采购需求

一、项目概况

本项目主要对四川省交通运输厅数据中心提供网络安全日常运行保障与网络安全重保与应急响应服务。

其中，网络安全日常运行保障包括：网络安全态势感知监测与分析服务、安全基线配置核查服务、重要应用系统安全风险评估、重要 web 应用安全监测服务、行业网络安全通报及评分服务、网络安全攻防演习和应急预案演练服务、系统渗透测试及新系统上云安全检查前安全检测、厅数据中心安全产品监测服务（日志管理与分析服务）、代码安全审计服务、漏洞扫描服务、网络安全相关培训及宣传周相关工作服务、相关安全管理制度补充完善及全年网络安全工作总结。

网络安全重保与应急响应服务包括：网络安全重保服务、网络安全应急响应服务。

二、采购服务清单

序号	采购内容	单位	数量
一、网络安全日常运行保障			
1	网络安全态势感知监测及分析服务	项	1
2	安全基线配置核查服务	项	1
3	重要应用系统安全风险评估	项	1
4	重要 web 应用安全监测服务	项	1
5	行业网络安全通报及评分服务	项	1
6	网络安全攻防演习和应急演练服务	项	1
7	系统渗透测试及新系统上云前安全检测	项	1
8	厅数据中心安全产品监测服务（日志管理与分析服务）	项	1
9	代码安全审计服务	项	1
10	漏洞扫描服务	项	1
11	网络安全相关培训及宣传周相关工作服务	项	1
12	相关安全管理制度补充完善及全年网络安全工作总结	项	1
二、网络安全保障与应急响应服务			
1	网络安全重保服务	项	1
2	网络安全应急响应服务	项	1

三、服务要求

总体要求：供应商至少应具备基于行为的实时安全监控、策略控制、安全事件主动发现和预警、态势感知及安全事件及时处置的能力，并做好日志管理、访问策略管理等安全基线配置核查相关工作。

1 网络安全日常运行保障

1.1 ★ 网络安全态势感知监测及分析服务

1.1.1 服务内容

对我厅所有网络节点流量进行采集，通过专业的信息安全态势感知平台进行挖掘分析，帮助我厅发现网络中存在的各种威胁和沦陷主机，实现全面的网络安全态势感知，并根据分析结果在第一时间提供相应的改进建议或处置策略，协助系统开发单位、机房运维单位等及时采取相应措施，尽快完成整改，减少安全问题带来的影响；具备日志采集识别告警、威胁情报采集管理、态势感知、安全运营与应急响应、安全治理等能力。

1.1.2 交付文件

项目交付物资料如下内容：

按照月、半年、全年的时间节点编写《四川省交通运输厅全流量检测报告》，内容包括但不限于时间节点内全厅流量检测情况、检测情况分析、工作不足、下个月（或下半年、第二年）工作改进措施等。

1.2 ★ 安全基线配置核查服务

1.2.1 服务内容

对厅数据中心相关安全对象的配置脆弱性进行全面检查。

1.2.2 服务范围

包括但不限于各类网络设备、安全设备、存储设备、主机设备，操作系统、数据库和中间件等的账号、口令、授权、日志安全要求，不必要的服务、启动项、注册表、会话设置，以及TELNET、SSH、SMB、RDP 等网络协议配置的核查。

1.2.3 交付文件

按照月、半年、全年的时间节点编写《四川省交通运输厅数据中心安全基线配置核查报告》，内容包括但不限于判定依据、检查点、标准值、实际值、加固方案等。

1.3 ★ 重要应用系统安全风险评估

1.3.1 服务内容

对厅数据中心重要应用系统进行安全评估，在提供的评估服务当中，参考信息系统安全等级保护 2.0 基本要求，主要从物理层面、网络层面、主机层面、应用层面开逐一展开评估，最终形成安全评估报告。

物理安全评估

检查关键或敏感的信息处理设施是否放置在安全区域内，并受到确定的安全边界的保护，包括适当的安全屏障和入口控制。这些设施要在物理上避免未授权访问、损坏和干扰。所提供的保护要与所识别的风险相匹配。

检查是否做到防止资产的丢失、损坏、失窃或危及资产安全以及组织活动的中断。应保护设备免受物理的和环境的威胁等。

网络安全评估

基础网络架构，网络传输加密，访问控制，网络设备安全漏洞，设备配置安全等方面进行评估。

主机系统安全评估

采用人工访谈与现场设备检查的方式对相关业务系统进行评估，通过与信息系统相关负责人的访谈了解项目范围内服务器系统的当前安全配置情况并对收集信息进行分析，并结合客户实际需求提供系统整改建议。

主要对以下主机内容进行检查：身份鉴别方式；帐号安全设置；远程管理方式；多余帐号和空口令检查；默认共享检查；文件系统安全；网络服务安全；系统访问控制；日志及监控审计；拒绝服务保护；补丁管理；病毒及恶意代码防护；系统备份与恢复；硬件冗余情况；硬盘分区格式；应用安全评估。

应用系统安全评估

对应用系统的运维人员进行访谈和调研，了解系统管理情况，建设情况，通过访谈从全局角度了解安全现状。从技术角度展开渗透测试、漏洞扫描、web 容器基线配置检查等安全手段发现应用系统存在的存弱点。

1.3.2 服务范围

包括但不限于以下系统(含市州配发软硬件)：

序号	信息系统名称
1	四川省级政务云交通云整合平台
2	四川省交通运输厅综合政务平台

3	四川省一体化政务服务平台交通运输网上行政审批服务系统
4	四川省交通运行监测与应急指挥系统
5	四川省道路运输综合管理与服务信息平台
6	四川省交通量调查及路况信息管理系统
7	四川省高速公路管理与服务综合信息平台
8	四川省公路水运工程质量安全监督管理平台
9	四川省普通公路养护综合平台
10	四川省航务海事综合信息平台
11	四川省交通旅游服务大数据应用试点工程
12	四川省交通运输行政执法综合管理信息系统
13	四川省交通运输统计分析监测和投资计划管理信息系统
14	四川省交通运输物流公共信息平台
15	综合规划业务平台系统
16	四川省交通运输行业专家库系统
17	四川省公路治超管理应用系统
18	四川省交通运输厅综合业务办理系统

1.3.3 交付文件

对四川省交通运输厅重要信息系统进行安全评估，根据安全评估开展情况输出（每季度不少于一次）：

《XX 系统安全评估报告》

《XX 系统渗透测试报告》

《系统风险清单跟进表》

1.4 ★ 重要 web 应用安全监测服务

1.4.1 服务内容

对厅数据中心互联网出入口进行 7x24 小时安全监测服务，对重要 Web 系统进行重点监测，监控服务内容包括但不限于以下几方面：

支持对网站可用性监测：HTTP 监测、DNS 监测、DDOS 攻击监测；

支持对网站安全事件监测：篡改-网站挂马，篡改-黑词黑链，篡改-内容变更仿冒网站（钓鱼网站），违规内容（敏感词）；

支持对网站安全漏洞监测，支持类型：漏洞扫描，威胁情报（包含安全舆情，0DAY,人工发现的漏洞等）；

监测到重要 Web 系统存在安全问题时，应第一时间给出整改建议，协助系统开发单位及时采取相应措施，尽快完成整改，减少安全问题带来的影响。

1.4.2 服务范围

包括但不限于以下系统：

序号	网站名称
1	四川省交通运输厅官网
2	四川信用交通
3	四川交通运输网上行政审批服务平台
4	四川省交通运输物流公共信息平台
5	四川省交通运输厅工程技术职称评审管理系统
6	四川省交通运输统计监测和投资计划管理信息系统
7	公路水路建设与运输市场信用信息服务系统
8	四川省交通运输行政执法综合管理系统
9	四川省交通运输厅综合政务平台
10	四川省交通旅游服务大数据应用系统
11	四川省交通量调查及路况信息管理系统
12	四川省高速公路管理与服务综合信息平台

13	四川省公路水运工程质量安全监督管理平台
14	四川省道路客运联网售票系统
15	四川省普通公路养护综合平台
16	四川省航务海事综合信息平台

1.4.3 交付文件

根据的四川省交通运输厅监测网站输出：

按照月、半年、全年的时间节点编写《四川省交通运输厅互联网安全检测报告》，内容包括但不限于时间节点内全厅互联网安全检测情况、检测情况分析、工作不足、下个月（或下半年、第二年）工作改进措施等。

1.5 ★ 行业网络安全通报及评分服务

1.5.1 服务内容

根据《四川省交通运输厅网络安全信息通报管理办法》开展厅网络安全信息通报服务、根据厅网络安全主管单位要求，收集统计各单位报送的评分依据材料，协助厅网络安全主管单位完成交通行业相关单位通报评分。

整理所收集发现的网络安全态势、外部威胁情报、各类脆弱性发现成果及厅直属单位、市（州）交通部门上报的信息安全情况，输出每月网络安全月报告及整改/告知通知书。月报告中的内容包括但不限于以下几个方面：

（1）行业网络安全总体情况。

（2）系统及网络运行状态。

（3）主机安全风险情况。

（4）系统渗透测试情况。

（5）重要 web 系统运行状况。

（6）网络安全预警及漏洞信息。

（7）国内外网络安全情况摘要。

1.5.2 服务范围

厅内需要通报的网络安全内容。

1.5.3 交付文件

包括但不限于：

《四川省交通运输厅 X 月网络安全报告》。

《四川省交通运输厅 X 季度评分通报》。

《四川省交通运输厅网络安全态势分析报告》。

1.6 ★ 网络安全攻防演习和应急演练服务

1.6.1 服务内容

根据四川省交通运输厅信息中心实际需求，开展全年不少于 2 次网络安全攻防演习和 2 次应急演练，攻防演习内容包括但不限于由服务商组建攻击队，编制攻防演习方案，对厅属相关单位目标系统开展网络安全攻击演练，并协助各相关单位对发现的系统问题进行修复整改，并编制攻防演习总结报告。

1.6.2 服务范围

应急演练事项包括但不限于以下内容：

ddos 事件应急演练

web 入侵事件应急演练

病毒蠕虫事件应急演练

挂马网页、篡改事件应急演练

勒索病毒事件应急演练

1.6.3 交付文件

成果包括但不限于：

《四川省交通运输厅网络安全攻防演习方案》

《四川省交通运输厅网络安全攻防演习总结报告》

《四川省交通运输厅网络安全应急演练方案》

《四川省交通运输厅网络安全应急演练总结》

《四川省交通运输厅信息安全故障处理登记表》

《四川省交通运输厅应急演练记录表》

1.7 ★ 系统渗透测试及新系统上云前安全检测

1.7.1 服务内容

1、对厅属相关单位的重要 WEB 系统及 21 个市（州）交通运输局门户网站进行远程扫描与渗透，找出系统的脆弱性、风险点，提出整改加固建议，并输出报告，每季度一次，并将结果在《四川省交通运输厅网络安全信息通报月报》中通报。

2、对四川省交通运输厅的新业务系统上云前进行安全检测及渗透测试，找出风险点，并提出整改加固建议。

3、根据采购方要求针对四川省交通运输厅数据中心机房系统进行安全检查及渗透测试，每季度不少于 1 次。

1.7.2 服务范围

厅属相关单位的重要 WEB 系统及 21 个市（州）交通运输局门户网站进行远程扫描与渗透。

1.7.3 交付文件

《渗透测试报告》

《系统上云安全检查报告》

1.8 ▲ 厅数据中心安全产品监测服务（日志管理及分析服务）

服务期间按要求对厅数据中心部署安全产品进行监测服务，完成告警日志收集、管理与分析，并对产品的策略配置提出专业建议，同时根据各设备的功能综合分析研判数据中心整体安全情况，分析报告每季度不少于一次。

1.9 ▲ 代码安全审计服务

服务期间对厅数据中心部署信息系统提供代码审计服务，包括但不限于系统重大版本更新、新系统上线、系统终验等场景。针对信息系统用最新的特征库进行代码扫描，提供扫描报告并解读报告，协助应用开发方修复代码漏洞；除以上条件外每半年开展不少于 1 次代码安全审计服务。

1.10 ▲ 漏洞扫描服务

服务期间对厅信息中心（含数据中心机房及市州配发设备）提供漏洞扫描服务，包括但不限于服务器、Web 应用、数据库、网络设备、安全设备、终端等。所提供产品支持 VPN 代理扫

描，可在其界面添加代理网络配置；常规情况下每月输出至少三次《漏洞扫描报告》。

1.11 ▲ 网络安全相关培训及宣传周相关工作服务

服务期间按照厅相关要求为厅网络安全成员单位提供两次以上网络安全相关知识培训；配合采购人做好网络安全宣传周相关工作；每年负责对 1 名厅网络安全相关人员提供技术培训，使其获得由国家行政机关批准成立的国家信息安全权威机构颁发的认证证书，项目包含报名、培训等各项费用。

1.12 ▲ 相关安全管理制度补充完善及全年网络安全工作总结

按照部、省、厅相关要求，针对厅数据中心网络安全现状以及网络安全相关制度框架体系，梳理并补充完善网络安全相关制度编制工作。

出具厅数据中心全年网络安全工作总结，内容包含但不限于防护成果、防护的不足及改进措施。

2 网络安全保障与应急响应服务

2.1 ★ 网络安全重保服务

2.1.1 服务内容

服务内容	具体描述
网络安全驻场服务	提供服务期内工作日 5*8 小时现场驻场服务（投标人须自行承诺，驻场人员应具有一年以上网络安全工作经验，具备独立应对网络安全事件处置能力），在国庆、两会、攻防演习等重保期间，采购人提出重保要求后提供 7*24 小时驻场服务。重保前按要求提交《XX 值守方案》，方案内容包括但不限于：驻场人员名单及排班，重保前、重保期间工作安排，重保期间以及重保结束报告提交等。 重保期间按要求全面深入排查网络安全风险，及时调整网络安全策略，切实加强网络安全防范和监测措施，及时进行漏洞修补、重点加固，全力做好重要时期网络基础设施、重点网站和业务系统的安全保障工作。**（驻场人员必须为投标人本单位职工，须提供人员在本单位的在职证明材料）**

应急响应	在服务期间，一旦发生网络安全事件，应及时进行网络隔离、并开展事件分析、信息上报、风险处置及安全加固等工作。主要包括： ①按照省及厅网络安全事件应急预案的相关要求，并结合有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件和其他网络安全事件等网络安全事件制定相应的操作规程，确保对安全事件的预防、监测、报告及应急处置等相关工作落地落实； ②对安全事件按照操作规程进行快速处置； ③分析安全事件原因； ④基于安全事件提供安全解决方案； ⑤风险处置； ⑥协助开展安全加固； ⑦提交应急响应总结：形成应急响应报告并及时提交网络安全情况表。
总结	若发生应急响应事件，形成应急响应报告。

2.1.2 交付文件

服务交付成果包括但不限于：

《安全事件处理操作规程》

《XX 值守方案》

《XX 事件应急响应报告》

《XX 值守报告》

《网络安全情况报送表》

2.2 ★ 网络安全应急响应服务

2.2.1 服务内容

根据厅数据中心实际情况，提供安全事件应急响应和处置方案，在发生信息破坏事件（篡改、泄露、盗窃、丢失等）、大规模病毒事件、Web 网站漏洞事件等相关的信息安全事件时，

提供应急响应专家协助处置服务。对发生应急响应事件进行分析，找出事件真相、查出威胁来源与安全弱点、找到问题正确的解决方法，协助判定事故责任。

2.2.2 服务范围

应急响应服务范围为厅数据中心所发生安全事件，包括但不限于：

钓鱼邮件、黑客入侵、病毒感染、APT 攻击、漏洞利用、网络攻击、数据外泄、事件通报、攻击溯源、网络异常、网站被黑、非法访问、网站挂马、网站暗链、网站篡改。

2.2.3 交付文件

应急响应服务的交付成果包括但不限于：

《xx 事件应急响应分析报告》

《网络安全情况报送表》

四、 商务要求

（一）服务期限：本项目服务期为合同签订之日起一年，服务期满 11 个月，中标人提出续签合同申请，经采购人研究同意后，可续签 12 个月服务期，最多续签 2 次。如服务期间出现较大及以上网络安全事故，采购人可随时提出不再续签要求。

（二）服务地点：采购人指定地点。

（三）付款方式：

1.签订合同，采购人在收到中标人递交的付款申请及正规发票后 15 个工作日内向中标供应商支付合同金额的 30%；

2.合同服务期过半后，采购人在收到中标人递交的付款申请及正规发票后 15 个工作日内向中标供应商支付合同金额的 40%；

3.服务期满并通过甲方验收，采购人在收到中标人递交的付款申请及正规发票后 15 个工作日内向中标供应商支付合同金额的 30%。

（四）履约保证金：不收取履约保证金。

（五）验收方法和标准

按国家有关规定以及招标文件的质量要求和技术指标、中标供应商的投标文件及承诺与本合同约定标准进行验收；采购人、中标供应商双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在招标文件与投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

注：带“★”项为实质性指标，如不满足其投标文件将被否决；