安全服务采购需求

一、项目概况

1、项目名称：琼海市社会管理信息化平台一期建设项目

2、包号： D包

3、预算金额（最高限价）：人民币壹佰肆拾伍万伍仟元整（￥：1455000.00元）

4、服务地点：采购人指定地点

二、项目内容

（一）安全风险评估服务

投标人依据《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 信息系统安全保障评估框架》（GB/T 20274）、《关于进一步明确省政务信息化项目密码应用有关要求的通知》（琼国密局字〔2021〕2号）等国家和海南省风险评估工作相关规范和标准，对琼海市社管平台信息资产所面临的威胁、存在的弱点、造成的影响，以及三者综合作用所带来风险的进行安全评估。风险评估的目的是为了提高客户方信息系统的服务水平，通过信息安全管理和技术方面的评估结果，对信息系统的安全状态做出初步判断，对单位发生安全事件的可能性和抵御安全风险的能力做出公正的、客观的评价，并对信息安全风险评估发现的安全问题和安全隐患，提供整改的建议，帮助各类技术人员采取正确的技术手段进行系统整改工作，以降低、消除、规避具体安全风险，确保信息系统的安全稳定运

行。对所发现的安全风险问题及存在的不足之处进行分析，为规划信息安全保障工作者提供决策依据，保障信息化建设成果。风险评估流程如下图所示，具体包括风险评估准备、资产识别、威胁识别、脆弱性识别、风险分析以及风险评估文件记录。

（二）安全加固服务

根据网络安全基础设施建设需求和网络安全等级保护工作需求，在客户允许的前提下，为客户完全、彻底地堵住这些安全缺陷和漏洞、去除这些薄弱环节。包括打补丁、停止不必要的服务、升级或更换程序、除去特洛伊后门程序、网络安全设备的安全配置，网络安全设备的安全加固，网络安全设备的优化配置、修改配置及权限以及针对复杂问题的专门解决方案。评估加固的范围主要是琼海市社会管理信息化平台系统中的主机系统和网络设备，以及相关的数据库系统等。安全加固服务主要以人工的方式实现。消除等级保护测评中以下网络安全、主机安全问题。

（三）渗透测试服务

渗透测试服务，是在相关委办局授权的前提下，以模拟黑客攻击的方式，对琼海市社管平台相关业务系统的安全漏洞、安全隐患进行全面检测，最终目标是查找业务系统的安全漏洞、评估业务系统的安全状态、提供漏洞修复建议。在渗透过程中，采用专业的漏洞检测技术、攻击技术、攻击工具和渗透团队编写的脚本。过程分为四步：计划与准备、信息收集、实施渗透、输出报告。计划与准备阶段主要是

根据网站反馈的内容制定项目实施方案与计划；信息收集与实施渗透是项目的实施阶段，输出报告主要是汇总和评估项目中发现的安全威胁，并输出文档。

（四）应急响应服务

鉴于近年来入侵技术的复杂性、隐蔽性越来越高，对于系统安全事故的处理不能只停于解决故障上，而应该要分析原因，查清入侵来源，提高整个系统安全水平。应急响应服务根据用户的响应请求进行初步判断，确定响应方式，进行入侵分析，处理被破坏的和非法的文件，恢复网络或系统正常操作，对事件进行分析报告，消除入侵隐患。实施相应的安全建议及服务。

（五）应急机制服务

网络安全事故接二连三，“WannaCry 勒索病毒”等信息安全事件。网络信息化行业成为不法黑客重要攻击目标，网络与信息安全突发事件的频繁发生，时刻挑战着单位在应对突发事件时的应急处置能力。如何应对网络与信息安全事件，在事件发生前及时预警、防止事件发生；事件发生时迅速处置、减少损失；事件发生后及时恢复，减少影响；成为单位面对的重要课题。通过网络安全应急预案的演练，可以使单位相关技术人员掌握网络安全应急处理的正确方法，熟悉预案的相关程序，确保在网络安全事件发生时，单位的应急工作能快速、高效、有序地进行，从而最大限度地保护信息系统的保密性、完整性

和可用性。同时通过演练，不断提高团队掌握应急工作的水平和效率，发现预案设计的不足，进一步完善应急预案。

（六）漏洞扫描及管理服务

为了更好的掌握系统的安全风险状况，进行漏洞扫描服务。漏洞扫描服务可以对不同操作系统下的计算机、网络设备、安全设备等进行漏洞检测。主要用于分析和指出有关网络的安全漏洞及被测系统的薄弱环节，给出详细的检测报告，并针对检测到的网络安全隐患给出相应的修补措施和安全建议。通过购买此服务，可以加强网络信息系统安全功能，提高内部网络安全防护性能和抗破坏能力，检测评估已运行网络的安全性能，为网络系统管理员提供实时安全建议等。

（七）安全管理制度体系建设服务

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管理制度设计。制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。对安全管理活动中的各类管理内容建立安全管理制度，对管理人员或操作人员执行的日常管理操作建立操作规程，形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系，从而指导并有效地规范各级部门的信息安全管理工作。由组织最高领导层指定或授权专门的部门或人员负责安全管理制度的制定，安全管理制度通过正式、

有效的方式发布，并进行版本控制。安全策略系列文档制定后，必须有效发布和执行。发布和执行过程中除了要得到管理层的大力支持和推动外，还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。信息安全领导小组应组织相关人员对于信息安全策略体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视安全策略系列文档。

（八）安全培训服务

针对项目建设单位人员和系统使用人员进行安全培训服务，包括安全意识培训、安全技术培训、安全管理培训等。安全意识培训：按客户需要组织信息安全意识培训。通过安全培训，使用户了解基本网络安全法律法规、政策知识和安全行为准则，并且具备一定的安全意识。安全技术培训：按客户需要组织信息安全技术培训。通过安全培训，使用户了解安全设备作用和使用、安全风险识别方法、漏洞防护技术、病毒防护等知识。安全管理培训：按客户需要组织信息安全管理培训。通过安全培训，使用户了解运维。

（九）密码应用安全测评

本项目目标是针对琼海市社会管理信息化平台开展可控的商用密码应用安全性评估，对其密码应用的合规性、正确性和有效性进行评估，给出信息系统在商用密码技术应用、密钥管理及安全管理等方

面与其相应安全等级信息系统密码应用基本要求之间的差距，并提供合理化建议，协助中共琼海市委政法委员会设计详细和合理的整改方案，通过整改工作使琼海市社会管理信息化平台达到与其相应安全等级信息系统密码应用基本要求。可以有效地提高中共琼海市委政法委员会信息安全建设的整体水平，并且指明方向，有利于在信息化建设过程中同步建设信息安全设施，保障信息安全与信息化建设相协调；有利于加强对涉及国家安全、经济秩序、社会稳定和公共利益的信息系统的安全保护和管理监督；有利于明确国家、法人和其他组织、公民的安全责任，强化政府监管职能，共同落实各项安全建设和安全管理措施。评估依据包括《关于进一步明确省政务信息化项目密码应用有关要求的通知》（琼国密局字〔2021〕2号）、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码应用测评要求》、《信息系统密码应用测评过程指南》、《信息系统密码应用高风险判定指引》、《商用密码应用安全性评估量化评估规则》、《商用密码应用安全性评估报告模板（2020版）》等进行密码应用安全测评。根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）和《关于进一步明确省政务信息化项目密码应用有关要求的通知》（琼国密局字〔2021〕2号）的内容，按照等级保护三级信息系统的要求，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等方面的测评等方面，开展商用密码应用安全性评估。

三、项目的实施要求

项目实施过程中，投标方应遵循国家标准、行业标准，以及海南省相关要求。如果国家或有关部门颁布了新的技术标准和规范，则投标人应按要求采用新的标准或规范。

（一） 项目实施要求

在项目实施中投标方必须做到：

1. 提供项目实施组织架构；

2. 提供详细的项目实施方案和计划进度说明书；

3. 中标方项目经理在项目期间每周至少来招标方现场 1 次进行工作汇报，且电话要保持 7*24 小时通畅；

4. 对于招标方的电话咨询和常规服务请求在 30 分钟内予以答复，紧急服务请求在 2 小时内到达招标方现场；

5. 严格按照双方确定的计划进度保质保量完成工作；

6. 规范项目实施过程中的文档管理；

7. 项目实施中要引入风险管理、质量管理、成本管理；

8. 签署《保密协议》。

（二） 实施团队要求

投标人须在投标文件中提供完整的实施团队名单及职责分工，所有人员必须属于投标单位在册员工（以社保缴纳证明为认定依据）。实施团队名单中所列人员的社保缴纳证明复印件需在投标文件中提供，并加盖公章。

（三） 项目验收

投标方必须书面通知招标方所完成的工作和准备进行验收的项目种类及验收开始时间，此通知书需经招标方认定后方可执行。

（四）验收组织

成立由招标方以及其他有关人员组成的验收小组，负责对项目进行全面的验收。

（五）验收标准

1. 中标方完成本合同项下所有安全服务内容；

2. 中标方按照本合同项下所有安全服务内容提交交付成果；

3. 中标方提交项目实施阶段中所有的过程文档；

4. 服务期：自合同生效且具备实施进场条件之日起 60 个工作日内完成