附件

“铸盾车联”2026车联网网络和数据安全专项行动任务清单

序号	2026年重点任务			企业材料提报
一	网络和数据安全主体责任	1.落实网络和数据安全主体责任。	各车联网企业应按照相关法律法规和标准规范要求，完善网络和数据安全管理机制和制度体系，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。处理重要数据的企业应明确安全管理部门和数据全生命周期管理相关岗位职责，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《工业和信息化部网络安全管理局关于进一步做好车联网平台网络安全备案管理工作的通知》（工网安函〔2025〕935号）等要求，通过全国车联网网络安全防护管理系统完成所属网络设施和系统的定级备案工作。	（1）企业应在每年3月10日前完成上一年度备案信息的更新确认。 （2）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》。

序号	2026 年重点任务			企业材料提报
		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《车联网服务平台符合性评测实施指南》（T/SHV2X 2—2025）《车联网服务平台风险评估实施指南》（T/SHV2X 3—2025）等要求，严格落实与车联网平台级别相适应的安全防护措施，自行或委托第三方开展符合性评测和安全风险评估并报送市通管局。定级为三级及以上的网络设施和系统每年开展一次，定级为二级的网络设施和系统每两年开展一次。	企业应在 11 月 30 日前向市通管局报送符合性评测和风险评估报告。
		4.开展车联网平台网络安全威胁通报。	市通管局依托车联网平台网络安全威胁通报机制，定期对上海市车联网服务平台、网络设施和系统开展网络安全威胁检测与问题通报。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和数据安全保障管理。	智能网联汽车生产企业应按照《汽车整车信息安全技术要求》（GB 44495—2024）《汽车软件升级通用技术要求》（GB 44496—2024）等要求，加强整车及车载信息交互系统、T-Box、汽车网关等关键零部件的安全保障，规范软件在线升级管理。升级软件包发布或更新前，企业应自行或委托第三方开展安全检测。	-

序号	2026 年重点任务			企业材料提报
		6.加强车联网应用程序网络和数据安全保障管理。	各车联网企业应建立车联网应用程序开发、测试、上线、升级等安全管理制度，提升应用程序身份鉴别、代码安全、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。	-
四	车联网数据安全	7.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《汽车数据出境安全指引（2026 版）》（工信部联网安〔2026〕27 号）和数据分类分级保护制度等要求，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。
		8.加强车联网数据安全风险评估管理。	各车联网企业应按照《工业领域数据安全风险评估规范》（YD/T 6415—2025）或《电信领域数据安全风险评估规范》（YD/T 3956—2024）等要求，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，及时采取适当措施消除或降低评估中发现的风险隐患。	企业应在 11 月 30 日前向市通管局报送数据安全风险评估报告。

序号	2026 年重点任务			企业材料提报
		9.加强汽车数据安全报送管理。	开展重要数据处理活动的汽车数据处理者应按照相关要求，落实汽车数据安全管理工作。	汽车数据处理者应按要求向市通管局报送年度汽车数据安全管理情况报告。
		10.加强车联网个人信息保护管理。	各车联网企业应按照《信息安全技术 个人信息安全规范》（GB/T 35273—2020）等要求，落实车联网个人信息保护和安全风险评估管理，涉及《个人信息保护法》第五十五条情形的车联网企业在个人信息处理活动前，应自行或委托第三方机构进行个人信息保护影响评估。	企业应在 11 月 30 日前向市通管局报送个人信息保护影响评估报告。
		11. 加强汽车数据出境安全管理。	涉及数据出境的车联网企业应按照《汽车数据出境安全指引（2026 版）》（工信部联网安〔2026〕27 号）等要求，开展数据出境活动，做好汽车数据出境安全保护。	企业应向市通管局报备评估报告、评估结果、数据类型和接收方等信息，报备内容不包含出境数据本身。
		12.加强数据共享安全管理。	各车联网企业应建立数据合作方安全管理制度，对数据合作方数据安全保护能力进行审核评估，明确数据合作方的数据安全责任义务，对数据共享使用情况进行监督管理。	涉及重要数据共享的企业，每年应至少开展一次合作方审核，并在 11 月 30 日前将审核情况报送市通管局。

序号	2026 年重点任务			企业材料提报
五	车联网安全应急处置	13.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（试行）》（工信部网安〔2024〕214 号）《上海市公共互联网网络安全突发事件应急预案》等要求，建立健全网络和数据安全应急响应机制，制定网络和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，明确响应流程、职责分工、处置措施等。企业应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的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	14.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》（工信部联网安〔2021〕66 号）等要求，明确本企业漏洞发现、验证、分析、修补、报告等工作程序。对需要采取软件、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。市通管局定期开展漏洞通报和抽查工作，相关企业结合漏洞通报信息及时进行漏洞验证，并反馈漏洞验证和整改结果。	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网络安全威胁和漏洞信息共享平台报送以及市通管局报送漏洞信息。

序号	2026 年重点任务			企业材料提报
七	L3 及以上自动驾驶网络和数据安全	15.加强 L3 及以上自动驾驶功能网络和数据安全保障管理。	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《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》（工信部通装〔2021〕103 号）《关于开展智能网联汽车准入和上路通行试点工作的通知》（工信部联通装〔2023〕217 号）《上海市智能网联汽车测试与应用管理办法》（上海市人民政府令第 60 号）等要求，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。	企业应将自动驾驶功能网络安全检测报告向市通管局报备。
		16.加强自动驾驶网络安全监测预警。	搭载自动驾驶功能的智能网联汽车生产企业和运营主体应建立网络安全监测预警机制和技术手段，对智能网联汽车、自动驾驶云平台及联网系统开展网络安全监测，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。	-
八	车联网供应链数据安全认证及数据安全能力成熟度评估	17.鼓励开展车联网供应链数据安全认证及数据安全能力成熟度评估。	鼓励车联网企业对涉及重要数据的供应商实施供应链数据安全准入评估及现场核查、鼓励车联网企业开展数据安全能力成熟度评估工作，提升行业整体网络和数据安全防护能力。	-