采购需求

一、服务内容和要求

（一）项目概况

为建立健全网络与信息安全保障体系，提高信息系统安全管理水平和安全防范能力，减少安全隐患和安全事故，有效保障系统安全、稳定运行，海南省市场监督管理局需采购网络安全保障服务

（二）采购服务方式

竞争性磋商

（三）服务内容

（1）网络安全管理制度建设、指导服务

依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》及省政府相关部门的要求，通过风险评估、安全规划等各种手段，协助采购人建立完整的网络与信息安全管理体系，防止信息系统出现安全事故或事件。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	信息安全管理制度建设服务	通过网络安全管理体系建设，明确主管领导、落实责任部门、落实安全岗位和人员、确定安全管理策略、制定安全管理制度、落实安全管理措施、落实《网络安全法》《数据安全法》《个人信息保护法》中安全管理的各项指标和要求，提高信息系统的管理与运维水平。	采购人网络安全管理体系	《网络安全管理制度》	一次	现场服务

（2）日志和审计数据分析服务

协助采购人确认信息系统部署的数据库审计、日志审计服务能满足等保要求，通过对采购人信息系统应用日志、数据库日志进行审计、分析，查找安全漏洞和数据泄露安全隐患。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型

1	日志和审计数据分析服务	信息系统部署的数据库审计、日志审计服务满足等保要求；对采购人信息系统应用日志、数据库日志进行审计、分析，查找安全漏洞和数据泄露安全隐患。	采购人信息系统	《日志和审计数据分析报告》	一次	现场服务

（3）渗透测试服务

采购人派出网络安全攻防团队（不少于 2 名高级渗透测试专家），对采购人指定的系统进行渗透测试，根据渗透测试情况出具报告，并给出整改建议，及时协助复测。通过测试最终达到发现和消除相关系统网络安全风险的目标。渗透测试途径包括：

1.黑盒测试。黑盒测试原意是指，把程序看作一个不能打开的黑盒子，在完全不考虑程序内部结构和内部特性的情况下，通过测试来检测每个功能是否都能正常使用。

在渗透测试中，黑盒测试则是指，测试人员在仅获得目标的 IP 地址或域名信息的情况下，对目标系统发起模拟入侵的尝试。

2.内部测试与外部测试。内部测试是指，测试人员在现场直接介入到内部网络，对目标系统发起模拟入侵的测试行为。外部测试则是指用户直接从互联网对测试目标系统进行访问和各类安全测试，这种测试用于验证来自互联网的威胁。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	渗透测试服务	通过模拟黑客可能使用的攻击方式和漏洞挖掘行为，对目标信息系统的安全进行深入安全检测，发现并验证漏洞，为信息系统管理人员提供安全加固建议。	海南 e 登记、特种设备综合管理系统、国家企业信用信息公示系统、海南省市场监管综合业务平台（二期）	《信息系统渗透测试报告》	一年 2 次	现场服务

（4）网络安全培训服务

为了加强海南省市场监督管理局相关人员的安全意识，提高岗位技能和相关安全技术技能，提供特定的网络安全培训。

序号	服务内容	服务说明	服务对象	主要成果文档	服务周期	服务类型

1	网络安全培训服务	通过网络安全培训提升海南省市场监督管理局相关人员网络安全意识、拓宽网络安全视野，强化信息安全组织管理能力，提升信息安全保障水平,并且通过专业技术培训，不断培养信息化相关人员的网络安全应急处置能力和防护水平。	海南省市场监督管理局相关人员	《培训PPT》及其他相关材料	一年2次	现场服务

（5）应急管理咨询（应急预案+演练）服务

开展应急演练，检验应急预案实用性、应急机制科学性、应急体制合理性、应急程序的适用性。根据应急预案规定的流程，进行相应的模拟演练，事后进行总结分析，对应急预案不足之处进行修订。同时，使得信息系统相关人员了解应急流程和责任，在安全事件发生时，能够有条不紊地开展应急工作，最大程度降低安全事件带来的负面影响和损失。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型
1	应急管理咨询（应急预案+演练）服务	编制完善《信息安全事件应急预案》，并对信息系统相关人员进行应急预案、应急技巧及对典型的信息安全事件进行预防等方面的培训，并针对《信息安全事件应急预案》开展相应的应急演练工作。	采购人信息系统	《应急预案修订》《应急演练总结评估报告》	一年1次	现场服务

（6）安全漏洞扫描评估服务

通过安全漏洞扫描评估服务，分析海南省市场监督管理局信息系统存在的各种安全漏洞及问题；帮助海南省市场监督管理局充分了解各个系统及服务器存在的安全隐患，建立安全可靠的WEB应用服务，改善并提升WEB应用系统抗各类WEB应用攻击的能力(如：注入攻击、跨站脚本、钓鱼攻击、信息泄漏、恶意编码、表单绕过、缓冲区溢出等)，并提出具体的安全解决方案，以及配合我单位及时对发现的问题进行整改。

序号	服务内容	服务说明	服务对象	主要成果文档	服务频率	服务类型

1	安全漏洞扫描评估服务	依据网络安全等级保护相关标准及规范，采用多种安全专用评估工具对信息系统进行全面深度漏洞探测，及时掌握信息系统安全状况，为改善并提高信息系统安全性提供依据；并提供详细的安全评估报告，报告内容包括扫描的漏洞详细信息、安全加固建议等，对所有漏洞弱点的相关背景提供详细描述、引用，以及相应的修复和改进建议；并提出具体的安全解决方案，以及配合我单位及时对发现的问题进行整改。	网络设备、安全设备、服务器、操作系统、数据库、Web 应用、所有三级定级信息系统	《安全漏洞扫描评估报告》（含安全漏洞验证）	一年4次	定期巡检现场服务

（7）WEB 云安全服务

通过 Web 云监测服务，可对 Web 系统的安全状态进行全方位监测，包括：网站漏洞（各类 Web 应用漏洞、网站敏感信息泄露）；安全事件（网页挂马、暗链、敏感关键字、变更）；可用性（网站访问速度、网站应用状态）；网站信息（ICP 备案、Alexa 排名、Whois 信息、IP、网站使用的三方组件及应用）等。

序号	服务内容	服务说明	服务对象	主要成果文档	服务周期	服务类型
1	WEB 云监测服务	1. 通过 Web 云监测服务，可对 Web 系统的安全状态进行全方位监测，包括：网站漏洞（各类 Web 应用漏洞、网站敏感信息泄露）；安全事件（网页挂马、暗链、敏感关键字、变更）；可用性（网站访问速度、网站应用状态）；网站信息（ICP 备案、Alexa 排名、Whois 信息、IP、网站使用的三方组件及应用）等。 2.当 Web 网站系统发生报警或故障时，配备专员第一时间响应云监测，提供安全保障咨询。 3.按每月输出《Web 网站系统安全运行情况报告》。	海南 e 登记	《Web 网站系统安全运行情况报告》	一整年	远程服务+定期巡检现场服务

（8）攻防演练服务

整个网络安全攻防演习期间的工作内容包括（但不限于）架构安全评估及加固、安全检测与防御能力提升、核心应用系统渗透测试、培训、陷阱主机部署测试、实战演习对抗安全值守、实施监测与分析、攻击事件溯源、处置、上报、护网总结分析、出具安全整改建议、系统安全加固等。派遣演习值守团队，团队人数不少于 3 人（每日现场值守人员不少于 2 人）。团队人员均须具备丰富网络攻防工作经验，能够熟练应对和处理突发网络安全事件。在演习期间现场值守，直至演习结束，值守团队应主要负责以下工作：

a)实时监测分析：根据监测人员发现的可疑安全事件，由值守团队进行安全事件确认，若存在威胁，将安全事件进行上报，并告知网络运维人员封堵攻击源。

攻击事件溯源、处置、上报：结合威胁情报、已发现攻击事件，对攻击事件进行溯源分析，发现漏洞提出安全加固建议，并协助业务人员进行安全加固，加固完成后二次漏洞验证，确保漏洞被修复；安全事件处置完毕，编写安全处置报告并上报演习指挥部。

序号	服务内容	服务说明	服务对象	主要成果文档	服务周期	服务类型
1	攻防演练服务	工作内容包括（但不限于）架构安全评估及加固、安全检测与防御能力提升、核心应用系统渗透测试、培训、陷阱主机部署测试、实战演习对抗安全值守、实施监测与分析、攻击事件溯源、处置、上报、护网总结分析、出具安全整改建议、系统安全加固等。	采购人信息系统	《Web网站系统安全运行情况报告》	不定期，根据省攻防要求	远程服务+现场服务

（9）数据防泄密服务

序号	服务内容	服务说明	服务对象	主要成果文档	服务周期	服务类型
1	数据防泄密服务	协助梳理我局数据资产，形成数据资产地图。建立相关的数据安全管理规范，进一步分析敏感数据泄密风险，提供数据防泄密的建议意见，并配合系统运维方部署防泄密或数据服务，防止敏感信息泄露。	海南e登记系统	《数据防泄密分析报告》	一整年2次	远程服务+现场服务

（10）备份数据的恢复性测试服务

序号	服务内容	服务说明	服务对象	主要成果文档	服务周期	服务类型
1	备份数据的恢复性测试服务	协助采购人开展信息系统的备份数据恢复性测试。	采购人信息系统	《备份数据恢复性服务报告》	一整年2次	远程服务+现场服务

二、商务条款

（一）合同签订期：自中标通知书发出之日起15个工作日内

（二）服务期限：签订合同之日起一年。

（三）售后服务要求：

（1）处理问题响应时间：当信息系统安全事件发生时，接到采购人通知后30分钟内到达采购人指定现场。

（2）其他：根据评审会、工作对接会、协调会等意见相应修改完善网络安全保障内容。

（四）其他要求：

（1）报价必须含以下部分，包括：

网络安全评估报告：现场调研、网络安全加固、方案编制、完成后续服务要求等相关费用，汇报材料及成果打印费用等材料费，有必要的保险费用和各项税金。

（2）本项目实行费用包干制，如提供服务过程中产生额外费用，由中标人自行负责，不接受转包及分包。

（3）付款方式：签订合同之日起，采购人收到中标方提供的有效发票后，10个工作日内支付50%合同金额。合同签订当年12月底前支付40%合同金额，项目验收通过后支付剩余合同金额。**验收未通过，服务期顺延，直至通过为止。**

（4）中标方不得以任何形式向与本项目无关的其他单位或人员提供本项目相关资料,如违反,必须赔偿采购人的所有损失，且采购人保留追究法律责任的权力。

（5）本项目成果及其相关知识产权权利归采购人所有。