附件1

护航新型工业化网络安全典型案例

申报表

案 例 名 称：

申 报 单 位： （加盖单位公章）

推 荐 单 位： （加盖单位公章）

申 报 日 期： 年 月 日

工业和信息化部编制

填 表 须 知

一、申报单位应仔细阅读案例遴选工作有关说明，如实、详细地填写每一部分内容。

二、除另有说明外，申报表单位基本信息部分不得空缺，申报书要求提供证明材料的，请在申报书附件处进行补充。

三、纸质版申报材料要求盖章处，须加盖公章，复印无效，申报材料（含附件）需加盖骑缝章，交由推荐单位统一邮寄。

四、电子版材料内容、格式、附件应与纸质版材料一致。

五、申报单位所申报的案例需拥有自主知识产权，对提供参评的全部资料的真实性负责。

一、申报单位基本情况

|  |  |
| --- | --- |
| 单位名称 | （请填写全称） |
| 组织机构代码/三证合一码 |  | 成立时间 |  |
| 单位地址 |  | 注册资本（万元） |  |
| 单位性质 | □国有企业 □民营企业 □合资企业□国有控股企业 □国有参股企业□其他（请注明）：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 联系人 |  | 联系电话 |  |
| 传真 |  | 电子邮箱 |  |
| 企业类别 | □工业企业□工业互联网平台企业□工业互联网标识解析企业□智能网联汽车生产企业□车联网服务平台企业□工业控制产品厂商□基础电信企业 |
| 申报方向 | □工业互联网安全分类分级案例□车联网网络安全防护案例□工业控制系统安全评估案例□工业控制产品漏洞治理案例□网络安全威胁监测服务案例 |
| 网络安全级别（申报工业互联网安全分类分级案例填写） | □三级 □二级 □一级 |
| 网络安全级别（申报车联网网络安全防护案例填写） | □五级 □四级 □三级 □二级 □一级 |
| 申报单位简介 | 企业基本情况（经营情况、主营业务、技术创新和成果转化等）、数字化网络化智能化应用或服务情况（应用新一代信息技术推动研发、生产、管理等各环节数转智改网联情况，5G工厂、数字工厂、智能工厂等建设情况），不超过1000字。 |

二、总体情况

各申报主体围绕申报案例方向，梳理填写对应方向内容。

**（一）工业互联网安全分类分级方向**

工业企业、工业互联网平台企业和标识解析企业按照《工业互联网安全分类分级管理办法》，建立企业网络安全管理制度和防护体系，开展自主定级、分级防护、符合性评测、安全整改等各环节工作，提升企业防护水平等情况。需附定级报告、评测报告、整改报告等相关证明材料。

**（二）车联网网络安全防护方向**

智能网联汽车生产企业、车联网服务平台企业开展车联网网络安全防护定级备案、安全防护、安全评测和隐患整改等情况。需附车联网网络安全防护定级备案信息、评测报告等相关证明材料。

**（三）工业控制系统安全评估方向**

工业企业按照《工业控制系统网络安全防护要求》，围绕安全管理、技术防护、安全运营、责任落实等四方面基线要求，实施工业控制系统网络安全评估工作、提升工业控制系统网络安全防护水平等情况。需附工业控制系统安全评估情况表、整改报告等相关证明材料。

**（四）工业控制产品漏洞治理方向**

网络安全企业、工业控制产品厂商、工业企业按照《网络产品安全漏洞管理规定》相关要求，开展漏洞发现、验证、修复和处置等工作，参与漏洞众测等活动情况。网络安全企业需附参与众测活动证明材料、原创漏洞证书等，产品厂商需附收到的漏洞通报信息、验证记录、补丁公告等，工业企业需附收到的漏洞通报信息、漏洞处置报告等证明材料。

**（五）网络安全威胁监测服务方向**

基础电信企业发挥网络优势，通过对工业企业互联网专线流量进行汇聚和监测分析，有效发现网络攻击、恶意程序传播等威胁和事件，并将安全监测数据和结果上报国家或省级工业互联网安全技术平台，支撑主管部门面向工业企业提供威胁共享、事件通报和处置等服务，赋能重点企业提升风险防范能力。需附开展工业企业流量监测分析、与国家或省级平台对接、支撑向工业企业开展监测服务等相关证明材料。

三、成效与亮点

根据申报方向，梳理在发现漏洞、消除风险、防护达标、能力提升等方面的成效，介绍案例的可借鉴可推广价值，提炼经验成效和特色亮点做法，总结网络安全护航企业数字化转型、赋能服务高质量发展的作用效果。需补充必要的数据、案例进行说明。

四、真实性承诺

我单位申报的所有材料，均真实、完整，如有不实，愿承担相应责任。

 法定代表人签章：

申报单位公章：

 年 月 日