2025 年护航新型工业化网络安全专项行动方案

为深入学习贯彻习近平总书记关于新型工业化的重要论述，全面贯彻落实中央经济工作会议精神和全国新型工业化推进大会部署，扎实推进 2025 年护航新型工业化网络安全专项行动（以下简称专项行动），进一步推动提升新型工业化网络安全保障能力，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，全面贯彻党的二十大和二十届二中、三中全会精神，锚定实现新型工业化这个关键任务，着眼实体经济和数字经济深度融合趋势，更好统筹发展和安全，坚持问题导向、目标导向、结果导向，突出重点管理、做优服务模式，以推动重点企业、重要系统、关键产品防护能力升级为核心，切实提高工业领域网络安全保障水平，着力支撑制造业高质量发展，为实现“十五五”良好开局奠定坚实基础。

二、工作目标

建立完善工业领域网络安全防护重点企业清单，深入实施工业互联网安全分类分级管理，面向不少于 800 家工业企业开展网络安全贯标达标试点，更新不少于 100 个车联网服务平台的定级备案，有效提高重点企业综合防护水平；深化工业控制系统网络安全评估，探索开展工业控制产品安全检测认证；组织全国范围新型工业化网络安全政策标准宣贯，

推动各地方宣贯工作覆盖属地不少于 20%的规上工业企业，切实增强工业领域网络安全意识和保障能力，以高水平网络安全护航制造业高质量发展。

三、重点任务

（一）突出重点管理，提高企业网络安全防护水平

1.推动分类分级扩面提质，梳理建立防护重点企业清单。

地方工业和信息化主管部门、通信管理局（以下统称地方主管部门）围绕原材料工业、装备工业、消费品工业和电子信息制造业等重点行业，结合制造业重点产业链高质量发展行动实施和地方产业发展规划实际，梳理属地关系国计民生和对重点产业链发展影响大（以在属地营业收入排名前 5%的规上工业企业为参考）的重点工业企业、工业互联网平台企业和标识解析企业，形成 2025 年工业领域网络安全防护重点企业清单。指导清单企业落实《工业互联网安全分类分级管理办法》，有序推动完成自主定级。地方主管部门开展企业定级核查，加强对定级不准确企业的科学指导，将定级为三级的企业名单报送工业和信息化部。（地方主管部门，有关企业）

2.聚焦重点企业防护提升，开展网络安全贯标达标试点。

工业和信息化部统筹组织工业互联网安全国家标准贯标工作，面向不少于 10 个省（区、市）开展贯标达标试点，推动试点企业完成自主定级、定级核查、分级防护、符合性评

测、安全整改等“五步走”工作，更高水平、更深程度引领重点企业网络安全保障能力建设。试点地方主管部门结合本年度分类分级管理工作，组织全部三级安全防护企业、行业龙头企业、数字化程度高的企业等60家以上重点企业开展试点，指导试点企业按照《工业互联网企业网络安全 第1部分：应用工业互联网的工业企业防护要求》《工业互联网企业网络安全 第2部分：平台企业防护要求》《工业互联网企业网络安全 第3部分：标识解析企业防护要求》国家标准，分类分级落实相适应的防护要求。鼓励各地方主管部门积极开展贯标工作，国家级专业机构加强宣标培训、达标评估等全环节服务，帮助企业逐项对标落实防护措施，服务企业网络安全能力达标跃升。（部网安局，地方主管部门，中国信通院、国家工信安全中心等专业机构，有关企业）

3.夯实优势产业安全基础，提升重要车联网平台安全防护能力。紧跟车路云网协同发展趋势，巩固提升车联网业务应用竞争优势，地方主管部门督促属地有关企业按照车联网网络安全防护定级备案实施要求，及时更新车联网平台定级结果和备案信息。指导属地有关企业根据车联网平台级别，采取相应的安全技术措施，定期开展网络安全符合性评测和风险评估，消除整改潜在风险隐患。（部网安局，地方主管部门，中国信通院等专业机构，有关汽车生产企业、车联网平台运营企业）

（二）聚焦关键环节，增强工业控制系统产品安全能力

4.组织开展工业控制系统网络安全评估。落实《工业控制系统网络安全防护指南》要求，面向重点行业企业，深化工业控制系统网络安全评估。通过企业自评估、现场核验等方式，结合系统实际应用场景，指导企业加强在用工业控制系统安全防护能力建设。结合评估实施情况，研究制定工业控制系统网络安全评估实施指南，明确评估程序、实施要点及方法，探索建立评估工作机制，切实提升工业控制系统网络安全防护水平。（部网安局，地方工业和信息化主管部门，中国信通院、国家工信安全中心等专业机构，有关企业）

5.推动重点工业控制产品网络安全检测认证。发布可编程逻辑控制器（PLC）安全技术等国家标准，加快推进分布式控制系统（DCS）等工业控制产品网络安全标准研制。面向非网络关键设备的重点工业控制产品，依托行业协会组织，制定检测认证工作方案，以自愿形式探索开展网络安全检测认证，推动形成检测产品名录，强化供给侧安全保障能力，提升工业控制产品安全水平。（部网安局，有关专业机构，有关企业）

（三）创新赋能模式，优化工业领域网络安全服务

6.服务重点产业链企业，统筹开展网络安全赋能工作。紧扣制造业重点产业链高质量发展行动，面向重点产业链企业，支持专业机构开展重要工业控制系统识别以及网络安全

现场诊断、风险监测、漏洞修复、通报处置等服务，推动提升重点产业链网络安全防护水平。地方主管部门加强企业网络安全风险在线监测、点对点威胁通报，发挥基础电信企业作用，帮助企业及时发现消除风险隐患，推动企业落实网络安全主体责任，提升重点产业链网络安全风险防范水平。（部网安局，地方主管部门，有关专业机构，有关企业）

7.聚焦安全保障需求，强化网络安全“护企惠企”。持续开展安全深度行，地方主管部门结合实际，加强典型案例、优质产品、解决方案等推广应用，壮大属地支撑服务力量，鼓励面向工业园区、企业开展网络安全诊断评估、赛事活动、人才培养等多样化服务。开展网络安全保险典型服务方案遴选，滚动更新典型服务方案目录，鼓励地方主管部门面向工业园区、工业供应链等打造网络安全保险服务新模式。（部网安局，地方主管部门，有关专业机构，有关企业）

8.全面提升安全认识，加强新型工业化网络安全宣贯。组织开展全国性新型工业化网络安全政策宣贯，深入宣贯工业领域网络安全政策标准，交流分享典型案例和经验做法。地方主管部门面向属地各市（区、县）主管部门网络安全工作负责人、重点工业企业安全管理和技术人员等，采取多种方式组织开展不少于1场省级工业领域网络安全专题宣贯活动，系统解读政策标准和工作要求。鼓励地方主管部门结合实际，扩大宣贯范围、丰富宣贯形式，切实提升企业网络安

全意识和能力。（部网安局，地方主管部门，有关专业机构，有关企业）

四、时间安排

（一）启动阶段（6月）。地方主管部门确定属地专项行动负责处室和人员，明确时间计划和安排，制定属地专项行动工作方案（模板见附件），于6月10日前报工业和信息化部（网络安全管理局）。

（二）推进阶段（7—10月）。地方主管部门加强统筹组织和实施保障，对照重点任务，逐项落实工作目标要求，推动各项工作有效有序落地。

（三）总结阶段（11月）。地方主管部门总结属地专项行动完成情况、经验成效、存在问题及下一步措施建议，形成专项行动总结报告，于11月28日前报工业和信息化部（网络安全管理局）。

五、工作要求

（一）加强组织领导。工业和信息化部统筹专项行动实施，推进重点任务落实，通过实地调研、座谈交流等方式，加大工作指导力度。地方主管部门要高度重视，将新型工业化网络安全纳入属地重点任务和有关规划，将网络安全作为制造业数字化转型等的基本要求一体推进，围绕达标评估、赋能服务等重点任务，加大政府采购服务、企业奖励补贴等支持力度。有关专业机构要做好技术支撑和服务保障。

（二）强化任务落实。地方工业和信息化主管部门、通信管理局要建立健全工作协同机制，根据职责分工分解落实工作，避免以偏概全，确保各项重点任务落到实处。

（三）开展总结推广。地方主管部门要加强工作举措、经验成效和创新做法的总结梳理，工业和信息化部将持续遴选护航新型工业化网络安全典型案例和成效突出地区，开展经验交流和成果通报，加大工作激励和宣传推广。

（四）加强风险防控。地方主管部门、有关专业机构等要切实做好风险管理，加强检测评估等工作全过程风险管控，在确保不影响企业生产运行和正常工作秩序前提下，稳妥有序推进各项工作。