工业控制系统信息安全自查情况表

**（企业登录平台填报）**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **一、工业企业基本情况** | | | | | | | | | | |
| 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： | | | | | | | |
| 联  系  人 | 姓名 | |  | | | | | 职务 |  | |
| 所属部门 | |  | | | | | 工作电话 |  | |
| 工  控  系  统  基  本  情  况 | 工业控制系统总数量 | | | | | （套） | | | | |
| 系统编号 | | | 系统名称 | | 系统简介（系统功能/网络架构） | | | | |
| 1 | | |  | |  | | | | |
| 2 | | |  | |  | | | | |
| ...... | | |  | |  | | | | |
| ...... | | |  | |  | | | | |
|  | | |  | |  | | | | |
| 系统互联情况： | | | | | | | | | |
| 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.应急预案演练情况：  □定期开展，演练周期：  □本年度已开展，演练时间：  □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 | | | | | | | |
| **二、控制系统基本情况** | | | | | | | | | | |
| 系统构成情况 | | 类型 | | | 设备 | | 国内品牌 | | | 国外品牌 |
| 工业网络安全设备 | | | 工业  防火墙 | | 台 | | | 台 |
| 工业  网闸 | | 台 | | | 台 |
| 主机外设  统一管理设备 | | 台 | | | 台 |
| 网络安全  监测设备 | | 台 | | | 台 |
| 深度包分析和过滤功能的防护设备 | | 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.是否安装工业主机防护设备（如防病毒软件、应用程序白名单软件）：  □是， 系统数量： （套）  □否， 系统编号：  （指上表中工控系统基本情况中的系统编号）  2.是否及时进行恶意代码库或白名单规则库更新升级：  □是， 系统数量： （套）  □否， 系统编号：  3.是否定期进行系统查杀：  □是， 系统数量： （套）  □否， 系统编号：  4.是否建立防病毒和恶意软件入侵管理机制：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 配置和补丁管理情况 | | 1.是否配置工业控制网络安全策略：  □是， 系统数量： （套）  □否， 系统编号：  2.是否配置工业主机安全策略：  □是， 系统数量： （套）  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：  □否， 系统编号：  3.是否配置工业控制设备安全策略：  □是， 系统数量： （套）  □否， 系统编号：  4.是否建立工业控制系统安全策略配置清单：  □是， 系统数量： （套）  □否， 系统编号：  5.是否定期进行配置清单的更新和维护：  □是， 系统数量： （套）  □否， 系统编号：   1. 是否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， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 边界安全防护情况 | | 1.是否直接与企业内网连接：  □是， 系统数量： （套）  □否， 系统编号：  □与企业网物理隔离，系统数量： （套）  2.是否直接与互联网连接：  □是， 系统数量： （套）  □否， 系统编号：  □与互联网物理隔离，系统数量： （套）  3.是否对工业控制系统网络进行安全域划分：  □是， 系统数量： （套）  □否， 系统编号：  4.各安全域之间是否进行逻辑隔离：  □是， 系统数量： （套）  隔离措施：□防火墙 □网闸 □其它：  □否， 系统编号： | | | | | | | | |
| 物理和环境安全防护情况 | | 1.是否采取物理安全防护区域防护措施：  □是， 系统数量： （套）  □否， 系统编号：  2.是否拆除或封闭工业主机上不必要的外设接口：  □是， 系统数量： （套）  □否， 系统编号：  3.是否使用外设安全管理技术手段对外设接口进行安全管理：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 身份认证情况 | | 1.是否使用身份认证管理手段：  □是， 系统数量： （套）  □否， 系统编号：   1. 是否根据最小权限原则分配账户权限：   □是， 系统数量： （套）  □否， 系统编号：  3.是否使用默认口令或弱口令：  □是， 系统数量： （套）  □否， 系统编号：  4.是否定期更新口令：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 远程访问安全情况 | | 1.是否面向互联网开通HTTP、FTP等网络服务：  □是， 系统数量： （套）  □否， 系统编号：  2.远程访问是否使用数据单向访问控制等策略进行安全加固：  □是， 系统数量： （套）  □否， 系统编号：  □不使用远程访问，系统数量： （套）  3.远程维护是否采用虚拟专用网络（VPN）等安全加固策略：  □是， 系统数量： （套）  □否， 系统编号：  □不使用远程维护，系统数量： （套）  4.是否保留工业控制系统相关访问日志：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 安全监测情况 | | 1.工业控制网络是否部署网络安全监测设备（如工业流量审计探针设备）：  □是， 系统数量： （套）  □否， 系统编号：  2.重要工业控制设备前端是否部署具备深度包分析和过滤功能的防护设备：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 资产安全情况 | | 1.是否建立工业控制系统资产清单：  □是， 系统数量： （套）  □否， 系统编号：  2.关键主机设备是否进行硬件冗余：  □是， 系统数量： （套）  □否， 系统编号：   1. 网络设备是否进行硬件冗余：   □是， 系统数量： （套）  □否， 系统编号：   1. 控制组件是否进行硬件冗余：   □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |
| 数据安全情况 | | 1.是否对静态存储的重要工业数据进行保护：  □是， 系统数量： （套）  □否， 系统编号：  2.是否对动态传输的重要工业数据进行保护：  □是， 系统数量： （套）  □否， 系统编号：  3.是否定期备份关键业务数据：  □是， 系统数量： （套）  □否， 系统编号：  4.是否对测试数据进行保护：  □是， 系统数量： （套）  □否， 系统编号：  □无测试环境， 系统数量： （套） | | | | | | | | |
| 供应链管理情况 | | 1.合同中是否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：  □是， 系统数量： （套）  □否， 系统编号：  2.是否与服务商签订保密协议：  □是， 系统数量： （套）  □否， 系统编号： | | | | | | | | |

**注1：**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。  
 **注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。

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。