

# 广东省经济和信息化委员会

---

粤经信融合函〔2017〕20号

## 广东省经济和信息化委转发工业控制系统 信息安全事件应急管理工作的通知

各地级以上市经济和信息化主管部门，顺德区经济和科技促进局：

为认真贯彻落实《中华人民共和国网络安全法》和《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号）精神，工业和信息化部印发了《工业控制系统信息安全事件应急管理工作的指南》（工信部信软〔2017〕122号）。现将工作指南转给你们，请根据该指南要求，指导本地区开展工控安全应急管理工作，制定本级工控安全事件应急预案，对于可能发生或已经发生的工控安全事件应及时向我委报告事态进展及处置情况。

  
广东省经济和信息化委  
2017年6月26日

（联系人：刘坤东、李尧，联系电话：13902491735、  
18688380026，邮箱：gdgkaq@163.com）

---

# 工业和信息化部文件

工信部信软〔2017〕122号

---

## 工业和信息化部关于印发《工业控制系统信息安全事件应急管理工作指南》的通知

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《中华人民共和国网络安全法》《国务院关于深化制造业与互联网融合发展的指导意见》（国发〔2016〕28号），指导做好工业控制系统信息安全事件应急管理相关工作，保障工业控制系统信息安全，制定《工业控制系统信息安全事件应急管理工作指南》，现印发你们。

工业和信息化部指导和管理全国工业控制系统信息安全应急

工作，并根据实际情况对指南进行修订。地方工业和信息化主管部门根据工业和信息化部统筹安排，指导和管理本行政区域内的工业控制系统信息安全应急工作。

特此通知。



(联系电话：010—68208171)

# 工业控制系统信息安全事件应急管理工作指南

## 第一章 总 则

第一条 为加强工业控制系统信息安全（以下简称工控安全）应急工作管理，建立健全工控安全应急工作机制，提高应对工控安全事件的组织协调和应急处置能力，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，维护国家经济安全和人民生命财产安全，依据《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》以及《国务院关于深化制造业与互联网融合发展的指导意见》等法规政策，制定本指南。

第二条 本指南适用于工业和信息化主管部门、工业企业开展工控安全应急管理工作。

第三条 工控安全事件是指由于人为、软硬件缺陷或故障、自然灾害等原因，对工业控制系统、工业控制系统数据造成或者可能造成严重危害，影响正常工业生产的事件。

第四条 坚持政府指导、企业主体，坚持预防为主、平战结合，坚持快速反应、科学处置，充分发挥各方力量，共同做好工控安全事件的预防和处置工作。

## 第二章 组织机构与职责

第五条 工业和信息化部指导地方工业和信息化主管部

门、应急技术机构、工业企业做好工控安全应急管理工作。

**第六条** 地方工业和信息化主管部门负责指导本地区工控安全应急管理工作。

**第七条** 工控安全应急技术机构负责具体开展工控安全风险监测、态势研判、威胁预警、事件处置等工作。

**第八条** 工业企业负有工控安全主体责任，应建立健全工控安全责任制，负责本单位工控安全应急管理工作，落实人财物保障。

### **第三章 工作机制**

**第九条** 工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业等建立工控安全联络员机制，指定工控安全应急工作联络员，报工业和信息化部备案，联络员和联络方式发生变化时需及时报工业和信息化部。工业和信息化部根据工作需要组织召开联络员会议。

**第十条** 地方工业和信息化主管部门指导本地区应急技术机构、工业企业建立工控安全应急值守机制，实行领导带班、专人值守工作制度，做好工控安全风险、威胁、事件信息日常监测和报告工作。应急响应状态下，实行“7×24”小时值守，加强信息监测、收集与研判，做好信息跟踪报告。

### **第四章 监测通报**

**第十一条** 工业和信息化部指导国家工业信息安全发展研究中心等技术机构，组织开展全国工控安全风险监测、预

警通报等工作，提升情报搜集、态势分析、风险评估和信息共享能力。

地方工业和信息化主管部门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。

**第十二条** 地方工业和信息化主管部门、工业企业定期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；针对可能超出本地区应对能力范围的安全风险和事件信息，及时上报，必要时工业和信息化部协调应急技术机构提供支持。

**第十三条** 工业和信息化部对可能影响我国工业控制系统的重大漏洞和风险，及时向有关行业、地区和工业企业发布情况通报。

## **第五章 敏感时期应急管理**

**第十四条** 在国家重要活动、会议等敏感时期，工业和信息化部指导地方工业和信息化主管部门、应急技术机构、工业企业开展工控安全事件预防和应急管理工作。

**第十五条** 地方工业和信息化主管部门、工业企业加强工控安全监测和风险研判，对可能造成重大影响的风险和事件信息应及时上报，必要时实行24小时零报告制度。重点单位、重要部位实施24小时值守，保持通信联络畅通。相

关工业企业应加强对工业控制系统的巡检巡查，原则上不在敏感时期对工业控制系统进行调整或升级。

## 第六章 应急处置

第十六条 对于可能发生或已经发生的工控安全事件，工业企业应立即开展应急处置，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。当事发工业企业应急处置力量不足时，可请求上级主管部门协调应急技术机构提供支援。

第十七条 有关地方工业和信息化主管部门和工业企业应及时向工业和信息化部报告事态发展变化情况和事件处置进展情况。报告信息一般包括以下要素：事件涉及的工业控制系统名称及运营管理单位、时间、地点、原因、来源、类型、性质、危害、影响范围、发展趋势、处置措施等。

第十八条 工业和信息化部指导、督促事发企业开展应急处置工作，必要时派出工作组赴现场指挥协调应急处置工作，协调应急技术机构提供技术支援。

第十九条 应急处置结束、系统恢复运行后，相关工业企业要尽快消除事件造成的不良影响，做好事件分析总结工作，总结报告应在 30 天内以书面形式报工业和信息化部。

第二十条 对于工控安全事件性质、起因、范围、损失等，工业和信息化主管部门和相关人员应做好舆论宣传和引导工作。

## 第七章 保障措施

第二十一条 工业和信息化部、地方工业和信息化主管部门、工业企业制定本级工控安全事件应急预案，定期组织应急演练。

第二十二条 工业和信息化部建立国家工控安全应急专家组，为工控安全应急管理提供技术咨询和决策支持。地方工业和信息化主管部门建立本地区工控安全应急专家组，充分发挥专家在应急管理中的作用。

第二十三条 加强对工控安全事件应急装备和工具的储备，及时调整、升级软硬件工具，建设完善工控安全事件应急技术服务平台，不断增强应急技术支撑能力。

第二十四条 各有关部门应积极利用现有政策和资金渠道，申请新增预算，支持工控安全应急技术机构建设、专家队伍建设、基础平台建设、技术研发、应急演练、物资保障等，为工控安全应急管理工作提供必要的经费支持。

第二十五条 本指南自 2017 年 7 月 1 日起施行。

---

抄送：国家工业信息安全发展研究中心。

---

工业和信息化部办公厅

2017年6月6日印发

---



公开方式：依申请公开

抄送：工业和信息化部电子第五研究所。