CNAS-CL46

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

2013 年 09 月 01 日 发布　　2015 年 06 月 01 日第一次修订　　2015 年 06 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-CL01：2006《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-CL01：2006《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-CL01:2006 中章、节条款号和名称，对 CNAS-CL01:2006 应用说明的具体内容在对应条款后给出。

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

1.2 本文件适用于所有从事信息安全检测的实验室。

2 引用标准

检测和校准实验室认可准则（CNAS-CL01:2006）

3 术语和定义

4 管理要求

4.1 组织

4.1.4 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；并且不应当承担所在组织研发的信息安全产品的第三方检测活动，以避免影响其判断独立性和检测诚信度。

4.1.5 实验室应：

a) 安排由熟悉项目管理、信息安全开发技术、信息安全测试技术及其标准、规程和规范的技术人员负责组织、实施信息安全检测任务。

c) 有政策和程序确保与被测对象的信息安全相关各方的机密信息和知识产权得到保护。至少应对检测过程、电子储存、检测结果传输的信息保护方式进行描述，避免信息的泄露和不当使用给被测对象的运行构成潜在安全风险。应制定并签署书面保密承诺书。

d) 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。

e）应具有至少 5 名满足 5.2 要求的信息安全检测技术人员，并应拥有与其检测任务相适应的场地、设施、设备、检测工具等资源。

g）由熟悉信息安全的检测过程、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；

h) 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监督，并应具有 1 名信息安全检测领域的技术负责人。

4.2 管理体系

4.3 文件控制

4.3.3.4 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。

4.4 要求、标书和合同的评审

4.4.1 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：

a）对检测项目的机密保护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。

b）对检测项目结束后如何处置检测对象应予以规定。

4.5 检测和校准的分包

4.6 服务和供应品的采购

4.7 服务客户

4.8 投诉

4.9 不符合检测和/校准工作的控制

4.10 改进

4.11 纠正措施

4.11.2 原因分析

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。

4.12 预防措施

4.13 记录的控制

4.13.1 总则

4.13.1.2 所有的记录应注明日期和签名，其保存期限应至少满 1 个认可周期，或按照客户要求的时限保存。

4.13.1.3 实验室应有程序确保所有的记录（包括任何形式的记录）的准确性、完整性和保密性。

4.13.1.4 以电子形式存储的记录应有相关人员标识和日期的信息，这些记录应有适当的标识和备份，应符合实验室的政策并确保记录的完整性，防止未经授权的访问和修改。

4.13.2 技术记录

4.13.2.1 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，以保证测试记录与被测对象的一致性。

4.13.2.3 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。

4.14 内部审核

4.15 管理评审

5 技术要求

5.1 总则

5.2 人员

5.2.1 从事信息安全检测的实验室应确保与技术有关的人员具备信息安全检测的能力。

信息安全检测人员应具有信息安全、计算机软硬件、通信或网络等相关专业本科或以上学历，至少 3 个信息安全检测项目的经历，且具有 1 年以上信息安全检测工作经历。

信息安全检测领域的技术负责人、授权签字人和意见解释人员应具备信息安全检测人员的专业背景，参加至少 5 个信息安全检测项目，且具有 3 年以上信息安全检测工作经历；实验室人员应接受过安全保密、知识产权保护方面的专门教育，并应具备安全保密意识和知识产权保护意识，以确保客户利益和商业机密不被泄露。

5.2.2 实验室的员工应经过相关培训、考核通过后方能上岗。实验室应保留所有技术人员（包括签约人员）的相关授权记录。

5.3 设施和环境条件

5.3.2 实验室应建立稳压、防静电和防范恶意代码的检测环境。例如：实验室应具备有效的恶意代码防护和软件/数据备份程序。实验室还应对检测环境在使用前进行核查。

5.3.3 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。

注：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。

5.4 检测和校准方法及方法的确认

5.4.1 总则

实验室应按照检测方法制定可操作的文件化程序。信息安全检测所采用的检测方法可能涉及：检测样本集（如病毒样本库、网络攻击数据包、漏洞库等）、检测用例集以及检测工具/平台等。所有检测方法都应经过适当的验证、确认及其文件化管理。实验室应确保测试使用的检测样本集为最新版本。

5.4.2 方法的选择

当有产品检测方法时，实验室应使用产品检测方法。

5.4.7.2 b) 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）。

5.5 设备

5.5.2 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。实验室应确保检测设备满足信息安全产品检测的要求。对于性能检测项目，实验室还应具备性能测试能力。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。

5.5.4 软件测试工具的不同版本，均应有唯一性标识。

5.5.5 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。

5.6 测量溯源性

5.6.2.2 检测

5.6.2.2.2 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，确认报告应指明可溯源到权威的测试集规范或其它有关的权威标准或规范。

5.7 抽样

5.8 检测和校准物品（样品）的处置

5.8.3 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。

5.8.4 实验室应向客户提供充分的保证，保证检测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。检测工作完成后，实验室应按合同要求的检后处置方式处置被测对象，并保留记录。

5.9 检测和校准结果质量的保证

5.9.1 实验室制定的质量控制计划还应包括：

（1）由同一检测人员对被测对象进行重复检测；

（2）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；

（3）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。

质量控制活动应有计划和实施记录，包括对比对测试结果的评价。

5.10 结果报告

5.10.7 结果的电子传送

实验室以电子方式传输的检测报告应使用电子签名或者以加密方式传输，以确保检测报告的完整性、机密性以及真实性。

——