附件 2

团体标准《电力行业外部攻击面运营管理指南》编制说明

一、工作简况

1.任务来源

深圳市润电信息科技有限公司根据电力行业网络安全发展发展，于 2025 年 8 月向深圳市网络与信息安全行业协会提出《电力行业外部攻击面运营管理指南》团体标准立项申请。深圳市网络与信息安全行业协会按程序批准该团体标准立项并发布公告。来自深圳市润电信息科技有限公司、绿盟科技集团股份有限公司、深信服科技股份有限公司、杭州安恒信息技术股份有限公司、中能融合智慧科技有限公司、深圳市魔方安全科技有限公司等单位的专家参与了标准的制定。

2.编制目的

“云大物移智”正在重塑电力行业数字基础架构，网络边界越来越模糊。现有的安全防护体系存在不足，无法应对日益复杂的电力行业暴露面安全治理需求。同时，在开展外部攻击面运营管理方面普遍缺少规范性指导文件，部分机构在外部攻击面运营存在管理不到位的情况，并导致信息安全事件发生。因此有必要订制一个标准来指导行业提升外部攻击面运营管理能力，规范行业的外部攻击面运营管理工作。

本标准的目的是立一个可供电力行业各单位机构参考的外部攻击面运营管理指南，解决各单位机构在进行了一定程度安全建设后必须面临的外部攻击面深化治理带来安全挑战及痛难点问题，让行业的外部攻击面运营管理能力和水平在一定程度上螺旋上升。

二、标准的属性

本标准为深圳市网络与信息安全行业协会制定发布的团体标准。

三、标准制定原则

按照 GB/T1.1-2020《标准化工作导则 第 1 部分:标准化文件的结构和起草规则》的要求和规定编写本标准内容。

本标准具有先进性、系统性、普适性、可操作性。

三、确定标准主要内容的依据

《电力行业外部攻击面运营管理指南》团体标准为首次制定，确定主要内容的依据具体如下：

1.法律法规要求

电力行业网络属于《中华人民共和国网络安全法》（网络安全法）、《中华人民共和国数据安全法》（数据安全法）定义的“关键信息基础设施”。。《中华人民共和国网络安全法》《电力监控系统安全防护规定》《中华人民共和国关键信息基础设施安全保护条例》等法规对防护提出更高要求。另一方面，《电力监控系统安全防护规定》：衔接细化第三章中的安全管理要求，并针对性对外部攻击面进行细化加强。

本标准契合上述法律法规要求，对电力行业外部攻击面领域做出运营管理指南。

2. 行业最佳实践

本标准充分参考外部攻击面风险管理领域广泛认可、经过验证并被证明为高效、可靠和安全的操作方式、技术选择、系统设计和管理策略。这些实践经验基于电力行业内多年知识积累，对于外部攻击面风险管理的规划、设计、实施和管理都具有重要的指导意义。

3.技术发展趋势

发电行业外部攻击面管理正转向主动智能防护体系。发电行业外部暴露面管理技术正转向主动动态治理。AI 驱动的 EASM 平台成核心，结合多源情报实时扫描 IP、域名、云资产等外部资产，精准识别影子资产与仿冒资产，解决资产数据质量问题。平台化整合成趋势，EASM 与 CAASM、BAS 融合构建统一管理平台，覆盖攻击路径测绘与漏洞验证。供应链安全通过自动化工具监测第三方组件漏洞，纳入外部风险评估体系。物联网设备强化端口管控，禁用冗余端口并加密传输，阻断外部入侵入口。

4.专家意见和学术研究

标准制订单位广泛征求网络安全行业专家的意见，从提升行业规范性、增强系统安全性、促进技术创新、便于系统集成和兼容性、提升行业国际竞争力等多个角度，确认标准具体规定内容。另一方面，标准制订单位通过搜索引擎、图书馆等渠道查阅

外部攻击面管理领域的学术研究成果，了解最新研究动态，将其融入标准之中。

五、国内外现有相关标准情况

在国际范围内，尽管“攻击面管理”这一概念并未在多数政策、法规和标准中以独立名词的形式明确提出，但许多国外的网络安全法规、标准和指导原则已对与攻击面管理密切相关的实践（如资产识别、脆弱性管理、持续监控、风险评估 与处置等）提出了要求。这些政策和标准为组织构建和完善攻击面管理体系提供了监管和合规层面的依据。以下是一些主要的国外政策、法规及标准示例：

（美国）NIST 网络安全框架（NISTCybersecurityFramework，CSF）。由美国国家标准与技术研究院（NIST）推出的自愿性框架，为识别、保护、检测、响应和恢复安全能力提供指导。其中资产管理（ID.AM）和漏洞管理（PR.IP）相关措施为攻击面管理实践提供直接参照。

（美国）美国网络安全与基础设施安全局（CISA）相关指令。CISA 发布的绑定操作指令（BOD），如 BOD23-01，要求 美国联邦民用部门执行持续漏洞扫描与清点资产，以减少可被利用的攻击面。

（欧盟）网络与信息安全指令（NISDirective）及 NIS2。要求成员国关键基础设施提供商与数字服务商加强网络安全风险 管理，包括风险识别、持续监控与漏洞管理，这实际推动了攻击面管理相关实践的落地。

（欧盟）欧洲网络安全法（EUCybersecurityAct）及欧洲网络与信息安全局（ENISA）指导文件。ENISA 发布的网络威胁 分析报告和最佳实践指南涵盖了资产识别、风险识别及缓解策略，为攻击面管理提供参考。

国内在网络安全和数据安全方面，从战略、法律、条例、规定和标准等多个层面提出了明确的要求，并强调了积极防御、 主动发现、及时处置和持续改进的重要性。国内网络安全技术规范标准虽未对“攻击面管理”进行专门定义，但其核心理念和要求已在多个标准中有所体现：

网络安全相关法律。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息 保护法》等法律推动了网络安全风险防控的重视，要求企业不仅要保护关键信息基础设施，还要保护个人信息和 数据安全，减少因资产

暴露面过大而带来的安全风险。如《中华人民共和国网络安全法》第二十一条要求网络运 营者应保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：第二十五条 网络运营者应及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。如《中华人民共和国数据安全法》要 求数据处理者采取必要措施保障数据安全，防止数据泄露、篡改和破坏。如《中华人民共和国个人信息保护法》 要求个人信息处理者采取必要措施保护个人信息安全，防止个人信息泄露、滥用和非法交易。

《关键信息基础设施安全保护条例》。该条例于 2021 年 9 月生效，要求关键信息基础设施运营者采取必要措施 保障关键信息基础设施安全，包括识别和管理关键信息基础设施攻击面，防止网络攻击和数据泄露。

《关键信息基础设施安全保护要求》(GB/T39204-2022)。该标准于 2023 年 5 月 1 日正式实施，对关键信息基础设施的安全保护提出了明确要求，包括分析识别、安全防护、检测评估、监测预警、主动防御、事件处置六个方面，提出应提升关键信息基础设施应对网络攻击能力。如针对发生的网络安全事件或发现的网络安全威胁， 提前或及时发出安全警示。建立威胁情报和信息共享机制，落实相关措施，提高主动发现攻击能力。以应对攻击行为的监测发现为基础，主动采取收敛暴露面、捕获、溯源、干扰和阻断等措施，开展攻防演习和威胁情报工作， 提升对网络威胁与攻击行为的识别、分析和主动防御能力。

目前上述现有法律法规、政策要求及标准中，暂未在外部攻击面的安全运管管理中提出明确的运营目标、过程管理及可供参考的最佳实践，本标准将填补这个空白。

六、重大分歧意见的处理经过和依据

本标准在制定过程中未出现重大分歧意见。

七、作为强制性标准或推荐性标准的建议

本标准建议作为推荐性标准发布实施。

八、其他应予说明的情况

无。