**《工业控制系统信息安全事件应急管理工作指南》解读**

发布时间：2017-06-15  来源：信息化和软件服务业司

为进一步贯彻落实《国务院关于深化制造业与互联网融合发展的指导意见》，依据《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》，工业和信息化部近日印发了《工业控制系统信息安全事件应急管理工作指南》（以下简称《指南》），旨在加强工业控制系统信息安全（以下简称“工控安全”）事件应急管理，提高工控安全事件应急处置能力，预防和减少工控安全事件造成的损失和危害，保障工业生产正常运行。

一、《指南》的出台背景

随着两化融合的不断深入，以及物联网、云计算和大数据等新一代信息技术的快速发展，工业控制系统智能化、网络化趋势日渐明显，病毒、木马等威胁向工业控制系统持续扩散。近年来，工控安全事件频频发生，工控安全漏洞数量持续增长，工业控制系统面临着日益严峻的安全形势。国家“十三五”规划《纲要》、网络强国、中国制造2025及“互联网+”等一系列战略部署的推进实施，对我国工控安全保障工作提出了更高的要求，迫切需要快速提升工控安全保障水平和事件应急处置能力，更好的支撑经济社会健康有序发展，维护国家安全。

二、总体考虑

密切结合工控安全事件应急工作实际，以防范重大工控安全事件为重点，厘清工业和信息化部、地方工业和信息化主管部门、技术支撑队伍和企业职责，加强工控安全事件应急管理和组织协调，提升工控安全事件应急处置能力。

（一）目的意义

**一是建立健全工控安全事件应急工作机制。**依据《国家网络安全事件应急预案》制定《指南》，进一步完善工控安全事件应急制度，形成有效的工控安全应急工作机制，为工控安全事件应急管理与处置工作提供依据与方法。

**二是提升工控安全事件应急处置能力。**《指南》明确了工控安全事件应急工作的组织机构和职责，确定了工控安全事件的监测通报、处置流程和具体措施，提出了应急队伍、专家组、物资和经费保障等应急力量和应急资源方面的要求，为应急处置工作提供行动指南。

**三是完善工控安全管理体系。**《指南》的研究制定和宣贯落实，与颁布的《工业控制系统信息安全防护指南》和正在编制的《工业控制系统信息安全防护评估工作管理办法》共同构建了工控安全管理体系。文件中提出的安全要求和管理方法覆盖了工业控制系统规划、设计、建设、运行、维护等全生命周期，为加强工控安全管理奠定了坚实基础。

（二）编制原则

**政府指导、企业主体。**政府通过完善政策措施、加强监督管理，指导企业树立工控安全主体责任意识，督促企业将工控安全作为生产安全的重要组成部分，做好工控安全应急相关工作，加快提升工控安全事件应急能力。

**预防为主、平战结合。**按照系统化、科学化管理思想，加强工控安全监测与风险预判，及时掌握工控安全态势，畅通信息传输渠道，充分发挥各方力量，将预防与消减有机结合，积极做好工控安全事件的预防和消减工作。

**快速反应、科学处置。**建立感知快、研判快、处置快、消减快的工控安全快速反应体系，不断强化工控安全事件应急队伍的整体应急水平和快速反应能力，科学管理、指挥有力，妥善处置工控安全事件。

三、《指南》的管理要求

《指南》对工控安全风险监测、信息报送与通报、应急处置、敏感时期应急管理等工作提出了一系列管理要求，明确了责任分工、工作流程和保障措施。

（一）加强风险监测

风险监测是掌握工控安全事件、感知风险动向的基础性工作。《指南》要求国家工业信息安全发展研究中心等技术机构、地方工业和信息化主管部门和工业企业做好风险监测工作。其中，国家工业信息安全发展研究中心等技术机构负责组织开展全国工控安全风险监测、预警通报等工作，地方工业和信息化主管部门负责组织开展本地区工控安全风险监测工作，工业企业组织开展本单位工控安全风险监测工作。

（二）开展信息报送与通报

信息报送与通报是帮助工控安全应急相关部门及时了解风险及事件全貌的重要途径。《指南》明确指出，地方工业和信息化主管部门、工业企业在开展风险监测的同时，要及时将重要监测信息报国家工业信息安全发展研究中心。国家工业信息安全发展研究中心负责汇总、整理和研判，并将结果报工业和信息化部。针对影响范围大、危害程度深的风险信息，工业和信息化部及时向有关行业、地区、企业通报。此外，对于可能超出本地区应对能力范围的安全风险和事件信息，地方工业和信息化主管部门应及时向工业和信息化部报告。

（三）做好应急处置

工控安全事件应急处置是应急工作的重中之重，做好工控安全应急处置对于维护国家安全、社会秩序、经济建设和公众利益都具有举足轻重的意义。对于工控安全应急处置工作，《指南》明确了以下几方面要求：**一是工业企业应积极开展先期处置。**对于可能或已经发生工控安全事件时，工业企业应采取科学有效方法及时施救，力争将损失降到最小，尽快恢复受损工业控制系统的正常运行。**二是重点做好应急处置中的信息报送。**应急处置过程中，地方工业和信息化主管部门和工业企业应及时报告事态发展变化情况和事件处置进展情况。**三是必要时工业和信息化部将组织现场处置。**必要时，工业和信息化部将派出工作组赴现场，指挥应急处置工作，并协调应急技术机构提供技术支援。**四是应急结束后及时开展总结评估。**《指南》要求，应急工作结束后，相关工业企业应做好事件分析总结工作，并按时上报。

（四）保障措施

《指南》要求，建立覆盖工业和信息化部、地方工业和信息化主管部门、工业企业三个不同层次的预案体系，促进工控安全应急管理工作规范化、制度化；通过定期组织开展应急演练，提高应对工控安全事件的技术能力；通过建立国家工控安全应急专家组和地方工控安全应急专家组，支持工控安全应急技术机构、基础平台建设，提升应急处置基础能力。

此外，《指南》还强调了国家重要活动、会议等重要敏感时期的应急管理要求，明确工业和信息化部做好应急指导，地方工业和信息化主管部门和工业企业加强风险监测、做好信息报送和应急值守等，确保重要敏感时期工业控制系统安全、平稳运行。