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

各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司，有关智能网联汽车生产企业、车联网服务平台运营企业，有关标准化技术组织：

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。智能网联汽车是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与车、路、人、云端等智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶的新一代汽车。在产业快速发展的同时，车联网安全风险日益凸显，车联网安全保障体系亟须健全完善。为推进实施《新能源汽车产业发展规划（2021-2035年）》，加强车联网网络安全和数据安全管理工作，现将有关事项通知如下：

一、网络安全和数据安全基本要求

（一）落实安全主体责任。各相关企业要建立网络安全和数据安全管理制度，明确负责人和管理机构，落实网络安全和数据安全保护责任。强化企业内部监督管理，加大资源保障力度，及时发现并解决安全隐患。加强网络安全和数据安全宣传、教育和培训。

（二）全面加强安全保护。各相关企业要采取管理和技术措施，按照车联网网络安全和数据安全相关标准要求，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，确保数据处于有效保护和合法利用状态，保障车联网安全稳定运行。

二、加强智能网联汽车安全防护

（三）保障车辆网络安全。智能网联汽车生产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。

（四）落实安全漏洞管理责任。智能网联汽车生产企业要落实《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。

三、加强车联网网络安全防护

（五）加强车联网网络设施和网络系统安全防护能力。各相关企业要严格落实网络安全分级防护要求，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。

（六）保障车联网通信安全。各相关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。

（七）开展车联网安全监测预警。国家加强车联网网络安全监测平台建设，开展网络安全威胁、事件的监测预警通报和安全保障服务。各相关企业要建立网络安全监测预警机制和技术手段，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。

（八）做好车联网安全应急处置。智能网联汽车生产企业、车联网服务平台运营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，定期开展应急演练，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》等规定向有关主管部门报告。

（九）做好车联网网络安全防护定级备案。智能网联汽车生产企业、车联网服务平台运营企业要按照车联网网络安全防护相关标准，对所属网络设施和系统开展网络安全防护定级工作，并向所在省（区、市）通信管理局备案。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。各省（区、市）通信管理局会同工业和信息化主管部门做好定级备案审核工作。

四、加强车联网服务平台安全防护

（十）加强平台网络安全管理。车联网服务平台运营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。

（十一）加强在线升级服务（OTA）安全和漏洞检测评估。智能网联汽车生产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。

（十二）强化应用程序安全管理。智能网联汽车生产企业、车联网服务平台运营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。

五、加强数据安全保护

（十三）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，智能网联汽车生产企业、车联网服务平台运营企业要建立数据管理台账，实施数据分类分级管理，加强个人信息与重要数据保护。定期开展数据安全风险评估，强化隐患排查整改，并向所在省（区、市）通信管理局、工业和信息化主管部门报备。所在省（区、市）通信管理局、工业和信息化主管部门要对企业履行数据安全保护义务进行监督检查。

（十四）提升数据安全技术保障能力。智能网联汽车生产企业、车联网服务平台运营企业要采取合法、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。各相关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，向所在省（区、市）通信管理局、工业和信息化主管部门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。

（十五）规范数据开发利用和共享使用。智能网联汽车生产企业、车联网服务平台运营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。

（十六）强化数据出境安全管理。智能网联汽车生产企业、车联网服务平台运营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所在省（区、市）通信管理局、工业和信息化主管部门报备。各省（区、市）通信管理局会同工业和信息化主管部门做好数据出境备案、安全评估等工作。

六、健全安全标准体系

（十七）加快车联网安全标准建设。加快编制车联网网络安全和数据安全标准体系建设指南。全国通信标准化技术委员会、全国汽车标准化技术委员会等要加快组织制定车联网防护定级、服务平台防护、汽车漏洞分类分级、通信交互认证、数据分类分级、事件应急响应等标准规范及相关检测评估、认证标准。鼓励各相关企业、社会团体制定高于国家标准或行业标准相关技术要求的企业标准、团体标准。

特此通知。

工业和信息化部

2021 年 9 月 15 日