CNAS-CL01-A020

检测和校准实验室能力认可准则在信息安全检测领域的应用说明

Guidance on the Application of Testing and Calibration Laboratories Competence Accreditation Criteria in the Field of Information Security Testing

中国合格评定国家认可委员会

2018 年 03 月 01 日 发布　　2018 年 09 月 01 日 实施

前 言

本文件由中国合格评定国家认可委员会（CNAS）制定，是结合信息安全检测的特点对 CNAS-CL01《检测和校准实验室能力认可准则》中的部分条款的应用说明，并不增加或减少该认可准则的要求。

本文件与 CNAS-CL01《检测和校准实验室能力认可准则》同时使用。

在结构编排上，本文件章、节的条款号和条款名称均采用 CNAS-CL01:中章、节条款号和名称，对 CNAS-CL01 应用说明的具体内容在对应条款后给出。

本文件代替 CNAS-CL46:2013《检测和校准实验室能力认可准则在信息安全检测领域的应用说明》。

本次修订主要根据 CNAS-CL01:2018《检测和校准实验室能力认可准则》对章节号重新进行了编排，并按照 CNAS 的统一要求调整文件编号。

检测和校准实验室能力认可准则在信息安全检测领域的应用说明

1 范围

本文件适用于所有从事信息安全检测的实验室。

2 引用文件

CNAS-CL01:2018《检测和校准实验室认可准则》

3 术语和定义

4 通用要求

4.1 公正性

4.1.3 如果实验室所在的组织从事信息安全检测以外的活动（例如，涉及信息安全相关的开发），应承诺并采取措施确保不利用被检测信息安全相关方的知识产权牟取利益。

4.1.4 实验室应建立并保持从事信息安全检测公正性和诚实性的政策和程序，并确保信息安全检测人员不参加被测对象的开发和咨询，确保实验室检测人员与产品开发商、系统集成商、安全集成商、其他有利害关系和可能影响检测结果的人员之间相互分离。

5 结构要求

6 资源要求

6.2 人员

6.2.2 信息安全检测实验室的人员应满足以下要求：

a) 信息安全检测人员应具有信息安全、计算机、通信或网络等相关专业本科或以上学历，从事信息安全检测工作 1 年以上，且至少参与过 3 个信息安全检测项目。

b) 信息安全检测领域的授权签字人和意见解释人员应具有信息安全、计算机、通信或网络等相关专业本科或以上学历，从事信息安全检测工作 3 年以上，且至少参与过 5 个信息安全检测项目。

c) 实验室人员应经过相关培训，考核通过后方能上岗。实验室人员还应接受安全保密和知识产权保护方面的培训，以确保客户利益和商业机密不被泄露。

d) 实验室应：

1) 至少具有 5 名信息安全检测人员；

2) 由熟悉信息安全项目管理、开发、测试及标准、规范、规程的技术人员负责组织实施信息安全检测任务；

3) 由熟悉信息安全检测过程、标准/规范/规程，信息安全质量评价和信息安全测试质量评价的人员，负责信息安全检测过程和产品的规范符合性审核监督；

4) 由熟悉信息安全测试需求、测试结果评价和判定准则的人员负责对信息安全测试输入和测试结果进行核查。

6.3 设施和环境条件

6.3.1 实验室应建立稳压、防静电和防范恶意代码的检测环境。实验室还应对检测环境在使用前进行核查。

6.3.4 b) 检测网络应与其他网络采取隔离措施。如果同时进行多个检测项目，实验室应保持检测环境的有效分离。当检测活动在实验室以外场所进行时，其检测环境也应满足要求，并确保检测活动在受控环境下执行。当通过实验室以外的网络实施远程检测时，应注意影响网络正常运行的环境条件。

6.4 设备

6.4.1 信息安全检测设备应包括硬件设备和软件检测工具。实验室应在每个项目测试前对检测设备进行核查。对于性能检测项目，实验室所选用的设备应是具有可追溯性的商用软件和硬件。

6.4.13 实验室应保存所有检测设备的档案。实验室的记录还应包括检测设备的配置信息、软件检测工具所需运行环境等信息。软件测试工具的不同版本，均应有唯一性标识。

6.5 计量溯源性

6.5.3 对于新的或发生了重大变化的无法进行外部溯源的方法和测试工具，实验室应采取措施检查测试方法和测试工具的有效性，检查措施可包括：

a) 适用时，对特定的信息安全产品样例进行检测，审查信息安全产品样例预埋问题的复现情况，确认其偏差。

b) 适用时，应溯源到权威的测试集规范或其它有关的权威标准或规范。

7 过程要求

7.1 要求、标书和合同的评审

7.1.1a) 实验室合同评审为签订信息安全检测合同而进行评审的政策和程序应包括：

1) 对检测项目的保密和知识产权保护要求，在合同中（或签订专门的协议）应予明确、充分规定。

2) 对检测项目结束后如何处置检测对象应予以规定。

7.2 方法的选择、验证和确认

7.2.1.3 实验室应确保测试使用的检测样本集（如病毒样本库、网络攻击数据包、漏洞库等）为最新版本。

7.4 检测或校准物品的处置

7.4.1 实验室应向客户提供充分的保证，确保测试工具或测试集不会将病毒或其他损坏因素引入到属于客户的硬件或软件中。检测完成后，实验室应按合同要求处置被测样品，并保留记录。

7.4.3 在接收检测样品时，实验室应对检测对象进行病毒检查并记录结果。

7.5 技术记录

7.5.1 检测记录应能够追溯到检测人员的操作和工作方法及检测环境，应详细记录检测环境配置（硬件和软件）、参数设置等信息，确保该检测在尽可能接近原条件的情况下能够重复。当被测对象包括软件时，实验室应建立配置管理的程序，确保测试记录与被测对象的一致性。

7.5.2 实验室应有措施保持同一技术记录的不同形态的内容修改、版本控制的一致性。

7.7 确保结果的有效性

7.7.1 实验室制定有效的质量监控方案还应包括：

a) 由同一检测人员对被测对象进行重复检测；

b) 由不同的检测人员使用相同方法对同一被测对象进行检测；

c) 使用不同的检测方法（技术）或同一类型的不同仪器或工具对同一被测对象进行检测。

实验室应保存监控活动的记录，包括对比对测试结果的评价。

7.8 报告结果

7.8.1 总则

7.8.1.2 实验室以电子方式传输的检测报告应使用加密方式传输，以确保检测报告的完整和保密。

7.11 数据控制和信息管理

7.11.3 实验室应建立数据（尤其是涉及到客户敏感数据、知识产权、安全缺陷等的检测数据、电子和纸质记录以及其他的材料）保护程序，以防止非授权人员的访问。当检测结束后，实验室应妥善删除检测过程中在被测对象上生成的测试数据（如：端口、策略、账号、口令等）。

注：纳入配置管理的电子版软件测试技术文档，可通过文档修改表记录版本号、修改内容、日期、修改人、审核人等信息的方式保持不同介质实物资料版本的一致；纳入受控管理的其他技术记录，可通过适合不同介质的加注方式记录修改内容、日期、修改人、审核人等信息。

8 管理体系要求

8.3 管理体系文件的控制（方式A）

8.3.2 实验室应有规定和措施，确保计算机系统中的文件与其它载体上的文件在

内容、修订、版本控制、发布、存档等方面的一致性。

8.7 纠正措施（方式A）

8.7.1b) 信息安全检测活动产生问题的原因还可能是：恶意代码、检测操作顺序、软件版本、参数设置、漏洞库、攻击特征库等。