服务范围及要求

（一）项目服务内容

编号	服务名称		服务期限
1	网络安全等级保护测评服务	征稽网络与环境系统　三级	自合同签订之日并取得备案证明具备实施条件起 60 个工作日内针对 3 个信息系统开展等级测评工作，并输出《网络安全等级保护等级测评报告》。
		新征费管理系统　三级	
		音视频监控系统 三级	
2	其他服务	网络安全整改建设方案设计服务	自合同生效之日并取得备案证明具备实施条件起 60 个工作日内完成，并输出《网络安全整改设计方案》。
3		网络安全应急响应服务	自合同生效之日起提供一年内 1 次网络安全应急响应服务。在信息系统出现安全事件时，将第一时间派遣专业的安全服务工程师提供现场支持服务，及时采取相关安全措施限制安全事件扩散和影响范围，尽可能减少损失，并协助排查安全事件原因，提出基于安全事件的解决方案，协助后续安全处置。
4	售后服务	网络安全培训服务	自合同签订生效之日起提供一年内 1 次网络安全培训服务。
		网络安全咨询服务	自合同签订生效之日起提供一年内网络安全咨询服务。

（二）项目服务要求

1、网络安全等级保护测评服务

供应商依据国家信息安全等级保护管理规定，按照《信息安全技术 网络安

全等级保护基本要求》（GB/T22239-2019）三级 S3A3G3 的有关管理规范和技术标准对海南省交通规费征稽局的信息系统进行等级测评，通过测评掌握信息系统的安全状况、排查系统安全隐患和薄弱环节、明确信息系统安全建设整改需求；衡量信息系统的安全保护管理措施和技术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；在完成测评后，针对每个信息系统，出具相应的测评报告。

（1）测评内容

供应商需对本项目所涉及到的系统要素进行确认、分析和梳理，提出详细的等保测评方案。

对信息系统的整体保护状况和信息系统组件，逐一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：

等级保护对象测评范围：安全技术测评和安全管理测评

序号	测评范围定义	测评内容
安全通用要求		
1	安全技术测评	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
2	安全管理测评	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
云计算安全扩展要求		
1	安全技术测评	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
2	安全管理测评	安全建设管理、安全运维管理

完成测评工作后，出具符合省公安机关要求的《网络安全等级保护等级测评报告》，提出相应的整改建议。

（2）测评实施

供应商在测评过程中，需按照《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、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。提供详细的测评服务方案并按照《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。

（3）测评服务工期：自合同签订之日并取得备案证明具备实施条件起45个工作日内完成。

（4）供应商在安全服务过程中，应根据服务规范和海南省交通规费征稽局要求提供系统、完整、清晰的服务日常报告。供应商提供的服务文档如下：

1）测评准备活动阶段：

《项目计划书》；

《信息系统调查表》；

《会议记录表》；

2）方案编制活动阶段：

《信息系统网络安全等级测评方案》；

3）现场测评活动阶段：

《现场测评授权书》；

《文档交接单》；

《会议记录》；

4）报告分析及编制活动阶段：

服务成果：提交所有系统的测评报告：

《网络安全等级保护【征稽网络与环境系统】等级测评报告》；

《网络安全等级保护【新征费管理系统】等级测评报告》；

《网络安全等级保护【音视频监控系统】等级测评报告》。

2、网络安全整改建设方案设计服务

供应商自合同生效之日并取得备案证明具备实施条件起60个工作日内，结合海南省交通规费征稽局的安全现状和测评结果，提供具有针对性的信息系统等级保护安全建设整改方案设计服务，针对等级测评过程发现的问题，供应商依据信息系统安全等级保护政策法规和标准规范，以及《关于开展信息安全等级保护安全建设整改工作的指导意见》(公信安[2009]1429号)的规定，并结合本单位的实际情况，针对信息系统输出相应的《网络安全整改设计方案》，包含信息系统安全建设整改技术方案与安全管理体系规划。

服务成果：《网络安全整改设计方案》。

3、网络安全应急响应服务

在信息系统出现安全事件时，提供远程或场应急响应处置服务；提供7×24小时的电话支持安全服务，当远程支持无法解决问题时，将第一时间派遣专业的安全服务工程师提供现场支持服务，及时采取相关安全措施限制安全事件扩散和影响范围，尽可能减少损失，并协助排查安全事件原因，提出基于安全事件的解决方案，协助后续安全处置。应急响应的安全事件包括如下：

1.计算机病毒与木马攻击安全事件；

2.网络攻击安全事件；

3.信息泄露或篡改事件；

4.网页代码篡改事件；

5.安全漏洞或漏洞攻击事件，包括相关网络安全监管部门发出的漏洞通报、安全预警等。

服务成果：输出《网络安全应急响应处置报告》。

4、网络安全培训服务

供应商自合同签订之日起提供一年内1次的网络安全培训服务。根据海南省交通规费征稽局信息系统的实际情况，制定信息安全等级保护的针对性培训方案，培训内容包括但不限于以下内容：

- 《中华人民共和国网络安全法》解读；
- 了解信息安全等级保护工作的相关流程及目的；
- 了解并掌握信息安全等级保护政策标准体系及其相关应用方法；
- 掌握信息安全等级保护定级备案相关流程及内容；
- 了解并掌握信息安全等级保护测评工作的相关要求及方法；
- 了解信息安全等级保护安全建设整改工作的相关内容及方法；
- 了解并掌握信息安全管理的重要性及落实的相关措施；
- 信息安全意识宣讲，提升全员信息安全意识；
- 云计算环境的安全防护技术内容；
- 信息安全攻防技术及渗透测试技术内容。

供应商应提供详细的培训方案（包括培训内容、时间、人数等）。如有特殊的培训内容要求，可以进行商定后，再行确定相应的培训课题及内容。每次培训后提交相应的安全培训课件资料。

5、网络安全咨询服务

供应商自合同签订生效之日起，提供免费的一年咨询服务。

（1）等级保护政策/标准咨询

随着国家信息安全等级保护的工作推进，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，提供于海南省交通规费征稽局各部门相关人员咨询，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）信息系统等级定级咨询

采购人在售后服务期间如果有新建系统，供应商需协助海南省交通规费征稽局对信息系统进行识别，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。

定级阶段，供应商需根据等保相关主管部门和国家工信部的要求和指南，协助海南省交通规费征稽局完成定级对象确认、系统定级和定级备案工作。

（3）等级保护自查咨询

按照等级保护相关政策要求，信息系统运营使用单位应定级对信息系统进行自查活动，在自查活动期间，供应商应提供相应的咨询服务。

服务标准：

项目实施过程中，供应商应遵循国家标准、行业标准。

1、项目实施要求

（1）提供的项目实施组织架构；

（2）提供详细的服务方案和计划进度说明书；

（3）提供详细、全面的人员培训计划和实施方案；

（4）项目实施完成后提供可靠的后期维护工作；成交方在项目期间每周至少来采购人现场 1 次，电话要保持 7*24 小时通畅，如遇到特殊情况需提前通知采购人并取得采购人的同意；

（5）对于采购人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 4 小时内到达采购人现场；

（6）严格按照双方确定的计划进度保质保量完成工作；

（7）规范项目实施过程中的文档管理；

（8）项目实施中要引入风险管理、质量管理、成本管理。

（9）为保证项目质量和售后服务保障的及时有效响应，要求参与本项目的供应商应满足如下要求：

1）供应商开展本项目信息安全等级保护测评服务期间，项目负责人每周至少来海南省交通规费征稽局 1 次汇报项目进展工作，电话要保持 7*24 小时通畅，如遇到特殊情况需提前通知海南省交通规费征稽局的相关人员。

2）供应商在开展本项目售后服务期间，对于采购人的紧急应急响应服务请求需在 2 小时内到达采购人现场。

2、实施团队要求

供应商在响应文件中应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响应文件中提供，并加盖公章。