广东省经济和信息化委员会

粤经信融合函〔2017〕8号

广东省经济和信息化委关于开展2017年工业控制系统信息安全检查工作的通知

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：

根据工业和信息化部办公厅《关于开展2017年工业控制系统信息安全检查工作的通知》（工信厅信软函〔2017〕194号）的要求，请你们组织本地区认真开展自查工作，于5月19日前将自查情况通过电子邮件方式反馈我委（制造业与互联网融合发展处）。

附件：工业和信息化部办公厅关于开展2017年工业控制系统信息安全检查工作的通知（工信厅信软函〔2017〕194号）

广东省经济和信息化委

2017年5月5日

（联系人：刘坤东，联系电话：020-8313 3375、13902491735，邮箱：ronghefazhan@163.com）

附件

工业和信息化部办公厅

工信厅信软函〔2017〕194号

工业和信息化部办公厅关于开展2017年工业控制系统信息安全检查工作的通知

各省、自治区、直辖市工业和信息化主管部门，各有关单位：

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》（国发〔2016〕28号）文件要求，推动《工业控制系统信息安全防护指南》落地实施，做好国家重大活动期间工业控制系统信息安全服务，加强对工业企业工业控制系统信息安全工作的指导和监督，我部将于2017年4月至6月开展工业控制系统信息安全检查工作。

请各地工业和信息化主管部门根据要求（详见附件）做好本地区自查工作，并于5月31日前将自查情况反馈部（信息化和软件服务业司）。我部将组织专业技术队伍对相关单位开展安全

抽查和深度核查，具体工作安排另行通知。

附件：工业控制系统信息安全自查表

工业和信息化部办公厅

2017年4月6日

（联系电话：010—68208171）

附件

工业控制系统信息安全自查表

填 表 说 明

一、组成结构

本表包含三个分表：

（1）工业控制系统信息安全检查情况汇总表

（2）工业控制系统运营单位基本情况表

（3）工业控制系统信息安全自查表

二、填写对象

各分表填写责任人如下：

（1）工业控制系统信息安全检查情况汇总表：由各地工业和信息化主管部门指定专人负责汇总填写。

（2）工业控制系统运营单位基本情况表：由各工业控制系统运营单位指定专人负责填写。

（3）工业控制系统信息安全自查表：由工业控制系统运营单位的各工业控制系统负责人填写。

表 1　工业控制系统信息安全检查情况汇总表

<table>
<tr><td colspan="2">省份名称</td><td colspan="3"></td></tr>
<tr><td>基本情况</td><td colspan="4">重要工业控制系统[1]运营单位总数：_____家
重要工业控制系统总数：_____套</td></tr>
<tr><td rowspan="20">系统构成情况</td><td>类型</td><td>设备</td><td>国内品牌</td><td>国外品牌</td></tr>
<tr><td rowspan="7">工业生产控制设备</td><td>可逻辑编程控制器（PLC）</td><td>台</td><td>台</td></tr>
<tr><td>分布式控制系统（DCS）</td><td>台</td><td>台</td></tr>
<tr><td>远程终端设备（RTU）</td><td>台</td><td>台</td></tr>
<tr><td>数控机床</td><td>台</td><td>台</td></tr>
<tr><td>工业机器人</td><td>台</td><td>台</td></tr>
<tr><td>智能仪表</td><td>台</td><td>台</td></tr>
<tr><td>其它</td><td>台</td><td>台</td></tr>
<tr><td rowspan="4">工业网络通信设备</td><td>工业交换机</td><td>台</td><td>台</td></tr>
<tr><td>工业路由器</td><td>台</td><td>台</td></tr>
<tr><td>串口服务器</td><td>台</td><td>台</td></tr>
<tr><td>其它</td><td>台</td><td>台</td></tr>
<tr><td rowspan="4">工业主机设备</td><td>工业主机[2]</td><td>台</td><td>台</td></tr>
<tr><td>组态软件&数据采集与监控系统（SCADA）软件</td><td>套</td><td>套</td></tr>
<tr><td>工业数据库</td><td>套</td><td>套</td></tr>
<tr><td>其它</td><td>台</td><td>台</td></tr>
<tr><td rowspan="4">工业生产信息系统</td><td>制造执行系统（MES）</td><td>套</td><td>套</td></tr>
<tr><td>ERP 管理系统</td><td>套</td><td>套</td></tr>
<tr><td>工业云</td><td>套</td><td>套</td></tr>
<tr><td>其它</td><td>套</td><td>套</td></tr>
<tr><td rowspan="4">工业网络安全设备</td><td>工业防火墙</td><td>台</td><td>台</td></tr>
<tr><td>工业网闸</td><td>台</td><td>台</td></tr>
<tr><td>主机安全防护设备</td><td>台</td><td>台</td></tr>
<tr><td>其它</td><td>台</td><td>台</td></tr>
<tr><td>安全软件选择与管理情况</td><td colspan="4">1、安装防病毒软件或应用程序白名单软件的重要工业控制系统数量：_____套
2、病毒库或白名单规则及时更新的重要工业控制系统数量：_____套
3、定期对工业控制系统进行查杀的重要工业控制系统数量：_____套
4、已建立防病毒和恶意软件入侵管理机制的重要工业控制系统数量：_____套</td></tr>
<tr><td>配置和补丁管理情况</td><td colspan="4">1、已建立工业控制网络安全配置策略的重要工业控制系统数量：_____套
2、已建立工业主机安全配置策略的重要工业控制系统数量：_____套
3、已建立工业控制设备安全配置策略的重要工业控制系统数量：_____套
4、已建立工业控制系统配置清单的重要工业控制系统数量：_____套
5、定期对配置清单进行更新和维护的重要工业控制系统数量：_____套
6、及时修复重大工控安全漏洞的重要工业控制系统数量：_____套</td></tr>
</table>

边界安全防护情况	1、直接与企业网连接的重要工业控制系统数量：_____套 2、直接与互联网连接的重要工业控制系统数量:_____套 3、对工业控制系统进行安全区域划分的重要工业控制系统数量：_____套 4、对工业控制系统安全区域实施逻辑隔离的重要工业控制系统数量：_____套
物理和环境安全防护情况	1、已明确划分重点物理安全防护区域并建立物理安全防护措施的重要工业控制系统数量：_____套 2、拆除或封闭工业主机上不必要外设接口的重要工业控制系统数量：_____套 3、使用外设安全管理技术手段管理外设接口的重要工业控制系统数量：_____套
身份认证情况	1、使用身份认证管理手段的重要工业控制系统数量：_____套 2、以最小特权原则分配账户权限的重要工业控制系统数量：_____套 3、未使用默认口令或弱口令的重要工业控制系统数量：_____套 4、定期更新口令的重要工业控制系统数量：_____套
远程访问安全情况	1、面向互联网开通 HTTP、FTP 等网络服务的重要工业控制系统数量：_套 2、使用数据单向访问控制等策略进行安全加固的重要工业控制系统数量：____套 3、使用 VPN 等远程接入方式的重要工业控制系统数量：_____套 4、保留工业控制系统相关访问日志的重要工业控制系统数量：_____套
安全监测和应急预案演练情况	1、在工业控制网络部署网络安全监测设备的重要工业控制系统数量：_____套 2、在重要工业控制设备前端已部署具备深度包分析和过滤功能防护设备的重要工业控制系统数量：_____套 3、已制定工控安全事件应急响应预案的重要工业控制系统运营单位数量：___家 4、定期对应急预案进行演练的重要工业控制系统运营单位数量：_____家 5、对应急响应预案进行修订的重要工业控制系统运营单位数量：_____家
资产安全情况	1、建立工业控制系统资产清单的重要工业控制系统数量：_____套 2、对关键主机设备进行冗余配置的重要工业控制系统数量：_____套 3、对网络设备进行冗余配置的重要工业控制系统数量：_____套 4、对控制组件进行冗余配置的重要工业控制系统数量：_____套
数据安全情况	1、对静态存储的重要工业数据进行保护的重要工业控制系统数量：_____套 2、对动态传输的重要工业数据进行保护的重要工业控制系统数量：_____套 3、定期备份关键业务数据的重要工业控制系统数量：_____套 4、对测试数据进行保护的重要工业控制系统数量：_____套
供应链管理情况	1、合同中已约定服务商在服务过程中应当承担的信息安全责任和义务的重要工业控制系统数量：_____套 2、与服务商签订保密协议的重要工业控制系统数量：_____套
落实责任情况	1、建立工控安全管理机制的重要工业控制系统运营单位数量：_____家

1 重要工业控制系统是指与国家安全、国家经济安全、国计民生紧密相关的，如钢铁、有色、化工、装备制造、电子信息、核设施、石油石化、电力、天然气、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热等工业生产领域中的工业控制系统。

2 工业主机是指工业生产控制各业务环节涉及组态、操作、监控、数据采集与存储等功能的主机设备载体，包括工程师站、操作员站、历史站等。

表 2　工业控制系统运营单位基本情况表

<table>
<tr><td rowspan="6">单位信息</td><td>单位全称</td><td colspan="2"></td><td>法人代表</td><td></td></tr>
<tr><td>通讯地址</td><td colspan="4">省　　市　　县（区）</td></tr>
<tr><td>单位网址</td><td colspan="2"></td><td>邮政编码</td><td></td></tr>
<tr><td>所属行业[1]</td><td colspan="2"></td><td>销售收入</td><td></td></tr>
<tr><td>经济类型</td><td colspan="4">□ 国有事业单位[2]
□ 国有及国有控制企业[3]（□ 中央　　□ 地方）
□ 股份制企业　　□ 外商及港澳台投资企业[4]
□ 集体企业　　□ 民营企业
□ 其他：_____</td></tr>
<tr><td rowspan="3">联系人</td><td>姓名</td><td colspan="2"></td><td>职务</td><td></td></tr>
<tr><td>所属部门</td><td colspan="2"></td><td>工作电话</td><td></td></tr>
<tr><td>电子邮件</td><td colspan="2"></td><td>传真</td><td></td></tr>
<tr><td rowspan="6">工控系统基本情况</td><td colspan="2">工业控制系统总数量</td><td colspan="3"></td></tr>
<tr><td colspan="2">系统名称</td><td colspan="3">系统简介</td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
<tr><td colspan="2"></td><td colspan="3"></td></tr>
</table>

工业安全管理情况	应急预案演练情况	1. 工控安全事件应急响应预案: □已制定，包括: □应急计划策略和规程 □应急计划培训 □应急计划测试与演练 □应急处理流程 □事件监控措施 □应急事件报告流程 □应急支持资源 □应急响应计划 □其它: _____ □未制定 2. 急预案演练情况: □定期开展，演练周期: _____ □本年度已开展 □将演练情况报网络安全主管部门 □未将演练情况报网络安全主管部门 □应急演练结束后对应急预案进行了评估和适用性修订 □应急演练结束后未对应急预案进行了评估和适用性修订 □本年度未开展 □未定期开展
	落实责任情况	1. 工控安全管理机制: □已建立，包括: □建立了工业控制系统安全管理制度 □成立了工业控制系统信息安全协调小组 □明确了工控安全管理责任人 □其它: _____ □未建立

注 1: 工控系统基本情况可另附表说明。

注 2: 此处工业控制系统的划分原则为 1）具体的完整的工业控制系统: 以企业工业自动化生产过程为基础，属于企业的一个自动化生产全过程或一个工业自动化生产装置; 或者是 2）工业控制系统中相对独立的一部分: 以企业工业自动化生产过程的局部环节为基础，属于企业的一个自动化生产全过程或一个工业自动化生产装置的工业控制系统中的相对独立的且物理边界清晰的某个安全区域或通信网络。

---

1 按照《国民经济行业分类》（GB/T4745-2011）规定填写。

2 按照《事业单位登记管理暂行条例》登记的，为社会公益目的、由国家机关举办或者其他组织组织利用国有资产举办的，从事教育、科技、文化、卫生等活动的社会服务组织。

3 按照《中华人民共和国企业法人登记管理条例》登记注册的三类经济组织:（1）全部资产归国家所有的（非公司制）国有企业;（2）全部资产归国家所有的国有独资有限责任公司;（3）由国有资本占控制地位的有限责任公司和股份有限公司，此处称国有控股公司。

4 包括港、澳、台资本和其他地区外资资本投资设立的独资或控股的独资公司、有限责任公司和股份有限公司。

表 3　工业控制系统信息安全自查表

<table>
<tr><td>系统名称</td><td colspan="4"></td></tr>
<tr><td rowspan="2">负责人</td><td>姓名</td><td></td><td>职务</td><td></td></tr>
<tr><td>所属部门</td><td></td><td>工作电话</td><td></td></tr>
<tr><td>功能描述</td><td colspan="4">（描述该系统的功能、业务流程）</td></tr>
<tr><td>业务互联</td><td colspan="4">（描述与其他工业控制系统、上层监控系统、MES 系统互联情况）</td></tr>
<tr><td>系统组成结构</td><td colspan="4">（描述该工业控制系统的组成情况、网络拓扑图等）</td></tr>
<tr><td rowspan="7">系统构成情况</td><td>类型</td><td>设备</td><td>国内品牌</td><td>国外品牌</td></tr>
<tr><td rowspan="6">工业生产控制设备</td><td>可逻辑编程控制器（PLC）</td><td>台</td><td>台</td></tr>
<tr><td>分布式控制系统（DCS）</td><td>台</td><td>台</td></tr>
<tr><td>远程终端设备（RTU）</td><td>台</td><td>台</td></tr>
<tr><td>数控机床</td><td>台</td><td>台</td></tr>
<tr><td>工业机器人</td><td>台</td><td>台</td></tr>
<tr><td>智能仪表</td><td>台</td><td>台</td></tr>
</table>

		其它	台	台
	工业网络通信设备	工业交换机	台	台
		工业路由器	台	台
		串口服务器	台	台
		其它	台	台
	工业主机设备	工业主机	台	台
		组态软件&数据采集与监控系统（SCADA）软件	套	套
		工业数据库	套	套
		其它	台	台
	工业生产信息系统	制造执行系统（MES）	套	套
		ERP 管理系统	套	套
		工业云	套	套
		其它	套	套
	工业网络安全设备	工业防火墙	台	台
		工业网闸	台	台
		主机安全防护设备	台	台
		其它	台	台
安全软件选择与管理情况	1. 工业主机防护设备（如防病毒软件、应用程序白名单软件）： □已安装，防护设备名称：_____ □未安装 2. 及时进行恶意代码库或白名单规则库更新升级： □是，目前库版本号：_____ □否，目前库版本号：_____ 3. 定期进行系统查杀： □是，查杀时间间隔：_____ □未进行定期查杀 4. 防病毒和恶意软件入侵管理机制： □已建立，包括：□定期扫描病毒和恶意软件 □定期更新病毒库 □查杀临时接入设备（如临时接入 U 盘、移动终端外设） □未建立			
	1. 工业控制网络安全配置策略： □已建立，包括：□网络分区分域 □非必要端口禁用 □其它：_____ □未建立			

配置和补丁管理情况	2. 工业主机安全配置策略: □已建立，包括: □远程控制管理禁用 □关闭默认账户 □最小服务配置 □关闭非必要文件共享 □启用登录口令复杂度要求 □其它: _____ □未建立 3. 工业控制设备安全配置策略: □已建立，包括: □口令策略合规性 □其它: _____ □未建立 4. 工业控制系统配置清单: □已建立，包括: □设备名称 □设备编号 □配置策略 □配置时间 □其它: _____ □未建立 5. 定期进行配置清单的更新和维护: □是，维护时间间隔: _____ 更新时间间隔: _____ □部分是，定期更新和维护的配置清单: _____ 时间间隔: _____ □否 6. 及时修复重大工控安全漏洞: □是 □否
边界安全防护情况	1. 直接与企业内网连接: □是 □否，组网方式（单选）: □独立 □使用防护设备进行隔离，防护设备名称及生产厂商: _____ □其它: _____ 2. 直接与互联网连接: □是 □否，组网方式（单选）: □独立 □使用防护设备进行隔离，防护设备名称及生产厂商: _____ □通过企业网连接 □其它: _____ 3. 对工业控制系统网络进行安全域划分: □是，划分原则: □安全域重要性 □业务需求 □其它: _____ □否 4. 各安全域之间进行逻辑隔离: □是，隔离措施: □防火墙 □网闸 □其它: _____ □否
物理和环境安全防护情况	1. 物理安全防护区域防护措施: □无 □门禁系统 □专人值守 □视频监控 □其它: _____ 2. 拆除或封闭工业主机外设接口: □是 □否，未拆除或封闭的外设接口包括: □USB □光驱 □无线 □其它: _____ 3. 使用外设安全管理技术手段进行安全管理: □是，方式: □主机外设统一管理设备（或软件）: _____ □隔离存放有外设接口的工业主机 □其它: _____

	□否
身份认证情况	1.使用身份认证管理手段: □是，包括: □口令密码 □USB-Key □智能卡 □生物指纹 □其它: _____ 2.最小权限原则分配账户权限: □是 □否 3.工业控制系统口令使用: □采用默认口令 □采用弱口令 □其它: *（口令策略要求）* 4.定期更新口令: □是，更新周期: _____ □否
远程访问安全情况	1.面向互联网开通通用网络服务: □是，包括: □HTTP □FTP □Telnet □其它: _____ □否 2.使用远程访问: □是，安全加固策略: □无 □采用数据单向访问控制 □其它: _____ □否 3.使用远程维护: □是，安全加固策略: □无 □采用虚拟专用网络（VPN） □其它: _____ □否 4.工业控制系统相关访问日志: □留存，留存期: _____ □未留存
安全监测情况	1.工业控制系统网络部署网络安全监测设备: □是，网络安全监测设备型号及生产商: _____ □否 2.重要工业控制设备前端部署具备深度包分析和过滤功能的防护设备: □是，防护设备型号及生产商: _____ □否
资产安全情况	1.工业控制系统资产清单: □已建立，包括: □设备名称 □设备编号 □设备型号 □设备类型 □生产厂商 □设备重要程度/密级 □设备版本 □启用时间 □责任部门 □责任人 □使用状态 □其它: _____ □未建立 2.关键主机设备是否进行硬件冗余: □是 □否 3.网络设备是否进行硬件冗余: □是 □否 4.控制组件是否进行硬件冗余: □是 □否
	1.对静态存储的重要工业数据进行保护: □是，保护措施: □数据加密 □隔离存放 □访问权限控制 □其它: _____

数据安全情况	□否 2. 对动态传输的重要工业数据进行保护： □是，保护措施：□数据加密 □数据隔离 □其它：_____ □否 3. 定期备份关键业务数据： □是，备份周期：_____ □否 4. 对测试数据进行保护： □是，保护措施：□数据加密 □数据销毁 □隔离存放 □访问权限控制 □其它：_____ □否
供应链管理情况	1. 服务商在服务过程中应当承担的信息安全责任和义务： □已约定，包括：_____ □未约定 2. 服务商签订保密协议情况：□已签订 □未签订

注：多套系统可复印分别填写。

1 工业主机是指工业生产控制各业务环节涉及组态、操作、监控、数据采集与存储等功能的主机设备载体，包括工程师站、操作员站、历史站等。

公开方式：依申请公开