附件

关于加强车联网(智能网联汽车)网络安全工作的通知

（征求意见稿）

各省、自治区、直辖市工业和信息化主管部门、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，有关车联网运营企业、智能网联汽车生产企业：

为贯彻《中华人民共和国网络安全法》，落实《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）产业行动计划》，指导基础电信企业、车联网运营企业、智能网联汽车生产企业加强车联网（智能网联汽车）网络安全管理工作，加快提升网络安全保障能力，促进车联网（智能网联汽车）产业规范健康发展。现将有关事项通知如下。

一、加强车联网网络安全防护

（一）保护车联网网络设施和系统安全。落实企业网络安全主体责任，建立车联网网络安全管理制度和操作规程，确定网络安全负责人，定期开展符合性评测和风险评估，及时消除网络安全风险隐患。严格落实分级防护要求，加强网络设施和系统资产管理，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。

（二）保障车联网通信安全。建立企业车联网身份认证和安全信任机制，强化车与车、车与路、车与云、车与设备等场景安全通信能力建设，推动跨车型、跨设施、跨企业互联互认互通。加强商用密码应用，开展商用密码应用安全性评估。

（三）开展车联网安全监测预警。建立网络安全监测预警机制和技术手段，面向智能网联汽车、联网系统等，开展运行安全监测、流量与行为监测分析，及时发现预警安全状态异常、恶意软件传播、网络通信异常、网络攻击等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。

（四）做好车联网安全应急处置。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》向有关主管部门报告。

（五）做好车联网网络安全防护定级备案。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，并向省级电信主管部门备案。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。各省级电信主管部门会同工业和信息化主管部门做好定级备案审核工作。

二、加强平台安全防护

（一）加强平台网络安全管理。采取必要的安全技术措施，加强智能网联汽车、边缘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，以及微服务、资源管理、应用程序编程接口（API）访问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，要落实国家关于关键信息基础设施安全保护有关规定。

（二）加强 OTA 服务安全和漏洞检测评估。开展 OTA 服务及软件包网络安全检测，及时发现服务和产品安全漏洞。加强 OTA 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 OTA 服务全过程网络安全监测和应急响应，及时评估网络安全状况，防范软件被篡改、损毁、泄露和病毒感染等网络安全风险。

（三）强化应用程序安全管理。建立车联网（智能网联汽车）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、关键数据保护等安全能力。加强车联网（智能网联汽车）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。

三、保障数据安全

（一）加强数据安全管理。建立健全数据安全管理制度，建立完善权限管理、监测预警、应急响应、投诉受理等保障措施，明确责任部门和责任人，加强人员教育培训。建立数据资产管理台账，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。

（二）提升数据安全技术保障能力。坚持“最小必要”原则采集数据，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。强化数据安全监测预警能力建设，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，向省级电信主管部门、工业和信息化主管部门报告，并配合开展相关监督检查，提供必要技术支持。

（三）规范数据开发利用和共享使用。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，对数据合作方的资质和能力进行审核评估，对数据共享使用情况进行监督管理。

（四）强化数据出境安全管理。在中华人民共和国境内收集和产生的个人信息和重要数据应当依法在境内存储。因业务需要确需向境外提供数据的，应当通过数据出境安全评估并向省级电信、工业和信息化等有关主管部门报备。各省级电信主管部门会同工业和信息化主管部门做好数据出境备案、安全评估、监督检查等工作。

四、强化安全漏洞管理

（一）建立安全漏洞管理机制。落实国家关于网络产品安全漏洞管理有关规定，建立车联网（智能网联汽车）安全漏洞管理机制，明确漏洞发现、分析、修补等工作程序，加强漏洞管理资源保障投入，确保漏洞得到及时修补和合理披露。

（二）加强安全漏洞发现收集。加强漏洞风险的主动监测、风险评估、技术验证等能力建设。建立漏洞信息接收渠道并保持畅通，主动收集用户、上下游供应商、网络安全企业、研究机构等发现的漏洞信息，加强与漏洞收集平台的协同联动。鼓励建立漏洞奖励机制。

（三）强化安全漏洞协同处置。发现或获知本企业网络设施和业务系统、智能网联汽车产品存在漏洞后，应当立即采取补救措施，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。加强上下游产品或组件存在漏洞的协同处置。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，并提供必要的技术支持。

工业和信息化部

2021 年　月　日