《自主可控网络安全技术 基于网络靶场的软件自主可控能力测试指南》（征求意见稿）编制说明

一、工作简况

1. **任务来源**当前，软件测试领域缺少面向自主可控安全能力的系统性测试方法，并且软件安全测试活动是离散的，安全风险管理缺少连续性。经过前沿用户探索和实践，证实基于网络靶场进行软件自主可控能力测试是实现系统性测试和连续性管理的有效途径。本标准基于上述最佳实践，提出一套面向软件自主可控能力进行系统性测试的方法论，以网络靶场为载体实现测试过程监测和测试结果的连续性管理，旨在帮助软件研制单位和使用单位提升自主可控能力的测试能力和管理水平。
2. **协作单位**参与本标准编制工作的主要单位及其分工如下：奇安信科技集团股份有限公司负责确立标准的方向和定位、管理标准编制的进度和质量、组织评审和改进等工作；软极网络技术（北京）有限公司负责制定标准的主体架构、编写主体内容、与各协作单位的沟通等工作；中关村华安关键信息基础设施安全保护联盟负责组织专家资源进行各阶段的评审，确保标准的引领性、实用性和规范性；工业互联网研究院、可信华泰科技有限公司、北京大学、长沙市轨道交通运营有限公司等单位基于各自实践经验对标准的相关章节进行编写或补充，以提升标准的实用性。各单位分工协作，共同完成了本标准的编制。
3. **主要工作过程**
   - **立项筹备阶段**：对两个测试机构、三个基于网络靶场进行软件自主可控能力测试项目的开发人员、交付人员和用户进行调研，梳理软件自主可控能力测试的现状和需求，发现存在以下问题：1）软件自主可控能力测试缺乏规范性；2）软件自主可控能力历次测试结果缺乏关联性管理；3）在没有网络靶场的情况下，对于自主可控软件的安全性只能做简单的合规性测试，难以进行复杂环境下的攻防测试，更无法进行上线运行后的的持续性检测。总结一套基于网络靶场进行软件自主可控能力测试的方法论，指导软件开发者、使用者和测试机构系统化、规范化地开展测试活动和管理测试结果是非常必要的。
   - **起草阶段**：起草组由各参编单位的代表组成，其中包括了自主可控软件的开发单位、使用单位和测试机构，以确保编制的测试指南符合不同角色的使用需求。起草阶段的主要工作内容包括：1）收集国内外相关的标准文档，作为制定本标准的参考材料，同时保证本标准的创新性；2）收集、整理相关市场项目的测试方案，从中吸取成功的做法；3）详细讨论测试评估工作各环节，确定本标准的框架和各部分的主要内容；4）分工写作；5）多轮次评审优化。

- **征求意见阶段（如果已经进行部分征求意见工作）：**已经开展了部分征求意见工作，以邮件和会议方式向具有基于网络靶场开展软件测试经验的企业用户征求意见，并吸纳反馈的意见进行优化。

二、标准编制原则和确定标准主要内容的依据

1. **编制原则**
   - 本标准起草过程中，在文件编制原则、文件结构的合理性、术语和定义的规范性等方面，严格按照 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》进行。
   - **科学性与合理性：**本标准中测试方法的选择、测试要素的确定等是基于最佳实践总结提炼的，经过科学论证具有普遍适用性，从而确保测试指南在实际应用中的可行性和有效性。
   - **通用性与适用性：**本标准中的测试方法是基于最佳实践总结提炼的，而且在标准编制各阶段向软件产品研制单位、使用单位、测评机构等相关方广泛征求意见，遵循文件使用者原则编制文件，从而确保符合实际工作场景需求，能够指导各相关方。
2. **确定标准主要内容的依据**
   - **范围确定依据：**在提升软件自主可控能力的总体目标下，有效的测试方法是非常必要的，但行业缺少对软件自主可控能力进行系统性测试的方法指导；与此同时，前沿实践证明基于网络靶场开展测试活动可实现对测试过程和结果的持续性管理，因此本标准定位为“基于网络靶场对软件自主可控能力进行持续性测试的方法论”，旨在弥补软件自主可控能力系统性测试方法这一缺失。
   - 本标准引用 GB/T 25069、GB/T 36630.1、GB/T 39412 - 2020、GB/T 43848 – 2024 文件，为术语的定义提供支持；引用 T/CSAC 001 – 2023 文件，参考其在仿真测试中测试环境搭建的步骤。
   - **术语和定义依据：**标准中界定的术语和定义，部分继承本系列标准的框架标准，如自主可控；部分参考现有国家标准，如安全可控、代码安全审计、开源许可证；部分基于行业惯例进行定义，如仿真测试、实网测试、安全众测；部分基于本标准特定需求进行定义，如软件资产、测试要素。

三、主要试验（或验证）的分析、综述报告，技术经济论证，预期的经济效果

1. **主要试验（或验证）情况**本标准是在若干最佳实践的基础上总结形成的方法论，其可行性已经过实践验证。实践是基于政务系统和科研系统开展的，详细信息不便公开。
2. **技术经济论证**
   - **技术可行性论证：**本标准涉及的网络靶场技术、软件分析技术等均为成熟技术，具备相关技术和产品的用户，可依据本标准的方法、结

合自身的业务需求和管理需求进行测试流程配置，开展测试工作。用户在选择网络靶场技术和产品时应考察其是否支持软件全生命周期测试的关联管理。

- **经济合理性论证**：采用本标准进行软件自主可控能力测试，需要用户建设网络靶场进行测试环境搭建、测试任务执行和测试结果管理，但通过提高软件质量、保障网络安全将带来更长远的受益。

3. **预期的经济效果**本标准实施后，将对软件产业发展起到积极的推动作用，通过提高软件产品的安全性和竞争力，加速国产化替代，从而为软件企业带来市场份额增长和经济效益提升；对使用软件的企业或组织而言，降低停服断供、软件后门等安全风险，避免可能由此带来的经济损失。

四、采用国际标准和国外先进标准的程度，以及与国际、国内同类标准水平的对比情况

1. **国际标准采用情况**未采用国际标准。
2. **与国际、国内同类标准对比**
   - **与国际同类标准对比**：国外没有自主可控相关标准可供参考。
   - **与国内同类标准对比**：国内具有多种网络安全测试相关标准，但通常是面向某一种场景的安全要求或测试方法，例如代码安全审计、基于网络仿真环境的测试等，缺失连续性安全管理，也缺少自主可控能力的综合性测试管理。本标准的创新性在于：1）面向自主可控能力的测试；2）对于软件资产历次测试的结果进行关联管理。

五、与有关的现行法律、法规和强制性国家标准的关系

本标准遵从《中华人民共和国国家安全法》、《中华人民共和国网络安全法》、《关键信息基础设施保护条例》、《网络安全审查办法》等现行的法律法规。本标准参考了网络安全测试相关的推荐性国家标准；在相关领域尚无强制性标准，不存在冲突之处。

六、重大分歧意见的处理经过和依据

在标准编制过程中未出现重大分歧意见。

七、标准作为强制性标准或推荐性标准的建议

从行业发展的多样性和灵活性考虑，建议本标准作为推荐性标准。

八、贯彻标准的要求和措施建议

1. **贯彻标准的要求**贯彻本标准，要求相关单位应具备网络靶场环境和软件生命周期各阶段涉及的测试软件、测试工具等，测试人员应掌握制定测试方案、搭建测试环境、执行测试任务、分析测试结果所需的知识和技能。
2. **措施建议**

- **培训措施**：建议相关方（软件研制单位、使用单位和测评机构）开展培训工作，针对标准内容组织培训课程，提高相关人员对标准的理解和执行能力。
- **激励措施**：建议行业主管部门，对于按照标准要求开展软件自主可控能力测试工作并取得一定收效的相关方（软件研制单位、使用单位和测评机构）给与奖励，扩大其示范效应。

九、废止现行有关标准的建议

不涉及。

十、其他应予说明的事项

无。