《电力系统网络安全风险评价与防御导则》

编制说明（征求意见稿）

一、工作简况

1 主要工作过程

起草（草案、调研）阶段：

2024 年 1 月，成立标准起草工作组，确定主笔人、起草单位，确定工作方法及工作内容，开展课题前期研究工作。2024 年 2 月至 5 月，启动团体标准编制工作，形成《电力系统网络安全风险评价与防御导则》立项申请书与草案，并提交至中国电工技术学会。2024 年 5 月邀请相关专家对草案进行讨论与研究，标准起草工作组根据专家意见对草案进行补充与完善，形成标准征求意见稿。

2 主要参加单位和起草工作组成员及其所做的工作

标准编写组收集了近几年来网络安全漏洞分类分级规则方面的相关资料，通过对比整理分析确定了标准主要技术内容，由国网山西省电力公司电力科学研究院、国网信息通信产业集团有限公司牵头完成标准编制、整理和完善，其他参与单位配合并负责收集相关资料、提出建议。

主要参与单位：国网山西省电力公司电力科学研究院、国网信息通信产业集团有限公司、四川中电启明星有限公司、华北电力大学、安徽继远检验检测技术有限公司、南京南瑞信息通信科技有限公司、北京中电普华信息技术有限公司。

主要参与人员：芦山、付昀夕、刘泽辉、王振亚、杨华、杨姝、周自强、马东娟、刘泽三、宫晓辉、凌浩洁、张文娟、闫晨阳、张敏、高紫婷、闫廷廷、黄元、李杉、李廷顺、靳鑫、潘安顺、富思、沈耀威、任彦斌、宋亚琼、王军、韩泽华、苑学贺、董爱强、刘振圻、南淑君。

二、标准编制原则和主要内容

1、标准编制原则

a.本标准的起草遵循《GB/T 1.1—2020 标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定，以科学性、先进性和经济性为原则，坚持实事求是，遵守国家有关法律、法规，同时符合团体标准要求。本项目为电力行业提供

一个统一的安全漏洞管理框架，通过系统化的漏洞评估和应对措施，实现对电力系统网络安全的持续监控和改进。

b.采用会议讨论的形式，集合信息技术、电力技术、网络安全等专家，将不同业务维度的专业技术融合一体，体现出标准编制的科学性、实用性和先进性。

2、标准主要内容

本标准分为 6 个章节，（1）范围；（2）规范性引用文件；（3）术语和定义；（4）符号、代号和缩略语；（5）网络安全漏洞分类：介绍软件、硬件、配置等来源的网络安全漏洞分类；介绍协同层、应用层、网络层、系统层、硬件层网络安全漏洞；介绍缓冲区溢出、SQL 注入、跨站脚本等网络安全漏洞及其应对方式；（6）网络安全漏洞分级：介绍按照网络安全漏洞分级的四个维度及分级方式：可获取性与公开程度、利用条件限制、危害等级、修复难度。

3、主要技术差异

本标准为新制度标准，无主要技术差异。

4、解决的主要问题

本标准适用于电力系统网络安全管理的各个层面，包括硬件设施、软件应用和网络通信。针对这些层面的特定漏洞，本标准介绍了漏洞的分类方法、分级标准及相应的防御措施，使得电力系统的网络安全能力得以增强，从而降低由于漏洞引起的安全事故的风险，保障电力系统的稳定和可靠运行，维护国家安全和公共利益。

三、主要试验（或验证）情况

本标准不涉及试验（或研制）情况。

四、标准中涉及专利的情况

本标准不涉及专利问题。

五、预期达到的社会效益、对产业发展的作用等情况

为漏洞建立标识，提供了一套评价方法，可以将漏洞按照风险程度进行分类和排序，按照分级安排优先级，确保有限资源针对性地修补高风险漏洞。提供更直观的风险说明，映射到明确的风险等级，帮助非技术人员理解和决策，分级规则帮助确保安全措施的实施满足特定的法规标准。

六、与国际、国外对比情况

本文件未采用国际、国外标准。

七、在标准体系中的位置，与现行相关法律、法规、规章及相关标准，特别是强制性标准的协调性

本标准与现行的相关法律、法规、规章与相关标准保持一致。

八、重大分歧意见的处理经过和依据

标准编制过程中广泛征集了专家意见，所有意见均按照标准编制程序进行了采纳，不存在重大分歧意见。

九、标准性质的建议说明

建议本团体标准的性质为推荐性团体标准。

十、贯彻标准的要求和措施建议

建议本标准批准发布 7 天后实施。

十一、废止现行相关标准的建议

无

十二、其他应予说明的事项

无