工业和信息化部文件

工信部协〔2011〕451号

关于加强工业控制系统信息安全管理的通知

各省、自治区、直辖市人民政府，国务院有关部门，有关国有大型企业：

工业控制系统信息安全事关工业生产运行、国家经济安全和人民生命财产安全，为切实加强工业控制系统信息安全管理，经国务院同意，现就有关事项通知如下：

一、充分认识加强工业控制系统信息安全管理的重要性和紧迫性

数据采集与监控（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器（PLC）等工业控制系统广泛运用于工业、能源、交通、水利以及市政等领域，用于控

制生产设备的运行。一旦工业控制系统信息安全出现漏洞，将对工业生产运行和国家经济安全造成重大隐患。随着计算机和网络技术的发展，特别是信息化与工业化深度融合以及物联网的快速发展，工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件，以各种方式与互联网等公共网络连接，病毒、木马等威胁正在向工业控制系统扩散，工业控制系统信息安全问题日益突出。2010 年发生的“震网”病毒事件，充分反映出工业控制系统信息安全面临着严峻的形势。与此同时，我国工业控制系统信息安全管理工作中仍存在不少问题，主要是对工业控制系统信息安全问题重视不够，管理制度不健全，相关标准规范缺失，技术防护措施不到位，安全防护能力和应急处置能力不高等，威胁着工业生产安全和社会正常运转。对此，各地区、各部门、各单位务必高度重视，增强风险意识、责任意识和紧迫感，切实加强工业控制系统信息安全管理。

二、明确重点领域工业控制系统信息安全管理要求

加强工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。各地区、各部门、各单位要结合实际，明确加强工业控制系统信息安全管理的重点领域和重点环节，切实落实以下要求。

（一）连接管理要求。

1. 断开工业控制系统同公共网络之间的所有不必要连接。

2. 对确实需要的连接，系统运营单位要逐一进行登记，采取设置防火墙、单向隔离等措施加以防护，并定期进行风险评估，不断完善防范措施。

3. 严格控制在工业控制系统和公共网络之间交叉使用移动存储介质以及便携式计算机。

（二）组网管理要求。

1. 工业控制系统组网时要同步规划、同步建设、同步运行安全防护措施。

2. 采取虚拟专用网络（VPN）、线路冗余备份、数据加密等措施，加强对关键工业控制系统远程通信的保护。

3. 对无线组网采取严格的身份认证、安全监测等防护措施，防止经无线网络进行恶意入侵，尤其要防止通过侵入远程终端单元（RTU）进而控制部分或整个工业控制系统。

（三）配置管理要求。

1. 建立控制服务器等工业控制系统关键设备安全配置和审计制度。

2. 严格账户管理，根据工作需要合理分类设置账户权限。

3. 严格口令管理，及时更改产品安装时的预设口令，杜绝弱口令、空口令。

4. 定期对账户、口令、端口、服务等进行检查，及时清理不必要的用户和管理员账户，停止无用的后台程序和进程，关闭

无关的端口和服务。

（四）设备选择与升级管理要求。

1. 慎重选择工业控制系统设备，在供货合同中或以其他方式明确供应商应承担的信息安全责任和义务，确保产品安全可控。

2. 加强对技术服务的信息安全管理，在安全得不到保证的情况下禁止采取远程在线服务。

3. 密切关注产品漏洞和补丁发布，严格软件升级、补丁安装管理，严防病毒、木马等恶意代码侵入。关键工业控制系统软件升级、补丁安装前要请专业技术机构进行安全评估和验证。

（五）数据管理要求。

地理、矿产、原材料等国家基础数据以及其他重要敏感数据的采集、传输、存储、利用等，要采取访问权限控制、数据加密、安全审计、灾难备份等措施加以保护，切实维护个人权益、企业利益和国家信息资源安全。

（六）应急管理要求。

制定工业控制系统信息安全应急预案，明确应急处置流程和临机处置权限，落实应急技术支撑队伍，根据实际情况采取必要的备机备件等容灾备份措施。

三、建立工业控制系统安全测评检查和漏洞发布制度

（一）加强重点领域工业控制系统关键设备的信息安全测评工作。全国信息安全标准化技术委员会抓紧制定工业控制系统关

键设备信息安全规范和技术标准，明确设备安全技术要求。重点领域的有关单位要请专业技术机构对所使用的工业控制系统关键设备进行安全测评，检测安全漏洞，评估安全风险。工业和信息化部会同有关部门对重点领域使用的工业控制系统关键设备进行抽检。

（二）建立工业控制系统信息安全检查制度。工业控制系统运营单位要从实际出发，定期组织开展信息安全检查，排查安全隐患，堵塞安全漏洞。工业和信息化部适时组织专业技术力量对重点领域工业控制系统信息安全状况进行抽查，及时通报发现的问题。

（三）建立信息安全漏洞信息发布制度。开展工业控制系统信息安全漏洞信息的收集、汇总和分析研判工作，及时发布有关漏洞、风险和预警信息。

四、进一步加强工业控制系统信息安全工作的组织领导

各地区、各部门、各单位要将工业控制系统信息安全管理作为信息安全工作的重要内容，按照谁主管谁负责、谁运营谁负责、谁使用谁负责的原则，建立健全信息安全责任制。各级政府工业和信息化主管部门要加强对工业控制系统信息安全工作的指导和督促检查。有关行业主管或监管部门、国有资产监督管理部门要加强对重点领域工业控制系统信息安全管理工作的指导监督，结合行业实际制定完善相关规章制度，提出具体要求，并加强督促检查确保落到实处。有关部门要加快推动工业控制系统信

息安全防护技术研究和产品研制，加大工业控制系统安全检测技术和工具研发力度。国有大型企业要切实加强工业控制系统信息安全管理的领导，健全工作机制，严格落实责任制，将重要工业控制系统信息安全责任逐一落实到具体部门、岗位和人员，确保领导到位、机构到位、人员到位、措施到位、资金到位。

二〇一一年九月二十九日

工业和信息化部办公厅　　2011年9月29日印发