

“铸盾车联” 2025 年车联网网络和数据安全专项行动任务清单

序号	2025 年重点任务			企业提报材料
一	网络和数据安全主体责任	1.落实网络安全和数据安全主体责任	各车联网企业应按照国家法律法规和标准规范要求，建立健全网络和数据安全管理机制和制度体系，明确组织架构、责任部门、管理负责人和工作责任人，落实网络和数据安全保障责任，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。处理重要数据的车联网企业应积极建立首席数据官制度。	-
二	车联网平台安全	2.加强车联网网络安全防护定级备案管理	各车联网企业应按照《车联网网络安全防护定级备案实施指南》等相关要求，依托全国车联网网络安全防护管理系统，对所属车联网服务平台、网络设施和系统定期开展网络安全防护定级工作，并向市通管局申请备案。	企业应提交《车联网网络安全防护定级报告》和《上海市车联网网络安全服务平台安全防护定级报告附件材料》。
		3.加强车联网网络安全符合性评测和风险评估管理	各车联网企业应按照《车联网服务平台网络安全防护要求》等相关要求，严格落实分级防护管理。同时按车联网安全相关评测、评估标准，自行或委托第三方机构开展符合性评测和安 全风险评估，并向市通管局报送。其中定级为三级及三级以上的车联网服务平台、网络设施和系统应当每年进行一次网络安全符合性评测和风险评估。定级为二级的车联网服务平台、网络设施和系统应当每两年进行一次。	企业在定级备案审核通过的 30 个工作日内完成评测评估工作，并提交《符合性评测报告》和《安全风险评估报告》。

序号	2025 年重点任务			企业提报材料
		4.开展车联网平台网络安全威胁通报	各车联网运营平台企业应及时落实整改并报告有关情况，采取安全技术措施加强安全防护，防范网络侵入、数据窃取等风险。	-
三	智能网联汽车产品安全	5.加强智能网联汽车产品网络安全保障管理	智能网联汽车产品生产企业应按照《汽车整车信息安全技术要求》等标准，加强整车及其关键零部件的网络和数据安全保障。相关智能网联汽车产品在上海市上市销售前或其网络功能有重要更新发布前，企业应自行或委托第三方机构对汽车整车、车载信息交互系统、T-Box、汽车网关等关键零部件开展安全检测。	-
		6.加强软件在线升级（OTA）安全保障管理	智能网联汽车产品生产企业应按照《汽车软件升级通用技术要求》等标准，加强软件在线升级管理，确保升级过程的安全性和合规性。在线升级软件在发布或更新前，企业应自行或委托第三方机构开展在线升级软件包网络安全检测。	-
		7.加强车联网应用程序网络安全保障管理	各车联网企业应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。在车联网应用程序发布或更新前，企业应自行或委托第三方机构开展车联网应用程序安全检测。	-

序号	2025 年重点任务			企业提报材料
四	车联网数据安全	8.加强车联网重要数据识别及目录备案管理	各车联网企业应按照《数据安全法》《网络安全法》《数据安全条例》和数据分类分级保护制度等相关要求，开展重要数据识别工作，形成并定期更新本企业重要数据目录。	(1)企业形成并定期更新重要数据目录，在7月31日前向市通管局备案。 (2)当重要数据条目数量或者存储总量等变化30%以上，或者其他备案内容发生重大变化时，企业应在三个月内向市通管局更新备案。
		9.加强车联网数据安全风险评估管理	各车联网企业应按照《数据安全法》《工业和信息化领域数据安全管理办法(试行)》等相关要求，自行或委托第三方机构每年对其重要数据处理活动至少开展一次数据安全风险评估，强化隐患排查整改。	企业在11月30日前向市通管局报送数据安全风险评估报告。
		10.加强车联网个人信息保护管理	各车联网企业应按照《个人信息保护法》《汽车数据安全管理若干规定(试行)》等相关要求，落实车联网个人信息保护和安全风险评估管理。涉及个人信息处理的车联网企业在处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息、其他对个人权益有重大影响的信息处理活动前，应自行或委托第三方机构进行个人信息保护影响评估。	企业在11月30日前向市通管局报送个人信息保护影响评估报告。

序号	2025 年重点任务			企业提报材料
		11.加强数据共享和出境安全管理	各相关车联网企业应明确数据共享和开发的利 用的安全管理责任和进行审核评估，并对数据共 据安全保护能力进行监督管理。需向境外提供中 使用情况进行监督。人民共和国境内收集和产 需向境外提供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。	企业需向境外提供中华人民共和国境内依 民的共和国境内的，应当依法依 规进行数据出境安全评估，报 并向市通管局报备，内容不 包含出境数据本身。
五	车联网安全 应急处置	12.加强车联网 网络和数据安全 事件应急处置管 理	各车联网企业应按照《工业和信息化领域数据 安全事件应急预案》《上海市公共互联网网络 安全突发事件应急预案》等相关要求，建立健全 安全网络和数据安全应急响应机制，制定网络 数据安全事件应急预案，强化网络和数据安全 事件分类分级处置能力，明确网络和数据安全 事件响应流程、职责分工、处置措施等。企业 应当每年至少组织开展一次应急演练，及时处 理安全威胁、网络攻击、数据安全风险等问题。	在发生危害网络安全事件或 较大及以上数据安全事件 时，企业应立即启动应 急预案，采取相应的补 救措施，并向市通管局报告。
六	车联网安全 漏洞管理	13.加强车联网 安全漏洞管理	各车联网企业应按照《网络产品安全漏洞管理 规定》等相关要求，明确本企业漏洞 发现、验证、分析、修补、报告等工作程序。	企业发现或获知车联网安 全漏洞后，应立即采取补 救措施，并向工业和信息化部 报告，同时向市通管局 报告，并通报漏洞信息。

序号	2025 年重点任务			企业提报材料
七	L3 及以上自动驾驶网络安全和数据安全	14.加强 L3 及以上自动驾驶功能网络安全保障管理	搭载自动驾驶功能的智能网联汽车生产企业和运营主体，在上海市行政区域内开展有条件自动驾驶、高度自动驾驶智能网联汽车道路测试、示范应用、示范运营、商业化运营活动前，应按照《关于加强智能网联汽车生产企业及产品准入管理的意见》《关于开展智能网联汽车准入和上路通行试点工作的通知》《上海市智能网联汽车测试与应用管理办法》等相关要求，自行或委托第三方机构对自动驾驶功能相关产品开展安全检测。	企业将自动驾驶功能网络安全检测报告向市通管局报备。
八	车联网网络安全和能力成熟度评估	15.试点开展车联网网络安全能力成熟度评估	车联网企业试点开展车联网网络安全能力成熟度评估工作，推动车联网企业在网络安全管理、数据全生命周期保护、技术防护能力等维度的成熟度提升。	-