附件:

工业控制系统网络安全情况自查表

填 表 说 明

  **一、组成结构**

本表包含四个分表：

表1.各市工业控制系统信息安全自查情况汇总表；

 表2.工业控制系统应用企业基本情况表；

 表3.工业控制系统应用企业自查情况汇总表；

表4.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：

表1.各市工业控制系统信息安全自查情况汇总表：由各地工业和信息化主管部门指定专人负责汇总填写。

表2.工业控制系统应用企业基本情况表：由各工业企业指定专人负责填写。

表3.工业控制系统应用企业自查情况汇总表：由各工业企业指定专人负责填写。

表4.工业控制系统信息安全自查表：由各工业企业正在应用的工业控制系统负责人填写。

表1 各市工业控制系统信息安全自查情况汇总表

|  |  |  |
| --- | --- | --- |
| 基本信息 | 填报地市 |  |
| 填报单位 |  |
| 填报人 |  | 职务 |  |
| 所属部门 |  | 工作电话 |  |
| 电子邮件 |  | 传真 |  |
| 本地区系统基本情况汇总 | 参与填报企业数量 |  |
| 工业控制系统数量 |  |
| 非工业控制系统数量（如门户网站、办公系统等） |  |
| 连接互联网的系统数量 |  |
| 上云系统数量 |  |
| 开展等级保护测评系统数量 |  |
| 开展工业互联网网络安全风险评估系统数量 |  |
| 开展网络安全检查系统数量 |  |
| 上一年度发生网络安全事件数量 |  |

注：本表由各地工业和信息化主管部门指定专人负责汇总填写。

表2工业控制系统应用企业基本情况表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 单位信息 | 企业全称 |  | 法人代表 |  |
| 通讯地址 | 省 市 县（区） |
| 企业网址 |  | 邮政编码 |  |
| 所属行业 |  | 上一年度销售收入 |  |
| 经济类型 | □ 国有及国有控制企业 （□ 中央 □ 地方）□ 股份制企业 □ 外商及港澳台投资企业□ 集体企业 □ 民营企业□ 其他： |
| 联系人 | 姓名 |  | 职务 |  |
| 所属部门 |  | 工作电话 |  |
| 电子邮件 |  | 传真 |  |
| 系统基本情况 | 工业控制系统数量 |  |
| 非工业控制系统数量（如门户网站、办公系统等） |  |
| 连接互联网的系统数量 |  |
| 上云系统数量 |  |
| 开展等级保护测评系统数量 |  |
| 开展工业互联网网络安全风险评估系统数量 |  |
| 开展网络安全检查系统数量 |  |
| 上一年度发生网络安全事件数量 |  |

注：本表由各工业企业指定专人负责填写。

表3 工业控制系统应用企业自查情况汇总表

企业名称：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 系统名称 | 系统类型 | 是否连接互联网 | 是否上云 | 是否开展等级保护测评 | 是否开展风险评估 | 是否开展网络安全检查 | 上年度是否发生安全事件 |
| 1 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 2 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 3 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 4 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 5 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 6 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 7 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |
| 8 |  | □ 工业控制系统□ 非工业控制系统 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 | □ 是 □ 否 |

注：本表由各工业企业指定专人负责填写。填写内容包含工业控制系统和非工业控制系统。

表4 工业控制系统网络安全自查表

（企业在用的工业控制系统逐个填写，每套系统填写一张表）

|  |  |
| --- | --- |
| 企业全称 |  |
| 系统名称 |  |
| 负责人 | 姓名 |  | 职务 |  |
| 所属部门 |  | 工作电话 |  |
| 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、USB接入、应用程序白名单软件等）：□已安装，防护设备名称：□未安装 |
| 配置和补丁管理情况 | 1.工业主机安全策略配置：□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2.及时修复重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞： □是 □否 |
| 边界安全防护情况 | 1.对工业控制系统网络进行安全域划分：□是 □否2.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： |
| 身份认证情况 | 1.使用身份认证管理手段：□口令密码 □USB-Key □智能卡 □生物指纹□其它： |
| 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.使用远程维护： □是，安全加固策略：□无 □采用虚拟专用网络（VPN） □其它： □否 |
| 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.关键主机设备是否进行硬件冗余：□是 □否2.网络设备是否进行硬件冗余：□是 □否3.控制组件是否进行硬件冗余：□是 □否 |
| 数据安全情况 | 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：□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 |

注：本表由各工业企业正在应用的工业控制系统负责人填写。

企业在使用的工业控制系统逐个填写，每套系统填写一张表，多套系统应分别填写。

名词解释：

1.工业控制系统：是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。其核心组件包括：数据采集与监控系统（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器系统（PLC）、人机交互界面设备(HMI)等。

2.信息系统（非工业控制系统）：是由计算机硬件、网络和通信设备、计算机软件、信息资源、信息用户组成的以处理信息流为目的的人机一体化系统。主要有五个基本功能，即对信息的输入、存储、处理、输出和控制。常见类型包括：网站系统、业务管理系统、办公自动化系统、信息资源处理系统等。