附件1

各市（区）工信主管部门负责人信息表

**（各地市工信主管部门填写）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **姓名** | **单位** | **职务** | **联系方式** |
| **负责人** |  |  |  |  |
| **联系人** |  |  |  |  |

附件2

工业控制系统信息安全检查情况汇总表

**（各地市工信主管部门填写）**

|  |  |
| --- | --- |
| 地市名称 |  |
| 基本情况 | 重要工业控制系统运营单位总数/家 |  |
| 重要工业控制系统总数/套 |  |
| 系统构成情况 | 类型 | 设备 | 国内品牌 | 国外品牌 |
| 工业生产控制设备类 | 可逻辑编程控制器（PLC）/台 |  |  |
| 分布式控制系统（DCS）/台 |  |  |
| 远程终端设备（RTU）/台 |  |  |
| 数控机床/台 |  |  |
| 工业机器人/台 |  |  |
| 智能仪表/台 |  |  |
| 其它/台 |  |  |
| 工业网络通信设备类 | 工业交换机/台 |  |  |
| 工业路由器/台 |  |  |
| 串口服务器/台 |  |  |
| 其它/台 |  |  |
| 工业主机设备 | 工业主机/台 |  |  |
| 组态软件&数据采集与监控系统（SCADA）软件/套 |  |  |
| 工业数据库/套 |  |  |
| 其它/台 |  |  |
| 工业生产应用系统类 | 制造执行系统（MES）/套 |  |  |
| ERP管理系统/套 |  |  |
| 工业云/套 |  |  |
| 工业应用程序（APP）/套 |  |  |
| 其它/套 |  |  |
| 工业网络安全设备类 | 工业防火墙/台 |  |  |
| 工业网闸/台 |  |  |
| 主机安全防护设备/台 |  |  |
| 其它/台 |  |  |
| 已开展安全等级保护测评的系统/套 |  |
| 使用工业互联网平台或工业云的系统/套 |  |
| 安全软件选择与管理情况 | 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 |  |
| 配置和补丁管理情况 | 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 |  |
| 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/套 |  |
| 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/套 |  |
| 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/套 |  |
| 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 |  |

注1：重要工业控制系统运营单位总数应大于或等于检查情况汇总数据中重要工业控制系统运营单位总数。

注2：重要工业控制系统总数应大于或等于检查情况汇总数据中重要工业控制系统总数。

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。

附件3

工业控制系统信息安全自查表

**（各企业组织填写）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位信息 | 单位全称 |  | 法人代表 |  |
| 通讯地址 | 省 市 县（区） |
| 单位网址 |  | 邮政编码 |  |
| 所属行业1 |  | 销售收入 |  |
| 经济类型 | □ 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：  |
| 负责人 | 姓名 |  | 职务 |  |
| 所属部门 |  | 工作电话 |  |
| 电子邮件 |  | 传真 |  |
| 联系人 | 姓名 |  | 职务 |  |
| 所属部门 |  | 工作电话 |  |
| 电子邮件 |  | 传真 |  |
| 工控系统基本情况 | 工业控制系统总数量/套 |  |
| 已开展安全等级保护测评的系统数量/套 |  |
| 系统名称 | 系统简介 |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 系统名称 | （多套系统可复制此表单分别填写） |
| 负责人 | 姓名 |  | 职务 |  |
|  | 所属部门 |  | 工作电话 |  |
| 功能描述 | （描述该系统的功能、业务流程） |
| 业务互联 | （描述与其他工业控制系统、上层监控系统、MES系统互联情况，） |
| 系统组成结构 | （描述该工业控制系统的组成情况、网络拓扑图等） |
| 安全等级保护测评开展情况 | （描述已开展安全等级保护测评的工业控制系统情况、计划开展安全等级保护测评的工业控制系统情况等） |
| 工业互联网平台或工业云使用情况 | （描述工业生产系统通过自己建设或使用第三方工业互联网平台或工业云的情况） |
| 系统构成情况 | 类型 | 设备 | 国内品牌 | 国外品牌 |
| 工业生产控制设备 | 可逻辑编程控制器（PLC）/台 |  |  |
| 分布式控制系统（DCS）/台 |  |  |
| 远程终端设备（RTU）/台 |  |  |
| 数控机床/台 |  |  |
| 工业机器人/台 |  |  |
| 智能仪表/台 |  |  |
| 其它/台 |  |  |
| 工业网络通信设备 | 工业交换机/台 |  |  |
| 工业路由器/台 |  |  |
| 串口服务器/台 |  |  |
| 其它/台 |  |  |
| 工业主机设备 | 工业主机/台 |  |  |
| 组态软件&数据采集与监控系统（SCADA）软件/套 |  |  |
| 工业数据库/套 |  |  |
| 其它/台 |  |  |
|  | 工业生产信息系统 | 制造执行系统（MES）/套 |  |  |
| ERP管理系统/套 |  |  |
| 工业云/套 |  |  |
| 工业应用程序（APP）/套 |  |  |
| 其它/套 |  |  |
| 工业网络安全设备 | 工业防火墙/台 |  |  |
| 工业网闸/台 |  |  |
| 主机安全防护设备/台 |  |  |
| 其它/台 |  |  |
| 已开展安全等级保护测评的系统/套 |  |
| 使用工业互联网平台或工业云的系统/套 |  |
| 安全软件选择与管理情况 | 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 |  |
| 配置和补丁管理情况 | 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 |  |
| 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/套 |  |
| 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/套 |  |
| 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/套 |  |
| 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 |  |

**注：多套系统可复印分别填写。**