附件

四川省加强车联网网络安全和数据

安全工作方案

按照工业和信息化部《关于加强车联网网络安全和数据安全工作的通知》（工信部网安〔2021〕134 号）要求，为进一步强化我省车联网网络安全和数据安全管理，建立健全车联网网络安全管理工作机制，提升车联网网络安全综合保障能力，特制定本方案。

一、总体要求

以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大和十九届二中、三中、四中、五中、六中全会精神，落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《通信网络防护管理办法》等法律法规，结合《新能源汽车产业发展规划（2021-2035年）《智能汽车创新发展战略》《车联网（智能网联汽车）产业发展行动计划》以及工业和信息化部《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于加强车联网卡实名登记管理的通知》等有关要求，进一步健全我省车联网安全管理体系，加强安全防护技术手段建设，督促企业落实主体责任，全面提升我省车联网安全保障水平，助力我省经济高质量发展。

1. 工作目标

 2021-2022年，指导各车联网建设、运营相关企业切实履行网络安全主体责任，建立健全网络安全和数据安全管理制度和工作机制，不断完善技术防护和保障措施，企业网络安全和数据安全防护能力有力提升，车联网网络安全保障体系初步建成。

 2023年以后，建立规范化、常态化的车联网网络安全和数据安全管理长效机制，车联网网络安全保障体系全面建成，车联网安全保障能力持续提升。

三、重点任务

（一）加强网络安全和数据安全基础管理

**1.落实安全主体责任。**各企业要建立健全网络安全和数据安全管理制度，指定网络安全工作负责人，明确管理机构及工作职责。建立企业内部监督、考核及问责机制，加大人力、财力、物力保障，建立常态化安全隐患排查整改工作机制，经常性开展网络安全和数据安全宣传、教育和培训。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**2.全面加强安全保护。**各企业要贯彻落实相关法律法规和《车联网信息服务平台安全防护技术要求》等车联网安全相关标准规范，从技术和管理两方面，加强汽车、网络、平台、数据等安全保护，监测、防范、及时处置网络安全风险和威胁，确保车联网安全稳定运行。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**3.做好车联网卡实名登记。**各企业要按照《关于加强车联网卡实名登记管理的通知》（工信部网安函〔2021〕246号）要求，切实做好车联网卡实名登记，并于2022年9月30日前组织完成已售出车联网卡实名补登记。车辆生产企业应加强车联网卡采购、使用、销售等基础管理；在车辆销售时，应参照电话用户真实身份信息登记相关标准规范，认真核验和登记车辆所有者（含单位用户）真实身份信息；车辆销售后，应将用户登记信息、车联网卡号码或识别码等基础信息及时传送至电信企业。电信企业在售前环节应做好购买车联网卡的车辆生产企业（或其授权企业）及责任人信息登记，在售后环节做好车联网卡用户信息登记；对符合实名登记要求的车联网卡，应按照最小必要原则开通用户所需的语音、短信、流量功能；对未按要求提供真实身份信息的车联网卡，应及时关闭除紧急呼叫、应急救援等影响生命安全以外的车联网卡功能。（责任单位：各智能网联汽车生产企业、各基础电信企业）

 （二）加强智能网联汽车安全防护

**4.保障车辆网络安全。**各企业要加强整车网络安全架构设计。加强车内系统通信安全保障，强化安全认证、分域隔离、访问控制等措施，防范伪装、重放、注入、拒绝服务等攻击。加强车载信息交互系统、汽车网关、电子控制单元等关键设备和部件安全防护和安全检测。加强诊断接口（OBD）、通用串行总线（USB）端口、充电端口等的访问和权限管理。（责任单位：各智能网联汽车生产企业）

**5.落实安全漏洞管理责任。**各企业要落实《网络产品安全漏洞管理规定》有关要求，明确本企业漏洞发现、验证、分析、修补、报告等工作程序。发现或获知汽车产品存在漏洞后，应立即采取补救措施，并向工业和信息化部网络安全威胁和漏洞信息共享平台（https://www.nvdb.org.cn）报送漏洞信息。对需要用户采取软件、固件升级等措施修补漏洞的，应当及时将漏洞风险及修补方式告知可能受影响的用户，并提供必要技术支持。（责任单位：各智能网联汽车生产企业）

 （三）加强车联网网络安全防护

**6.加强车联网网络设施和网络系统安全防护能力。**各企业要严格落实网络安全分级防护和“三同步”工作要求，在网络系统的规划、建设、使用过程中，同步建设网络安全保障措施。加强网络设施和网络系统资产管理，合理划分网络安全域，加强访问控制管理，做好网络边界安全防护，采取防范木马病毒和网络攻击、网络侵入等危害车联网安全行为的技术措施。自行或者委托检测机构定期开展网络安全符合性评测和风险评估，及时消除风险隐患，并将测评及整改情况报省通信管理局、省经济和信息化厅。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**7.保障车联网通信安全。**各企业要建立车联网身份认证和安全信任机制，强化车载通信设备、路侧通信设备、服务平台等安全通信能力，采取身份认证、加密传输等必要的技术措施，防范通信信息伪造、数据篡改、重放攻击等安全风险，保障车与车、车与路、车与云、车与设备等场景通信安全。鼓励相关企业、机构接入工业和信息化部车联网安全信任根管理平台，协同推动跨车型、跨设施、跨企业互联互认互通。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**8.开展车联网安全监测预警。**各企业要建立网络安全监测预警机制和技术手段，鼓励接入省级车联网安全监测平台。各基础电信企业的移动恶意程序监测和处置技术手段要具备车联网监测和处置能力。各企业要对智能网联汽车、车联网服务平台及联网系统开展网络安全相关监测，及时发现网络安全事件或异常行为，并按照规定留存相关的网络日志不少于6个月。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**9.做好车联网安全应急处置。**各企业要建立网络安全应急响应机制，制定网络安全事件应急预案，定期自主开展应急演练，积极参与行业应急演练，及时处置安全威胁、网络攻击、网络侵入等网络安全风险。在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照《公共互联网网络安全突发事件应急预案》等规定向省通信管理局、省经济和信息化厅报告。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

**10.做好车联网网络安全防护定级备案。**各企业要按照《网络安全法》《通信网络安全防护管理办法》要求，对所属网络设施和系统开展网络安全防护定级工作，并在通信网络安全防护管理系统（www.mii-aqfh.com）进行备案。对新建网络设施和系统，应当在规划设计阶段确定网络安全防护等级。（责任单位：各基础电信企业、智能网联汽车生产企业、车联网服务平台运营企业）

（四）加强车联网服务平台安全防护

**11.加强平台网络安全管理。**各企业要采取必要的安全技术措施，加强智能网联汽车、路侧设备等平台接入安全，主机、数据存储系统等平台设施安全，以及资源管理、服务访问接口等平台应用安全防护能力，防范网络侵入、数据窃取、远程控制等安全风险。涉及在线数据处理与交易处理、信息服务业务等电信业务的，应向省通信管理局依法取得电信业务经营许可。认定为关键信息基础设施的，要落实《关键信息基础设施安全保护条例》有关规定，并按照国家有关标准使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。（责任单位：各车联网服务平台运营企业）

**12.加强在线升级服务（OTA）安全和漏洞检测评估。**各企业要建立在线升级服务软件包安全验证机制，采用安全可信的软件。开展在线升级软件包网络安全检测，及时发现产品安全漏洞。加强在线升级服务安全校验能力，采取身份认证、加密传输等技术措施，保障传输环境和执行环境的网络安全。加强在线升级服务全过程的网络安全监测和应急响应，定期评估网络安全状况，防范软件被伪造、篡改、损毁、泄露和病毒感染等网络安全风险。（责任单位：各智能网联汽车生产企业）

**13.强化应用程序安全管理。**各企业要建立车联网应用程序开发、上线、使用、升级等安全管理制度，提升应用程序身份鉴别、通信安全、数据保护等安全能力。加强车联网应用程序安全检测，及时处置安全风险，防范恶意应用程序攻击和传播。（责任单位：各车联网服务平台运营企业、智能网联汽车生产企业）

  （五）加强数据安全保护

**14.加强数据分类分级管理。**按照“谁主管、谁负责，谁运营、谁负责”的原则，各企业要建立数据管理台账，实施数据分类分级管理，制定重要数据清单，加强个人信息与重要数据保护。每年至少开展一次数据安全风险评估，强化隐患排查整改，并向省通信管理局、省经济和信息化厅报告。（责任单位：各智能网联汽车生产企业、车联网服务平台运营企业）

**15.提升数据安全技术保障能力。**各企业要采取合法、正当方式收集数据，针对数据全生命周期采取有效技术保护措施，防范数据泄露、毁损、丢失、篡改、误用、滥用等风险。各企业要强化数据安全监测预警和应急处置能力建设，提升异常流动分析、违规跨境传输监测、安全事件追踪溯源等水平；及时处置数据安全事件，向省通信管理局、省经济和信息化厅报告较大及以上数据安全事件，并配合开展相关监督检查，提供必要技术支持。（责任单位：各智能网联汽车生产企业、车联网服务平台运营企业）

**16.规范数据开发利用和共享使用。**各企业要合理开发利用数据资源，防范在使用自动化决策技术处理数据时，侵犯用户隐私权和知情权。明确数据共享和开发利用的安全管理和责任要求，对数据合作方数据安全保护能力进行审核评估，对数据共享使用情况进行监督管理。（责任单位：各智能网联汽车生产企业、车联网服务平台运营企业）

**17.强化数据出境安全管理。**各企业需向境外提供在中华人民共和国境内收集和产生的重要数据的，应当依法依规进行数据出境安全评估并向省通信管理局、省经济和信息化厅报备。（责任单位：各智能网联汽车生产企业、车联网服务平台运营企业）

四、进度安排

**（一）推进落实阶段（2021年11月至2022年6月底)。**各企业要对照工作要求，精心制定实施方案，推进各项工作落实。各企业要于2022年3月底前完成存量车联网相关网络和系统的定级备案，于2022年6月底前完成相关网络系统的网络安全符合性测评和风险评估，开展数据安全风险评估，及时报送相关情况。

**（二）督导检查阶段（2022年7月至2022年10月底)。**2022年7月至12月,省通信管理局组织对各企业相关网络和系统开展网络安全远程检测，会同省经济和信息化厅对各企业工作落实情况开展实地督导检查。

**（三）巩固提升阶段（2022年11月至长期)。**各相关企业要对车联网网络安全和数据安全工作进行梳理，认真查找存在的问题和不足，提炼好的经验做法，形成工作总结于2022年12月底前报省通信管理局、省经济和信息化厅。省通信管理局、省经济和信息化厅将指导各企业构建四川省车联网安全长效管理工作机制，持续提升车联网安全保障能力。

五、工作要求

**（一）加强组织领导。**各企业要充分认识新形势下车联网网络及数据安全工作的重要性，加强组织领导，明确工作责任部门和责任人，细化职责，层层落实。请各企业于2021年12月20日前将责任部门及联络人信息报省通信管理局、省经济和信息化厅。

**（二）强化责任落实。**各企业要按要求制定工作方案，进一步明确工作目标、细化任务和举措，加强安全自查和整改，狠抓安全责任落实。省通信管理局将视情况将相关工作纳入基础电信企业网络与信息安全责任考核以及电信企业网络安全“双随机”抽查。

**（三）加强信息报送。**各企业要对相关工作进行认真梳理总结，按要求将工作开展情况、存在的问题及薄弱环节、措施建议等报主管部门。对于工作落实情况较好的企业，将考核加分，在申报项目、争创试点中予以优先推荐。