；
- 提供测评过程相关文件，包括调研表、技术测评记录、会议纪要等。

（四）项目工期（服务时间）

合同签订生效且达到进场条件后60个工作日内完成网络安全等级保护等级测评服务、整改指导服务，并按要求出具相关服务成果及报告。

服务地点：采购人指定地点。

（五）售后服务及其它要求

乙方提供详细的技术支持和服务方案，技术支持和服务方案包括（但不限于）：

（1）如在测评中出现不符合项，乙方提供相应的整改建议及相关方案。对于测评中发现的主机和网络设备漏洞，乙方提供项目验收后一年的跟踪服务，对本次评估范围内的问题提供远程技术咨询，对

于漏洞的修补、问题的排除给出建议和指导，自项目验收通过之日起计算。

（2）提供及时有效的售后服务，乙方在本地有服务机构，承诺如果中标则在海南省设置有不少2名技术人员的售后服务技术支持团队，并承诺提供的售后保障计划应包含7*24小时的技术支持服务，重大活动期间提供现场的技术支持服务，针对突发应急事件提供4小时内到现场处置的服务响应保障，问题解决后24小时内，提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况。

四、付款方法和条件：

4.1 付款货币：人民币。

4.2 自合同签订生效之日起，甲方收到乙方开具的有效发票后10个工作日内支付合同总价款的50%，即人民币大写：叁万玖仟陆佰元整（￥39,600.00元）。

4.3 完成合同约定的全部服务提交正式报告并通过验收后，甲方收到乙方开具的有效发票后10个工作日内向乙方支付合同未支付款项，即人民币大写：叁万玖仟陆佰元整（￥39,600.00元）。

4.3 乙方指定按以下账户名称、开户银行和账号进行结算和支付：

乙方账户名称：海南正邦信息科技有限公司

乙方开户银行：中国银行海口龙珠支行营业部

账　　号：2662 5619 1890

4.5 由于财政资金拨款不到位而导致甲方逾期付款的，甲方不承担违约责任。

五、成果交付

合同签订生效且达到进场条件后60个工作日内完成网络安全等级保护等级测评服务、整改指导服务，并按要求出具相关服务成果及报告。

交付内容包括（但不限于以下内容）：

- 《网络安全等级保护测评报告》；
- 《网络安全整改建议方案》；
- 提供测评过程相关文件，包括调研表、技术测评记录、会议纪要等。

六、服务验收的标准

乙方完成了采购需求的所有服务内容，并提交以下服务成果：

《网络安全等级保护测评报告》；

《网络安全整改建议方案》；

提供测评过程相关文件，包括调研表、技术测评记录、会议纪要等。

七、双方职责

7.1 甲方职责：

7.1.1 按乙方需要及时提供项目的相关资料。

7.1.2 应指定专门联络人员配合乙方做好项目工作；如乙方提出异议，应及时组织相关各方协调解决出现的问题。

7.1.3 需提供乙方进入甲方设施或设备场地进行安全测试的便利条件。

7.1.4 乙方若到现场提供技术服务，应有人配合工作。

7.2 乙方职责：

7.2.1 按照承诺合理组织安排，做好项目的服务工作，按时完成项目所要求的各项服务内容。

7.2.2 随时跟进项目进展，及时解决项目问题。

7.2.3 优质并按时提交合同要求的各项阶段成果。

7.2.4 按照甲方的要求及时告知甲方项目进度。

八、违约金或者损失赔偿额的计算方法

8.1 若因甲方原因，未能按期支付合同款项，逾期超过 90 日的，乙方有权解除本合同。若乙方解除本合同的，甲方需按合同总价的10%向乙方支付违约金。

8.2 若因乙方原因，未能按期执行合同，逾期超过 90 日的，甲方有权解除本合同。若甲方解除本合同的，乙方应退还甲方已经支付的全部款项，并按合同总价的 10 % 向甲方支付违约金。

8.3 合同非违约方应将索赔金额及事由书面通知违约方，若违约方有异议，应在收到通知10个工作日内以书面形式回复守约方，再由双方协商确定。若违约方收到通知后10个工作日内未予答复守约方，即视为认可通知及其内容。

8.4 除下一条规定的不可抗力外，如果乙方没有按照合同规定的时间交货和提供服务，甲方可从合同款中扣除违约赔偿费，每延迟一个工作日迟交货物（含软件及相关服务）或未提供服务，按合同金额的0.5%计扣违约赔偿费。但违约赔偿费的最高限额为合同金额的15%。如果乙方延迟交货时间超过一个月，甲方有权终止合同，并按合同约定及法律规定追究乙方的违约责任。

8.5 如果双方中任何一方由于战争、严重火灾、水灾、台风和地震以及其它经双方同意属于不可抗力的事故，致使合同履行受阻时，履行合同的期限应予以延长，延长的期限应相当于事故所影响的时间。

九、技术情报和资料的保密

9.1 乙方在履行本合同过程中触及和知晓的甲方的设计方案、设备、网络情况、业务程序及方式、管理的方法制度和专有技术等甲方应用系统的相关资料和信息，无论此种信息的形式和目的为何，均为甲方的保密信息。

9.2 未经甲方书面同意，乙方不得复制、记录或以其他方式泄露上述信息。乙方承诺在合同期内及合同期满后叁年不向任何政府监管部门之外的其他第三方透露上述信息。否则，乙方应按合同总价的 10 %向甲方支付违约金，并赔偿因此给甲方造成的全部损失。

十、不可抗力

10.1 合同订立后双方或一方由于不可抗力而影响合同履行时，则迟延履行合同的时间自动顺延为该合同的履行期限，并可根据实际情况部分或全部免予承担违约责任。但因迟延履行合同后，发生不可抗力的，不能免除责任。

10.2 受不可抗力影响方应在不可抗力事件发生之日起 48 小时内以传真或电子邮件形式告之对方。

10.3 受不可抗力影响方应在不可抗力事件消除后 48 小时内以传真或电子邮件 形式告之对方，如不可抗力事件影响超过三个月以上时，双方应重新协商合同的履行问题，并尽快达成补充协议或重新签订合同。

10.4 因不可抗力事件导致的费用由双方按以下方法分别承担：双方协商解决。

十一、合同纠纷处理

本合同执行过程中发生纠纷，作如下 （2） 处理：

（1）提交海南仲裁委员会按照其仲裁程序和规则进行仲裁。

（2）在甲方所在地人民法院提起诉讼。

十二、合同生效

本合同由甲乙双方签字盖章后生效。

十三、合同鉴证

采购代理机构应当在本合同上签章，以证明本合同条款与磋商文件、响应文件的相关要求相符并且未对招标内容或技术参数进行实质性修改。

十四、组成本合同的文件包括

（一）合同条款；

（二）中标通知书；

（三）服务成果

上述合同文件内容互为补充，如有不明确，由甲方负责解释。

十五、合同备案

本合同一式陆份，中文书写。甲方 叁 份、乙方 贰 份，招标代理机构执 壹 份。

甲方：

单位名称(盖章)：海口海事法院

地　　址：海南省海口市美兰区白龙南路28号

统一社会信用代码：11460000081740056

法定（授权）代表（签字或盖章）：

联系电话：0898-66118106

2025 年 7 月 8 日

乙方：

单位名称(盖章)：海南正邦信息科技有限公司

地　　址：海南省海口市龙华区长堤路23号[illegible]城三层301

统一社会信用代码：91460000742597627A

法定（授权）代表（签字或盖章）：

联系人：李亚女

联系电话：13876461324

2025 年 7 月 8 日

招标代理机构声明：本合同标的经海南海政招标有限公司依法定程序采购，合同主要条款内容与响应文件的内容一致。

招标代理机构：海南海政招标有限公司（盖章）

地　　址：**蓝天路31号名门广场北区B座3002房**

经办人：

2025 年 7 月 8 日

附件：服务成果及相关报告

序号	交付物名称
1	《核心网络（以最终采购人确认名称为准）（三级）等级保护测评报告》
2	《核心网络（以最终采购人确认名称为准）等级保护安全整改建议方案》
附注： 为高效高质完成本项目，本项目的实施过程中将部分或者全部使用但不局限于以下工具：正邦测评报告编制系统 V2.0、正邦测评方案编制系统 V2.0、正邦测评调研分析系统 V2.0、正邦党政机关网络安全服务平台 V2.0、正邦现场测评实施系统 V2.0、正邦测评计划书生成系统 V2.0、正邦定级备案生成系统 V2.0、正邦指导书生成系统 V2.0、正邦风险评估生成系统 V2.0、正邦风险分析生成系统 V2.0、正邦测评整改方案编制系统 V2.0、远程安全评估系统 V2.0、正邦测评项目管理系统 V1.0、正邦测评项目任务派发系统 V1.0、正邦综合管理平台 V1.0 等。	

附件：中标通知书

海南省政府采购成交通知书

采购编号：HZ2025-154
包编号：3
采购计划批复号：460000-2025-JH-00512

海南正邦信息科技有限公司：

海南海政招标有限公司受海口海事法院的委托，就海口海事法院信息化基础设施建设项目（采购项目编号：HZ2025-154，采购计划批复号：460000-2025-JH-00512）采用竞争性磋商进行采购，经规定采购程序，贵公司为本项目成交人，成交报价为海口海事法院信息化基础设施建设项目等保测评（总价）：79200元。中标项目内容详见《成交一览表》。

请贵公司于成交公告发布之日起（成交通知书应当于同日发出）5个工作日内，按照采购文件确定的事项与采购单位签订政府采购合同（磋商文件与成交人的投标文件为合同的组成部分）。特此通知。

成交一览表

货币单位：人民币元

服务类

品目号	品目编号及品目名称	采购标的	服务范围	服务要求	服务时间	单位	服务标准	金额（元）
3-1	C16060000 测试评估认证服务	C16060000-测试评估认证服务	核心网络（以最终采购人确认名称为准）测评	详见磋商文件	合同签订生效且达到进场条件后60个工作日内完成网络安全等级保护等级测评服务、整改指导服务，并按要求出具相关服务成果及报告。	项	详见磋商文件	79,200.00

※具体内容详见成交人响应文件

成交供应商联系人：	李亚女

联系电话：	13876461324
联系地址：	
用户单位：	海口海事法院
联系人：	罗先生
联系电话：	0898-66118106
联系地址：	

海南海政招标有限公司
2025年06月18日