工业和信息化部关于印发《工业控制系统信息安全行动计划（2018-2020年）》的通知

工信部信软[2017]316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，有关中央企业：

为贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》等文件精神，加快我国工业控制系统信息安全保障体系建设，提升工业企业工业控制系统信息安全防护能力，促进工业信息安全产业发展，制定《工业控制系统信息安全行动计划（2018-2020年）》。现印发你们，请结合实际，抓好贯彻落实。

附件：工业信息安全行动计划（2018-2020年）

工业和信息化部

2017年12月12日

附件

工业控制系统信息安全行动计划

（2018-2020年）

工业控制系统信息安全（以下简称工控安全）是实施制造强国和网络强国战略的重要保障。近年来，随着中国制造全面推进，工业数字化、网络化、智能化加快发展，我国工控安全面临安全漏洞不断增多、安全威胁加速渗透、攻击手段复杂多样等新挑战。为全面落实国家安全战略，提升工业企业工控安全防护能力，促进工业信息安全产业发展，加快我国工控安全保障体系建设，制定本行动计划。

一、总体要求

（一）指导思想

全面贯彻落实党的十九大精神，以习近平新时代中国特色社会主义思想为指引，坚持总体国家安全观，以落实企业主体责任为关键，紧紧围绕新时期两化深度融合发展需求，重点提升工控安全态势感知、安全防护和应急处置能力，促进产业创新发展，建立多级联防联动工作机制，为制造强国和网络强国战略建设奠定坚实基础。

（二）基本原则

坚持安全和发展同步推进。树立正确的网络安全观，坚持以安全保发展，以发展促安全，安全和发展并重。确保信息安全与信息化建设同步规划、同步建设、同步运行。

坚持落实企业主体责任。确立企业工控安全主体责任地位，强化责任意识，把工控安全作为工业生产安全的重要组成部分，将安全要求纳入企业生产、经营、管理各环节。

坚持因地制宜分类指导。准确把握工控安全在不同行业、不同地区的发展基础和特征，结合工控安全威胁的多样性和复杂性，分类别、分层次、分步骤精准施策。

坚持技术和管理并重。统筹技术防护与安全管理，充分运用先进技术提升工控安全防护能力，创新企业安全管理机制，全面落实安全管理制度。

（三）主要目标

到 2020 年，全系统工控安全管理工作体系基本建立，全社会工控安全意识明显增强。建成全国在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（一网一库三平台），态势感知、安全防护、应急处置能力显著提升。培育一批影响力大、竞争力强的龙头骨干企业，创建 3-5 个国家新型工业化产业示范基地（工业信息安全），产业创新发展能力大幅提高。

二、主要行动

（一）安全管理水平提升

落实企业主体责任。企业依据《中华人民共和国网络安全法》建立工控安全责任制，明确企业法人代表、经营负责人第一责任者的责任，组建管理机构，完善管理制度。贯彻落实《工业控制系统信息安全防护指南》安全要求，持续加大工控安全投入，落实防护技术改造和隐患治理专项经费，积极开展防护能力评估。

落实监督管理责任。工业和信息化部统筹制定工控安全政策标准，开展宣贯培训，定期组织全国检查评估，对纳入审查范围的工业控制系统产品与服务实施安全审查。地方工业和信息化主管部门加快工控安全地方性法规建设，建立重要工业控制系统目录清单，加强日常监督管理，安排专项资金推动地方监测、预警、应急等保障能力建设，持续完善地方工控安全保障体系。

（二）态势感知能力提升

建设全国工控安全监测网络。支持国家级工业信息安全技术机构持续完善主动监测、被动诱捕、威胁情报获取等工控安全在线监测手段，扩展工业控制系统资产识别种类，提高识别精准度和搜索效率。建设以国家工控安全在线监测平台为中心，涵盖省级重要节点的监测网络，实现对全国重要工业控制系统运行状态、风险隐患的实时感知、精准研判和科学决策。

实施信息共享工程。鼓励行业主管部门、企业、科研院所、联盟协会等机构和个人积极参与信息共享工作，建立共享清单，明确共享内容，推动形成政府引导、企业主体、社会参与、利益共享的工作机制。充分利用云计算、大数据等技术手段，建设国家工控安全信息共享平台，实现信息的安全、可靠、及时共享。

（三）安全防护能力提升

加强防护技术研究。支持建设工控安全靶场、仿真测试等共性技术平台，研发工控安全防护技术工具集，加强分区隔离、安全交换、协议管控等关键技术攻关。开展防护能力建设试点示范，形成可复制、可推广的安全防护整体解决方案。探索工业云、工业大数据等新兴应用的安全架构设计，开展工业互联网安全防护技术研究和创新。

建立健全标准体系。制定工控安全分级、安全要求、安全实施、安全测评类标准，加快工控安全防护能力评估、工业控制系统设备产品安全、工业互联网平

台安全等急用先行标准的发布和应用，鼓励企业、科研院所、行业组织等参与国际标准化工作。

（四）应急处置能力提升

开展信息通报预警。制定《工业信息安全信息报送与通报管理办法》，建立信息通报员、日常信息通报、应急信息通报、风险预警等制度。建设工控安全信息通报预警平台，及时发布风险预警信息，跟踪风险防范工作进展，形成快速高效、各方联动的信息通报预警体系。

建设国家应急资源库。按照《国家网络安全事件应急预案》总体要求，支持国家级工业信息安全技术机构建设应急资源库，实现信息采集、辅助决策、预案演练等功能。在突发工业信息安全事件时，支撑行业主管部门协调技术专家和专业队伍对事件开展分析研判，并调动相关应急资源及时有效的开展处置工作。

（五）产业发展能力提升

培育龙头骨干企业。面向工控安全领域产业发展需求，加快培育一批技术水平高、业务规模大、竞争能力强的工业控制系统生产企业和安全服务商，支持龙头骨干企业突破核心技术，研发关键产品、提高服务能力、创新商业模式，联合工业企业开展优秀产品及解决方案示范，推动行业应用。

创建国家新型工业化产业示范基地（工业信息安全）。选择工业基础雄厚、产业链条完备、聚集效应明显的地区建设国家新型工业化产业示范基地（工业信息安全）。围绕工业控制系统技术研发、应用示范、产融合作、人才培养等关键环节，探索产业发展路径，促进产业集聚发展，发挥先行先试和示范带动作用。

三、保障措施

（一）加强组织协调

在国家制造强国建设领导小组统一领导下，加强工控安全保障体系重大决策、重大工程和重大问题的统筹协调，全面落实行动计划各项任务。各地工业和信息化主管部门要加强本地区统筹管理，做好行动计划的贯彻落实和组织保障。

（二）加大政策支持

坚持政府引导和市场运作相结合，充分调动社会力量支持工控安全保障体系建设。支持有条件的地方设立专项，加大对工控安全基础设施建设、关键技术验证测试平台建设、产业创新发展的支持力度。利用国家政策性信贷资金支持工业信息安全产业示范基地建设。

（三）加快人才培养

鼓励工业企业加强与院校合作，联合培养工控安全专业人才。打造国家工控安全高端智库，为工控安全战略部署、规划制定、决策咨询、重大问题提供智力支持和技术支撑，培养一支门类齐全、技术精湛的工控安全专业人才队伍。

（四）鼓励社会参与

充分发挥行业协会、产业联盟等中介组织的积极作用，支持开展技术研发、技能竞赛、标准推广、公共服务、国际合作等工作，促进技术交流、加强信息沟通，形成政产学研用高效联动的发展格局。