附件4

数字产品数据安全和隐私保护

检验检测机构能力要求

#### Requirements for the Capability of Digital Product Data Security and Privacy Protection Inspection and Testing Organization

（征求意见稿）

中国出入境检验检疫协会 发布

2024-XX-XX实施

2024-XX-XX发布

P/CIQA-199-2024

团体标准

ICS 35.240

CCS L 80

目录

[前言 I](#_Toc177706478)

[1 范围 1](#_Toc1710506416)

[2 规范性引用文件 1](#_Toc117751323)

[3 术语和定义 1](#_Toc1214046774)

[4 一般要求 1](#_Toc760867257)

[4.1 公正性 1](#_Toc1778354161)

[4.2 保密性 1](#_Toc120984981)

[5 组织结构要求 2](#_Toc1875045605)

[6 人员要求 2](#_Toc1716447157)

[7 设施与设备要求 2](#_Toc1179537548)

[8 过程要求 3](#_Toc1066023779)

[8.1 检测方法和程序 3](#_Toc205586732)

[8.2 检测样品的处置 3](#_Toc2142500348)

[9 检测记录与报告要求 3](#_Toc2145039587)

[9.1 检测记录 3](#_Toc1872356520)

[9.2 检测报告 3](#_Toc1618152149)

[10 管理体系要求 3](#_Toc550262635)

[参考文献 4](#_Toc1199522463)

1. 前言

本文件按照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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中国出入境检验检疫协会网络安全标准化技术委员会（CIQA/TC16）提出并归口。

本文件起草单位：北京时代新威信息技术有限公司、北京爱思考科技有限公司、北京数易轩科技有限公司、… …。

本文件主要起草人：… …。

本文件知识产权归中国出入境检验检疫协会所有。任何单位或个人未经许可，不得以营利为目的，印制、出版、翻译、转发或复制全文或部分文字。

本文件是首次发布。



数字产品数据安全和隐私保护检验检测机构能力要求

* 1. 范围

本文件规定了对数字产品数据安全和隐私保护检验检测机构的能力以及从事检测活动的公正性和一致性的要求。

本文件适用于数字产品数据安全和隐私保护检验检测机构能力建设、合格评定等活动。

* 1. 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 27000 合格评定 词汇和通用原则（ISO/IEC 17000，IDT）

CNAS-CL01 检测和校准检验检测机构能力认可准则（ISO/IEC 17025）

* 1. 术语和定义

GB/T 27000界定的以及下列术语和定义适用于本文件。

数字产品　digital products

消费者日常生活、工作中使用的智能化、可联网的数字终端设备。主要包括：智能办公产品、智能娱乐产品、智能健康产品、智能穿戴产品、智能车联网产品、智能监控设备、智能无人机、智能机器人等。

隐私privacy

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

检验检测机构 inspection and testing organization

具备数字产品数据安全和隐私保护检测能力的组织。

* 1. 一般要求

公正性

* + 1. 检验检测机构应公正地实施检测活动，并从组织结构和管理上保证公正性。
    2. 检验检测机构应对检测活动的公正性负责，坚决抵制商业、财务或任何其他形式的外部压力，以确保检测结果的客观性和准确性。
    3. 检验检测机构应持续监控并识别可能影响公正性的潜在风险。一旦发现此类风险，应立即采取措施消除或将其降至最低，并保留相应证据以证明所采取措施的有效性。

保密性

* + 1. 检验检测机构对在检测过程中获取或产生的所有信息负有严格的管理责任。除非客户已公开或双方另有协议，否则所有信息均应被视为机密，予以严格保密。
    2. 检验检测机构应建立健全的保密管理制度，明确保密责任人，确保信息的保密性、安全性和可控性。同时，应采取先进的技术和管理手段，如数据加密、访问控制等，以防止信息泄露或被非法使用。
  1. 组织结构要求
  2. 检验检测机构应是在中华人民共和国境内依法成立并能够承担相应法律责任的法人。不具备独立法人资格的检验检测机构应当经所在法人单位授权。
  3. 检验检测机构对其出具的检测数据、结果负责，并承担法律责任。

全：对送检产品

* 1. 检验检测机构应规定检验检测机构的组织和管理体系（结构），明确与检测活动相关部门、人员的职责以及相互关系。
  2. 检验检测机构应充分识别检测活动中可能产生的风险，并通过多种措施对可能面临的风险加以规避和控制，并保留风险识别和对应措施的评审记录。
  3. 检验检测机构应获得《中国合格评定国家认可委员会检验检测机构认可证书》。
  4. 人员要求
  5. 检验检测机构应制定人员管理制度，其中包括人员录用、考核、日常管理、离职、保密协议等方面的内容和要求。
  6. 检验检测机构应当具有与其从事检测活动相匹配的检测技术人员和管理人员。总检测技术人员应不少于10人，且针对每一独立产品检测领域，确保至少配备两名专业技术人员，以保障检测工作的专业性和深度。
  7. 检测人员应理解和掌握数字产品相关技术标准，熟悉数字产品数据安全和隐私保护检测方法、流程和工作规范等方面的知识，具有依据检测结果做出专业判断以及出具检测报告等任务的能力。
  8. 检测人员应具有中国出入境检验检疫协会颁发的网络安全检测人员认证证书或国家、行业认可的网络安全相关的资格证书。授权签字人应具备网络安全、数据安全专业知识，取得国家或行业认可的与网络安全、数据安全相关的资格证书。
  9. 检验检测机构应在管理层中分别任命一名技术主管和质量主管，分别全面负责检测技术工作和质量管理工作。
  10. 设施与设备要求
  11. 检验检测机构应具有固定的办公场所和专业机房，配备满足数字产品数据安全和隐私保护检测业务需要的设备、设施，配备必要的专业检测、分析工具。
  12. 检测工具使用前需进行版本核验，确保为最新版本（包括规则库、插件等）。检验检测机构自行研发的工具需经过功能性、安全性和结果准确性验证，并保留验证记录，以保障检测设备和工具运行状态良好，并通过定期更新、升级维持检测数据的准确习惯。
  13. 检验检测机构采用的与检测活动相关的管理系统、设备设施的核心技术及关键部件宜优先选择具备我国自主知识产权的产品，以强化技术自主性和安全性。
  14. 检验检测机构应建立设备管理制度，明确设备设施管理职责，规范仪器设备的采购、使用、维护及运行管理的各个环节，确保检验检测机构运行的高效与合规。
  15. 过程要求
  16. 检测方法和程序
      1. 检验检测机构应制定检测过程管理程序（如检测方法、检测前准备、检测方案编制、检测管理、检测报告编制以及相应的作业指导书、记录等），并确保现行有效，便于检测人员获取、阅读。
      2. 检验检测机构应确保使用最新有效版本的检测方法。
      3. 如果检验检测机构的检测活动现场涉及数字产品部件或固件的拆解作业，应制订安全实施拆解作业指导书，并配备必要的保护设备。
  17. 检测样品的处置
      1. 检验检测机构应采取措施避免被测产品（样品）在检测期间可能发生的风险。必要情况下，应告知被测产品（样品）提供方检测过程中可能产生的风险，与产品提供方确认规避风险的保护措施，并经过被产品提供方书面确认。
      2. 检测完成后，被测样品原则上由检验检测机构保管至留存期满。期满后，检验检测机构负责销毁。若样品提供方请求取回样品，检验检测机构应明确告知相关风险，经双方签署书面同意书后，方可允许取回。

1. 检测记录与报告要求

9.1 检测记录

* + 1. 检测记录应规范、清晰。检测记录均需检测人员签字确认。
    2. 检验检测机构应保存检测工具的升级或维护记录，至少应包括工具名称、工具版本、升级后的最新版本、升级日期和升级维护责任人等。
    3. 检验检测机构应保存检测工具的病毒或恶意代码检查记录。
  1. 检测报告
     1. 检验检测机构应按照CNAS-CL01检测和校准检验检测机构能力认可准则（ISO/IEC 17025）第7.8条的要求出具数字产品数据安全与隐私保护检测报告。
     2. 检测报告应包括所有检测结果、根据检测结果做出的专业判断以及理解和解释这些结果所需要的所有信息，以上信息均应正确、准确、清晰地表述。

10 管理体系要求

检验检测机构应建立符合CNAS-CL01检测和校准检验检测机构能力认可准则（ISO/IEC 17025）第8章要求的管理体系。

参考文献