NIST Special Publication 800-70 Revision 4

IT 产品国家检查列表计划 - 用户和开发人员检查列表指南

翻译 樊山

（仅以此文给尚在病榻的挚友）

Stephen D. Quinn

Murugiah Souppaya

Melanie Cook

Karen Scarfone

本出版物可从 https://doi.org/10.6028/NIST.SP.800-70r4 免费获取

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-70 Revision 4

IT 产品国家检查列表计划 - 检查列表用户和开发人员指南

Stephen D. Quinn

Murugiah Souppaya

Melanie Cook

计算机安全部信息技术实验室

Karen Scarfone

Scarfone Cybersecurity

Clifton, VA

本出版物可从 https://doi.org/10.6028/NIST.SP.800-70r4 免费获取

February 2018

美国商务部长 Wilbur L. Ross，Jr.秘书

美国国家标准与技术研究院院长 Walter Copan，美国国家标准和技术研究院 NIST 负责人兼商务部副部长

目录

译者申明

本次翻译工作主要由自由职业者樊山完成，限于翻译水平及能力问题，文稿中还存在很多瑕疵，诚请各位读者在阅读过程中不吝指正。

本文原文可在美国 NIST 官方网站下载，本翻译为公益翻译。仅供参考，建议阅读范围：网络运营者、网络运营商、CERT、政府网络安全管理机构等。

诚请更多爱好者加入这项工作。

邮箱：fanfox7405@163.com 微信号：tianyx74

2018 年 2 月 25 日

权威

本出版物由 NIST 根据 2014 年联邦信息安全现代化法案（FISMA）44 美国法令§3551 及以下公法（P.L.）113-283 的法定责任制定。NIST 负责制定信息安全标准和准则，包括对联邦信息系统的最低要求，但这些标准和准则不适用于国家安全系统，未经适当的联邦官员对这些系统行使政策权限的明确批准。 本指南符合管理和预算局（OMB）A-130 号通告的要求。

本出版物中没有任何内容应该与商务部长根据法定权力制定的强制性和对联邦机构具有约束力的标准和指导方针相抵触。 这些准则也不应被解释为改变或取代商务部长，OMB 主任或任何其他联邦官员的现有权力。本出版物可由非政府组织自愿使用，且不受美国版权保护。 但是，NIST 会认可归属。

National Institute of Standards and Technology Special Publication 800-70 Revision 4 Natl. Inst. Stand. Technol. Spec. Publ. 800-70 Rev. 4, 52 pages (February 2018) CODEN: NSPUE2

本出版物可从 https://doi.org/10.6028/NIST.SP.800-70r4 免费获取

计算机系统技术报告

美国国家标准与技术研究院（NIST）的信息技术实验室（ITL）通过为国家测量和标准基础设施提供技术领导来促进美国的经济和公共福利。 ITL 开发测试，测试方法，参考数据，概念验证实施和技术分析，以促进信息技术的发展和生产性使用。 ITL 的职责包括制定管理，行政，技术和物理标准以及联邦信息系统中除国家安全相关信息之外的具有成本效益的安全和隐私准则。 SP 800 系列报告了 ITL 在信息系统安全方面的研究，指导方针和推广工作，以及与行业，政府和学术机构的合作活动。

摘要

安全配置检查列表是一份文档，其中包含将信息技术（IT）产品配置到操作环境，验证产品配置是否正确和/或识别对产品进行未经授权的更改的说明或过程。使用这些检查列表可以最小化攻击面，减少漏洞，减少成功攻击的影响，并识别可能未被发现的更改。 为了便于制定检查列表并使检查列表更加有组织和可用，NIST 建立了国家检查列表计划（NCP）。本出版物解释了如何使用 NCP 查找和检索检查列表，还介绍了参与 NCP 的政策，程序和一般要求。

关键词

变化检测；检查列表；信息安全；国家检查列表计划（NCP）；安全配置检查列表；安全内容自动化协议（SCAP）；软件配置;漏洞

致谢

美国国家标准与技术研究院（NIST）的作者 Stephen Quinn，Murugiah Souppaya 和 Melanie Cook 以及 Scarfone 网络安全的 Karen Scarfone 希望感谢所有参与 SP 800-70 修订的个人和组织。 贡献者包括 NIST 的 Harold Booth，Bob Byers 和 David Waltermire；可可系统公司的 Harold Owen，Christopher Turner 和 Chuck Wergin；G2 公司的 Tim Lusby 和 Dragos Prisaca

作者承认以下帮助开发 SP 800-70 早期版本的个人和组织：

- 苹果
- Booz Allen Hamilton：Paul Cichonski，Anthony Harris 和 Paul M. Johnson
- 互联网安全中心（CIS）：Clint Kreitner
- 疾病控制和预防中心（CDC）
- 国防信息系统局（DISA）：Terry Sherald
- 能源部（DOE）
- G2，Inc.：Greg Witte
- 微软公司：Chase Carpenter，Kurt Dillard 和 Jesper Johansson
- 国家安全局（NSA）：Paul Bartock，Trent Pitsenbarger 和 Neal Ziring
- NIST：John Banghart，Matt Barrett，Harold Booth，David Ferraiolo，Timothy Grance，Blair Heiserman，Jeffrey Horlick，Arnold Johnson，Suzanne Lightman，Mark Madsen，Edward Roback，Ron Ross，Michael Rubin，Carolyn Schmidt，Matt Scholl 和 John Wack（原始版本的合作者）
- Sun Microsystems：Glenn Brunette
- 赛门铁克公司

NIST 还要感谢国土安全部对 NIST IT 产品国家检查表计划的赞助和支持。

读者

本文件是为公共和私营部门的现有和潜在检查列表开发人员和用户编写的。 检查列表开发人员包括信息技术（IT）供应商，财团，行业，政府组织以及公共和私营部门组织中的其他人员。 检查列表用户包括政府机构，企业，小型企业和其他组织中的最终用户，系统

管理员和 IT 经理以及私人公民。 假定本文档的读者熟悉一般的计算机安全概念。

商标信息

执行摘要

安全配置检查列表（也称为锁定，强化指南或基准）是一系列指令或过程，用于将 IT 产品配置到特定的操作环境，用于验证产品是否已正确配置，和/或用于识别未经授权的产品变更。 IT 产品可能是商业的，开源的，政府现成的（GOTS）等等。

检查列表可以包含模板或自动脚本，补丁信息，可扩展标记语言（XML）文件和其他程序。 检查列表旨在由每个组织量身定制，以满足其特定的安全和操作要求。通常，IT 供应商为他们自己的产品创建核对检查列表; 然而，其他组织也会创建检查列表，例如学术界，财团和政府机构。使用精心编写的标准化检查列表可以显着降低 IT 产品的漏洞风险。 检查列表可以特别有助于小型组织以及资源有限的个人保护其系统。

NIST 维护国家检查列表存储库，该存储库是一个公开可用的资源，其中包含有关特定 IT 产品或 IT 产品类别的各种安全配置检查列表的信息。该存储库位于 https://checklists.nist.gov/，包含描述每个检查表的信息。该存储库还包含一些检查列表的副本，主要是由联邦政府开发的检查列表，并与其他本地检查检查列表有关。用户可以使用各种标准浏览和搜索存储库以查找特定的检查列表。 拥有一个集中的检查列表存储库使组织可以更轻松地找到最新的权威版本的安全检查列表并确定哪些最能满足他们的需求。

本文档面向安全配置检查列表的用户和开发人员。 对于检查列表用户，本文提供了如何从 NIST 国家检查列表存储库中选择检查列表，评估和测试检查列表并将其应用于 IT 产品的建议。 对于检查列表开发者，本文阐述了参与 NIST 国家检查列表计划（NCP）的政策，程序和一般要求。

本文件中为检查列表用户和开发人员提出的主要建议包括以下内容：

组织应该将检查表应用于操作系统和应用程序，以减少攻击者可以尝试利用的漏洞数量，并降低成功攻击的影响。

没有任何检查列表可以使系统或产品 100％安全，使用检查列表不会消除对正在进行的安全维护（例如修补程序安装）的需要。 然而，使用检查列表强调系统对软件缺陷（例如，通过应用补丁和消除不必要的功能）并安全配置系统通常会减少系统受到攻击的方式数量，从而提高产品安全级别并保护免受未来的威胁。 检查列表还可用于验证系统评估的某些类型安全控制的配置，例如确认符合某些联邦信息安全现代化法案（FISMA）要求或其他安全要求。

联邦机构在可用时必须使用 NCP 的适当安全配置检查列表。 2017 年 1 月，联邦采购法规（FAR）第 39 部分进行了更新。第 39.101 段（c）段规定：“在获取信息技术时，各机构应包括适当的信息技术安全政策和要求，包括使用国家标准与技术研究院网站 https://checklists.nist.gov。代理签约官员应与需要的官员协商，以确保纳入适当的标准。”[1]另外，FISMA 要求各联邦机构确定最低限度可接受的系统配置要求并确保其符合要求[2]。因此，联邦机构以及联邦政府产品供应商应该使用 NIST 资源库获取或实施和共享这些检查列表。 NIST 鼓励核对检查列表开发人员对 NIST 特别出版物（SP）800-53 中所描述的安全控制进行断言，以促进联邦机构的 FISMA 合规性检查。[1]

组织在 IT 产品选择过程中应考虑安全配置检查列表的可用性。

在选择检查列表时，检查列表用户应仔细考虑每个检查列表的自动化程度，来源，标准使用情况和其他相关特性。

NIST 认识到一些检查列表比其他检查列表更加自动化和基于标准。 例如，非自动检查列表提供了基于形式化的关于人员如何手动更改产品配置的描述。 自动检查列表是机器可读的。 完全遵守安全内容自动化协议（SCAP）的自动检查列表（也称为 SCAP 内容）具有以标准化 SCAP 格式记录的所有安全设置; 已使用 NIST SCAP 内容验证工具（SCAPVal）2 进行语法测试，以符合 SCAP 相关规范; 并包括低级安全设置和高级安全性要求之间的映射。

当针对特定产品提供多个检查列表时，组织应考虑每个检查列表标准的自动化程度和使用情况。 一般来说，SCAP 检查列表可以比其他检查列表更加一致和高效地使用。 检查表之间可能有其他显着差异; 例如，一个检查列表可以包括与操作系统（例如，网络浏览器和电子邮件客户端）捆绑在一起的软件，而另一个检查列表仅针对该操作系统。 另一个例子是核对检查列表所依据的假设（例如操作环境）。 核对检查列表用户应该识别这些差异并确定哪些核对检查列表看起来合适，并且需要进一步分析。

核对检查列表来源对于联邦民事机构的用户特别重要，他们应首先搜索政府授权或强制的检查列表（例如，由 FAR 第 39 部分规定）。 一般来说，这些用户应该搜索 NIST 制作的检查列表，这些检查列表是为民间机构使用而量身定制的。 如果没有 NIST 制作的检查列表可用，那么应该使用由国防信息系统局（DISA）或国家安全局（NSA）提供的机构制作的检查列表。 如果政府授权的正式检查列表不存在，鼓励组织使用供应商制作的检查列表。 如果供应商生产的检查列表不可用，则可以使用在 NCP 网站上公布的其他检查列表。

检查列表用户在将其应用于生产系统之前应该对检查列表进行定制和测试。

检查列表对组织来说不是强制性的，应该被视为组织自定义的起点。 虽然这些设置基

于对安全威胁和漏洞的充分了解，但它们无法考虑组织特定的安全和操作要求，现有的安全控制以及其他可能需要更改的因素。 组织应仔细评估检查列表设置并赋予其相当的权重，然后进行必要的更改以使设置适应组织的环境，要求，策略和安全目标。 对于安全需求显着不同的环境，检查列表尤其如此。 所有与检查列表设置的偏差都应该记录下来供将来参考，并且包括每个偏差背后的原因以及偏离设置的影响。

在应用将用于更改产品设置的检查列表之前，用户应首先在非关键系统上进行测试，最好在受控的非操作环境中进行测试。 NIST 存储库中的每个检查表都经过了开发人员的测试，但是开发人员的测试环境和组织的运行环境通常存在显着差异，其中一些差异可能会影响检查列表部署。 在某些情况下，安全控制修改会对产品的功能和可用性或其他产品或安全控制产生负面影响。 因此，执行测试以确定对系统安全性，功能和可用性的影响非常重要；记录测试结果；并采取适当措施解决任何重大问题。

核对检查列表用户在选择核对检查列表时应考虑到其操作环境，检查列表开发人员应将核对检查列表定位到一个或多个操作环境。

当他们可以在通用的操作环境中运行时，检查列表显着更有用。 NCP 已经确定了几个广泛和专门的操作环境，例如独立和管理，至少有一个环境对大多数受众应该是共同的。 通过彻底识别和描述这些环境，用户可以更轻松地选择最适合其特定操作环境的安全检查表，并允许开发人员更好地将检查表定位到与其操作环境相关的一般安全特性。

NIST 强烈鼓励 IT 产品供应商为其产品开发安全配置检查列表并将其提供给 NIST National Checklist Repository。

NIST 鼓励 IT 产品供应商为其产品开发安全配置检查列表，因为供应商在可能的安全配置设置方面拥有最丰富的专业知识，并且能够最好地理解设置如何相互影响和相互影响。

创建安全配置检查列表的供应商应通过 NCP 将其提交纳入国家检查列表存储库。 NCP 以一致的方式提供了开发检查列表的过程和指导。 对于检查列表开发人员，步骤包括初步开发检查列表，检查检查列表测试，根据 NCP 指南记录检查列表，并向 NIST 提交检查列表包。 NIST 根据程序要求筛选核对检查列表，然后发布持续 30 天的公众评论检查列表。 在公众审查期间以及随后的问题解决之后，检查检查列表会在 NIST 检查检查列表存储库中与其信息一起列出。 检查列表维护可能由供应商执行，导致发布更新的检查列表。 当 NIST 过期或不正确时，NIST 会退还或归档检查列表。

1. 介绍

1.1 目的和范围

本文档介绍了检查列表的使用，优点和管理，并解释了如何使用 NIST 国家检查列表计划（NCP）来查找和检索检查列表。 该文件还介绍了参与 NCP 的政策，程序和一般要求。

1.2 文档组织

第 2 部分包含检查表概述，描述 NIST NCP 的优势及其工作原理。

第 3 节提供了关于 NCP 中使用的预定义检查表操作环境的其他详细信息，以帮助开发人员创建符合安全实践的检查列表。 第 3 部分介绍的材料也可以帮助检查列表用户选择最适合其自身运营环境的检查列表。

第 4 节包含潜在的检查列表用户的信息。描述如何使用 NCP 来查找和检索最符合确定需求的检查列表。它还包含关于如何实施检查列表的指导，包括如何分析具体的操作环境，然后根据情况调整检查列表。

第 5 节为当前和未来的检查列表开发人员提供指导。本指南包含有关准备检查列表并将检查列表提交给 NIST 以列入检查列表存储库程序的信息。

附录 A 列出了本文件的参考资料。

附录 B 包含参与 NCP 必须满足的程序和法律要求。

附录 C 包含 NCP 参与和徽标使用协议表格。

附录 D 详细说明了美国政府配置基线（USGCB）检查列表必须符合的附加要求。

附录 E 包含本文档中使用的缩略语列表。

附录 F 提供了本文档中使用的术语的词汇表。

附录 G 提供了文档最新版本的更改日志。

2. NIST 国家检查列表计划

用户计算机面临很多威胁，每天都会发现 IT 产品（例如操作系统和应用程序）中的新漏洞。 修补程序可能不会立即用于新的漏洞，从而导致需要通过重新配置来快速部署临时

缓解措施，直到有可用的修补程序。另外，由于 IT 产品通常面向各种受众，限制性安全设置通常不会默认启用，这意味着很多 IT 产品在其默认配置中会很快受到攻击。 即使有经验的系统管理员了解许多不同 IT 产品的合理安全设置集，这也是一项复杂，艰巨且耗时的任务。

虽然 IT 安全解决方案非常复杂，但安全配置检查列表却是一个简单而有效的工具。为了促进安全配置检查列表的开发并符合 2002 年网络安全研究与发展法案（公法 107-305）（CSRDA）[3]的要求，NIST 为 IT 产品制定了国家检查列表计划（NCP）。 本节包含 NCP 的概述。 它首先描述检查列表的内容，并举例说明经常创建检查列表的 IT 产品类型。 接下来介绍使用安全配置检查列表的好处，例如提高组织的基本安全级别。 它还解释了 NCP 的目标和益处，其中包括提高检查列表的质量，适用性和可用性。

2.1 安全配置检查列表

安全配置检查列表（也称为锁定指南，强化指南，安全指南，安全技术实施指南[STIG]或基准测试）[3]本质上是一个文档，其中包含用于将 IT 产品配置到操作环境的说明或过程，验证产品是否已正确配置，和/或用于识别产品未经授权的配置更改。 IT 产品可能是商业的，开源的，政府现成的（GOTS）等等。

使用精心编写的标准化配置检查列表可以减少 IT 产品的漏洞暴露，特别有助于小型组织和个人保护其系统。 检查列表不仅可以由 IT 供应商开发，也可以由具有 IT 产品安全技术能力的其他组织开发。 安全配置检查列表可能包含以下任何一项：

- 自动设置或验证各种安全相关设置（例如，可执行文件，修改设置的安全模板，安全内容自动化协议（SCAP）XML（可扩展标记语言）文件和脚本）[4]的配置文件。
- 指导、核查检查列表用户手动配置 IT 产品的文档（例如文本文件）
- 说明安全安装和配置设备的推荐方法的文档
- 为审计，认证机制（例如密码）和周边安全等提供指导方针的政策和程序化文件。

并非安全配置检查列表中的所有指令都需要严格解决安全设置。 检查列表还可以包括专门的安全功能，例如寻找对主机的攻击假象，或者管理实践，例如启用节能功能。

通常，系统管理员或最终用户按照检查列表中的说明将产品或系统配置为在检查列表中实施的安全级别，或者验证产品或系统是否已正确配置。 系统管理员可能需要修改检查列表以包含本地安全策略。

安全检查列表所针对的设备和软件类型的例子如下：

- 通用操作系统和移动操作系统
- 常见的应用程序，如电子邮件客户端，Web 浏览器，文字处理器，个人防火墙和防病毒软件
- 诸如路由器，交换机，防火墙，虚拟专用网（VPN）网关，入侵检测系统（IDS），无线接入点和电信系统等基础设施设备
- 诸如域名系统（DNS），动态主机配置协议（DHCP），Web，简单邮件传输协议（SMTP）和数据库服务器等应用程序服务器
- 其他网络设备，如扫描仪，打印机和复印机。

2.2 使用安全检查表的好处

如果开发正确，安全检查列表可以帮助用户配置 IT 产品，使其具有比默认设置更多的保护功能。 将检查列表应用于操作系统和应用程序可以减少攻击者可以尝试利用的漏洞数量，并减少成功攻击的影响。 使用检查列表提高了系统安全性的一致性和可预测性，特别是与用户培训和意识活动以及其他支持安全控制相结合。与使用检查列表相关的其他好处包括以下内容：

- 提供基本的安全级别以防范常见和危险的本地和远程威胁（例如恶意软件，拒绝服务攻击，未经授权的访问和不恰当的使用）
- 验证系统评估的某些技术安全控制的配置，例如确认是否符合某些联邦信息安全现代化法案（FISMA）要求或其他要求，以及理解错误配置导致的暴露情况。
- 显著减少研究和开发已安装 IT 产品的适当安全配置所需的时间
- 允许较小的组织利用外部资源来实施建议的实践安全配置
- 降低因系统妥协而导致公众丧失信心或尴尬的可能性（例如，重大违反个人身份信息（PII））。

尽管出于安全合规目的使用安全检查表可以显着提高组织的整体安全级别，但使用检查列表不能使系统或产品 00％安全。使用检查列表强调系统对隐藏的软件缺陷的强化，通常会导致更高级别的产品安全性和保护免受未来威胁（例如，零日漏洞）的影响。 使用符合 FISMA 关联安全控制要求的检查列表配置其产品的 IT 供应商将为联邦机构内的配置设置提供更多一致性。即使代理商必须修改检查列表以针对其特定应用程序和操作环境微调配置设

置，此配置还将为建立和验证最低配置设置提供更具成本效益的方法。

2.3 NIST 国家检查表计划概述

许多组织创建了检查列表；然而，这些检查列表在质量和可用性方面差异很大，并且随着软件更新和升级的发布，它们可能会过时。如果没有中央检查列表存储库，找到安全检查列表可能很困难。 此外，检查列表可能在核查检查列表的目的或提供的安全级别方面有很大不同。 此外，可能很难确定核查的检查列表是否是最新检查列表，或检查列表应如何实施。

为了促进 IT 产品安全检查表的开发并使检查表更加有组织和可用，NIST 建立了 NCP。NCP 的目标是 -

- 通过为供应商和其他检查列表开发人员提交一份正式框架向 NIST 提交检查列表，促进开发和共享检查列表
- 为开发人员提供指导，以帮助他们创建符合常见操作环境的标准化，高质量检查列表
- 通过提供更好的文档记录和更多可用的检查单指导来帮助开发人员和用户
- 鼓励软件供应商和其他各方制定检查列表
- 为检查检查列表的审查，更新和维护提供一个受管理的流程<提供一个易于使用的检查检查列表信息库
- 以标准格式提供检查列表内容
- 鼓励使用自动化技术来应用检查列表。

联邦机构在有需要时必须有可使用的 NCP 适当安全配置检查列表。2017 年 1 月，联邦采购法规（FAR）第 39 部分进行了更新。 第 39.101 段（c）规定：“在获取信息技术时，各机构应包括适当的信息技术安全政策和要求，包括使用国家标准与技术研究院网站 https://checklists.nist.gov。代理签约官员应与需要的官员协商，确保合并适当的标准。“[1]

2.4 由 NCP 列出的检查单类型

NCP 处理与特定 IT 产品相关的检查列表，例如特定品牌和路由器型号的检查列表。一些检查列表可能会引导用户访问其他检查列表。[5] 例如，数据库产品的检查列表可能引用运

行数据库产品的操作系统的检查列表。 NCP 包括两大组核对表：

- **自动化**。 自动检查检查列表是通过一个或多个工具使用的检查列表，可根据检查检查列表的内容自动更改或验证设置。 许多检查列表是用可扩展标记语言（XML）编写的，并且有一些特殊工具可以使用 XML 文件的内容来检查和更改系统设置。例如，安全内容自动化协议（SCAP）通常用于以标准化的方式表示核对检查列表内容，并可通过支持 SCAP 的工具进行处理。[6]
- **非自动化**。 顾名思义，非自动化检查检查列表是为手动使用而设计的检查检查列表，例如描述管理员为保护系统或验证其安全设置而应采取的步骤的形式化指示。

NCP 中的安全配置检查列表可以帮助组织满足 FISMA 的要求。 FISMA 要求各机构确定可接受的最低限度系统配置要求并确保其符合要求。检查列表还可以将特定的技术控制设置映射到相应的 NIST 特殊出版物（SP）800-53 控件，这可以使合规性验证更加一致和高效。 因此，鼓励联邦机构以及联邦政府产品供应商使用 NIST 存储库获取或开发和共享这些检查列表。检查表的开发和共享可以减少在联邦政府广泛使用的 IT 产品（例如普通操作系统，服务器和客户端应用程序）中“重塑车轮”。

NIST 检查列表资源库（位于 https://checklists.nist.gov/）包含有关自动化和非自动化检查列表的信息，这些检查列表已经开发和筛选以符合 NCP 的要求。 该存储库还包含一些检查列表的副本，主要是由联邦政府开发的检查列表，并且指向其他检查列表的位置。 用户可以浏览检查列表说明，以使用各种不同的字段查找和检索特定的检查列表。 检查列表程序的邮件列表可在 https://nvd.nist.gov/general/email-list 找到。

3. 检查列表的操作环境

为确保尽可能多的用户从检查列表中获得价值，建议检查列表作者为广泛的操作环境创建检查列表，除非有令人信服的理由关注专门的操作环境。 NCP 确定了几个广泛和专业化的运营环境，其中至少有一个应该是大多数受众共同的。通过识别和描述这些环境，开发人员可以更好地将他们的检查列表定位到与环境相关的一般安全要求，并允许最终用户更轻松地选择最适合其环境的检查列表。

本节介绍为 NCP 定义的操作环境，以及每种环境的一般威胁描述和基本技术安全实践。这两个广泛的操作环境被称为独立（或小型办公室/家庭办公室[SOHO]）和托管（或企业）。

三种典型的自定义环境（可能是更广泛的环境的子集）是专用安全限制功能（SSLF），传统和美国政府。

IT 产品用户在初步确定他们自己的安全要求和需求时可能会发现查阅文档的这一部分很有用（在第 4 节详细介绍）。 开发人员在构建检查列表时可能会发现本节很有用，因为根据这些环境及其策略定制检查列表检查列表将使开发人员能够为各种产品创建安全合规核对检查列表，但仍然遵循与环境相关的一般统一技术安全实践和设置。这在第 5 节详细讨论。在向 NIST 提交检查列表之前，开发人员应确保他们拥有本文档的最新版本，因为操作环境标准的更新可能会定期发生。最新版本可在 https://checklists.nist.gov/[7]上以单独的文件形式提供。

3.1 独立环境

独立环境描述了基于集中管理的设备（即由单个组织管理的许多设备）的独立管理的设备（例如台式机，笔记本电脑，智能手机，平板电脑），而不是托管环境（参见第 3.2 节）。独立环境通常最不安全。 维护独立系统的个人无法被假定使用相同的企业安全控制，以及难以具有与经过培训的管理员相同的一般安全专业知识。当功能成为主要焦点时，通常会出现不太安全的环境，并且不够重视平衡设备安全性和功能的关系。 因此，独立检查列表应该比较容易被家庭用户或新手系统管理员理解和实施。

3.2 管理环境

管理环境（也称为企业）包含集中管理的 IT 产品，涵盖从服务器，打印机到台式机，笔记本电脑，智能手机和平板电脑等各种应用。管理检查列表适用于高级最终用户和系统管理员。典型托管环境的管理特性使管理员可以集中控制设备上的各种设置。身份验证，帐户和策略管理也可以集中管理，以便在整个组织内保持一致的安全状态。

管理环境比独立环境更具限制性，功能更少。但是，由于托管环境的受支持和受控性质，在托管环境中使用更多功能限制性设置通常比在独立环境中更容易[8]。托管环境还倾向于实施多层防御（例如，防火墙，防病毒服务器，IDS，补丁管理系统和电子邮件过滤），从而为系统提供更好的保护。

3.3 专门的安全限制功能定制环境

自定义环境包含系统，其功能和安全程度不适合其他类型的环境。专用安全限制功能（SSLF）是一种典型的高度限制和安全的定制环境;它通常保留给具有最高威胁和相关影响的系统。这种系统的典型例子是面向外部的网络，电子邮件和 DNS 服务器，其他公开访问的系统和防火墙。它还包含含有机密信息(例如人员记录,医疗记录和财务信息的中央存储库）或执行重要组织功能（例如会计，工资单处理和空中交通管制）的计算机。这些系统可能被第三方作为攻击目标，但也可能是组织内部的可信任方面的目标。由于 SSLF 环境中的系统面临攻击或数据暴露的高风险，因此安全优先于功能。系统的数据内容或任务目的具有的价值，以至于有利于安全的积极取舍超过了对其他有用系统属性（如遗留应用程序或与其他系统的互操作性）的潜在负面影响。

一个 SSLF 环境可能是另一个环境的一个子集。 例如，托管环境中的三个桌面可以将组织的机密员工数据视为托管环境中的 SSLF 环境。 此外，移动工作人员使用的笔记本电脑（例如组织管理）可能是独立环境中的 SSLF 环境。 SSLF 环境也可能是任何其他环境之外的独立环境，例如政府安全安装处理敏感数据。

SSLF 检查列表适用于经验丰富的安全专家和系统管理员，他们了解实施严格的技术安全措施的影响。 如果家庭用户和其他没有安全专业知识的用户尝试将 SSLF 检查列表应用到他们的系统，他们通常会受到不必要的系统功能限制，并可能导致系统无法修复的损害。

3.4 传统环境

传统环境是自定义环境的另一个示例。 传统环境包含可能需要进行安全保护才能应对当前威胁的旧系统或应用程序，但它们通常使用旧的，安全性较低的通信机制，并且需要能够与其他系统通信。 在传统环境中运行的非传统系统可能需要更少的限制性安全设置，以便它们可以与传统系统和应用程序进行通信。 传统环境通常是其他环境的子集。

3.5 美国政府环境

美国政府环境是自定义环境的另一个例子。这个环境包含联邦政府系统。这些系统需要根据政策规定的规定配置进行保护。例如，联邦桌面核心配置（FDCC）是由管理和预算办公室（OMB）授权的安全配置策略。为支持 FDCC 策略而开发的原始检查列表存在多个版本的

Microsoft Windows，Windows 防火墙和 Internet Explorer。这些检查列表比以前的检查列表更广泛，包括 Web 浏览器，个人防火墙和其他软件的设置。配置设置还包括旨在提高性能，能效，兼容性和互操作性的非安全相关设置。这些设置主要基于 Microsoft 在其安全指南中推荐的配置设置，但它们已经过定制以考虑联邦政府的安全要求。许多联邦系统被 OMB 的 FDCC 授权要求使用这些检查列表。

自那时以来，美国政府一直致力于开发一套新的安全配置检查列表，以增强现有支持 FDCC 政策的检查列表。这些新的检查列表被称为美国政府配置基线（USGCB）。与原始检查列表一样，USGCB 检查检查列表也支持 FDCC 政策，USGCB 检查检查列表针对各种安全和非安全设置，这些设置主要基于产品供应商推荐的设置，但可根据联邦要求进行定制。 USGCB 计划由 CIO 理事会架构和基础设施委员会（AIC）的技术基础设施小组委员会（TIS）在 2010 年创建，作为 FDCC 政策的演变。 USGCB 检查列表被称为“基线”，因为它们定义了必须实施的最低配置集合。新的 USGCB 基准发布，以取代原来的 FDCC 检查列表（Windows XP，Windows Vista 和 Internet Explorer 7），原 FDCC 检查列表在当时已弃用。 USGCB 检查列表也为其他平台创建，比如红帽企业版 Linux 桌面。

USGCB 配置设置旨在主要部署到受管系统。 支持 FDCC 政策和 USGCB 基线的原始检查列表旨在主要通过自动化工具应用于系统。 由于组织的许多设置（如加密算法选项和无线服务）可能会影响系统功能，因此组织在部署操作环境之前应彻底测试所有检查列表和基线。在部署之后，还可以通过自动化手段检查设置，以符合检查列表和基线。

4. 检查列表用法

本节介绍检查检查列表用户在检索和使用检查列表时要遵循的高级流程。 虽然从家庭用户到系统管理员的所有核对表用户都有自己的特定要求，但所描述的过程将适用于大多数情况。本节包括对当地环境威胁和风险进行初步分析的指导，并列出此类攻击的潜在影响。然后介绍通过 NIST 检查列表存储库选择和检索检查列表的过程，并推荐分析，定制和应用检查列表的步骤。

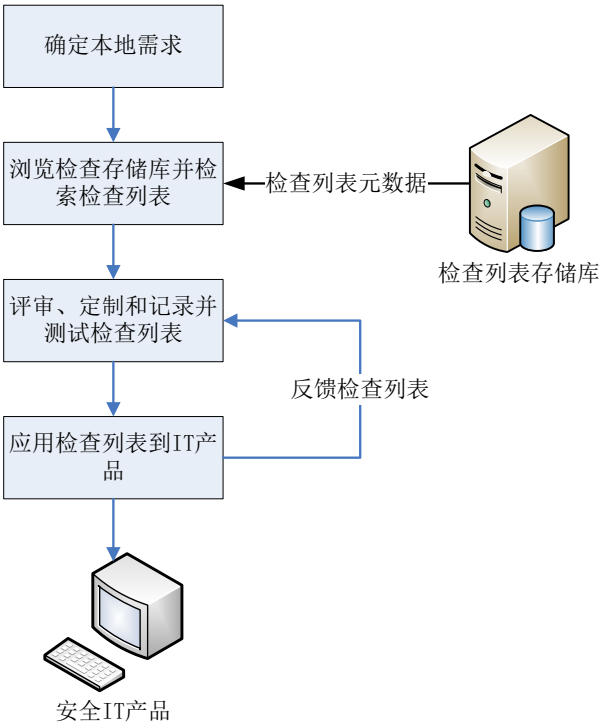

图 1：检查列表用户流程概述

图 1 显示了使用检查列表的一般过程。获取和使用核对检查列表所涉及的简单直接的一般步骤

1. 用户收集他们的本地需求（例如 IT 产品，操作环境和相关的安全需求），然后购买或购买最适合他们需求的 IT 产品。

2. 用户浏览检查列表存储库以检索符合用户操作环境和安全要求的检查列表。 如果产品的默认设置是安全的，检查 NIST 检查列表存储库以查看该检查列表的更新仍然很重要。

3. 用户查看检查列表并选择最符合要求的检查列表，然后根据需要定制和记录检查列表，以考虑当地政策和功能要求，测试检查列表并向 NIST 和检查列表开发人员提供反馈。

4. 用户准备部署检查列表，例如进行配置或数据备份，然后在生产中应用检查列表。

以下部分描述了每个步骤中包含的活动的详细信息。

4.1 确定本地要求

组织通常在实际选择和购买特定 IT 产品之前进行需求分析。 这样的分析将包括确定组织的需求（产品必须做什么）和产品的安全需求（例如相关安全策略）。 个人最终用户可以执行相同的流程，尽管它可能不是一种正式过程。 由于以后很难添加安全性，因此最好在将安全性纳入 IT 操作（无论大小）为前提进行评估。

在规划安全性时，首先必须定义必须减轻的威胁。 使用检查列表的组织应进行风险评估，以确定针对其系统的特定威胁，并确定现有安全控制在抵御威胁方面的有效性; 然后他们应该执行风险缓解来决定应实施哪些附加措施（如果有的话），如 NIST SP 800-37 修订版 1，“应用联邦信息系统风险管理框架指南：安全生命周期方法[6]”中所述，。执行风险评估和缓解有助于组织更好地了解他们的需求并决定他们是否需要修改或增强选定的检查列表。

风险缓解方法包括直接和简单的步骤，即使对于 IT 安全性方面可能不是特别精明的个人家庭用户也是如此。 重要步骤包括以下内容：

- **确定功能需求**。该产品必须做什么？为了确保选择的安全控制措施是适当的，有必要提前确定最终用户的要求，例如远程办公人员的远程访问或 Web 服务器向员工提供内部信息的必要条件;也就是说，他们实施了适当的安全解决方案，并仍然允许系统满足其功能要求。
- **识别威胁和漏洞**。威胁是特定威胁源成功利用特定漏洞的潜在可能性。漏洞是可能被意外触发或可被故意利用的弱点。此步骤的目标是识别适用于正在考虑的 IT 产品或系统的潜在威胁源以及可能由潜在威胁源利用的漏洞。
- **识别安全需求**。此步骤的目标是确定所需的控制，以最大限度地减少或消除产生威胁或系统漏洞的可能性（或概率）。它回答了这样的问题：“产品必须提供哪些安全功能？”有了这些信息,组织就可以更明智地选择哪种 IT 产品最能满足其需求。

NIST 还撰写了多份文件和指南，以帮助联邦机构在选择信息安全产品以及获取和使用经过测试/评估的产品时提供帮助。 NIST 提供的另一个关键资源是识别与 IT 产品有关的漏洞相关信息，即国家漏洞数据库（NVD）。[9] 该网站提供了一个搜索引擎，用于识别系统漏洞和可用于纠正漏洞的补丁信息。

4.2 浏览和检索检查列表

在确定本地需求并识别 IT 产品后，核对检查列表用户准备浏览 NIST 核对检查列表存储库。为帮助用户获得可通过经 SCAP 验证的产品处理的检查列表，根据内容类型（自动化程度和标准化）和权限（负责生成检查列表所代表的原始安全配置指南的组织）对核对检查列表进行分类。用户可以根据内容类型，IT 产品或权限以及通过搜索检查列表名称和摘要以查找用户指定条款的关键字搜索来浏览检查列表。搜索结果显示了检查列表的详细检查列

表信息和任何 SCAP 内容的链接，以及与检查列表相关的任何支持资源的链接。选择特定检查列表将显示一个描述模板，其中包含大量信息以帮助用户确定检查列表是否适合其特定目的。根据用户的需求，描述角色和技能（例如，家庭用户与企业管理员）的某些字段比其他字段更重要。

一些检查列表可以处理多个应用程序或操作系统，例如来自单个组织的多个产品。为帮助用户从检查列表详细信息页面导航站点，可以使用“检查列表组”链接;它代表基于共同来源材料的检查列表分组。例如，DISA（国防信息系统局）桌面检查列表包含多种产品（包括浏览器和防病毒产品）的配置设置。NCP 根据这些单独的目标分解检查检查列表信息，但通过核查检查列表组将其方便地链接到同一源文件。

在某些情况下，产品的特定版本可以使用多个检查列表。这样的检查列表通常是相似的，但它们有重要的不同，例如提供的自动化程度，目标受众（例如，提供一般性建议与符合联邦特定要求的一般建议）以及检查列表目的（重新配置产品与识别成功的妥协的产品）。 为了帮助核对检查列表用户能够容易地识别核对检查列表之间的主要差异，NIST 按内容类型对检查列表进行了分类，例如：

- **形式化。**形式化检查列表提供了人们如何手动改变产品配置的叙述性描述。
- **自动化。**自动检查列表以机器可读格式记录其安全设置，无论是标准还是专有。一个示例是产品特定的配置脚本。这些检查列表可能包含 SCAP 的某些元素（例如，它们可能包含 CCE [通用配置枚举]标识符），但不完全遵守 SCAP 规范。
- **SCAP 内容。**SCAP 内容检查列表遵循 NIST SP 800-126 中的 SCAP 规范，以机器可读的标准化 SCAP 格式记录安全设置。 SCAP 内容检查列表可以通过经过 SCAP 验证的产品进行处理，这些产品已由经过认证的独立测试实验室验证，符合适用的 SCAP 规范和要求。已使用 NIST SCAP 内容验证工具（SCAPVal）[10]评估了国家检查表程序库中可用的 SCAP 内容。此评估确保核查检查列表符合 SCAP 规范。当应用“等于或大于”时，SCAPVal 工具不评估逻辑错误的检查列表，例如使用“等于”运算符。

一些 SCAP 内容检查列表已经过至少一个治理机构的审核。已知这些 SCAP 检查列表可在启用 SCAP 的工具上运行，并包含可从外部映射到各种安全框架中所表示的高级安全要求的低级别安全设置映射（例如，各个安全配置问题的标准化标识符）（例如，FISMA 的 SP 800-53 控制）。 第 3.5 节中描述的 USGCB 检查列表是审核 SCAP 内容检查列表的例子。

当针对特定产品提供多个检查列表时，组织应考虑每个检查列表标准的自动化程度和使用情况。 一般来说，SCAPexpressed 检查列表可以比其他检查列表更加一致和高效地使用。

检查表之间可能有其他显着差异；例如，一个检查列表可以包括与操作系统（例如，网络浏览器和电子邮件客户端）捆绑在一起的软件，而另一个检查列表仅针对该操作系统。另一个例子是核对检查列表所依据的假设（例如操作环境）。 核对检查列表用户应该识别这些差异并确定哪些核对检查列表看起来合适，并且需要进一步分析。

检查列表来源对联邦民事机构的用户特别重要，他们应首先搜索政府授权或强制的检查列表。 一般来说，这些用户应该搜索 NIST 生成的检查列表，这些检查列表是为民用机构量身定做的。 如果没有 NIST 制作的检查列表可用，那么应该使用由国防信息系统局（DISA）或国家安全局（NSA）提供的机构制作的检查列表。 如果政府授权的正式检查列表不存在，鼓励组织使用供应商制作的检查列表。 如果供应商生产的检查列表不可用，则可以使用在 NCP 网站上公布的其他检查列表。

组织通常使用关联的字母数字版本标识符（例如 R1.2.0）提交检查列表。不幸的是，这些标识符没有普遍的含义。某些组织可能会在添加新的检查，删除旧技术，添加补丁或仅基于审阅日期时更改版本号。相反，其他组织可能会更新其检查列表并且不会更改版本号。为了澄清对检查列表的更新，NCP 使用“检查列表修订版”的概念。核查检查列表修订版表明即使版本标识符没有变化，事情也发生了变化。例如，如果组织没有更改文档的版本号，但内容已更新（例如，补丁是针对特定月份添加的），则当前核对检查列表将被列为已归档并且具有已更新补丁内容的核对检查列表将显示为当前检查列表。同样，如果提交组织更新版本标识符，则 NCP 会将当前检查检查列表列出为已存档并链接到新核查检查列表。在检查列表详细信息页面，用户可以通过“归档修订”链接导航到检查列表历史记录。

4.3 审核，定制和记录以及测试检查列表

核查检查列表用户应下载核查检查列表的所有文件并仔细检查。 文件应解释任何必要的准备活动，如备份系统。 由于检查列表可能不完全符合用户的具体要求，因此查看检查列表对于确定检查列表是否需要定制 [11] 以及系统或产品在应用检查列表后是否需要进一步更改很有用。

如果使用了给定的安全检查列表，用户的审查可以确定对组织当前策略和实践的影响。组织可能会确定核查检查列表的某些方面不符合特定组织特定的安全和操作需求。组织应仔细评估检查列表设置并赋予其相当的权重，然后进行必要的更改以使设置适应组织的环境，要求，策略和安全目标。[12] 对于安全需求显着不同的环境，检查列表尤其如此。组织应根据

当地的规则，条例和要求制定核查检查列表;例如，联邦民事机构需要确保核查检查列表符合联邦信息处理标准（FIPS）140“加密模块安全要求”中的加密要求。由于检查列表可能会在组织内多次使用，因此检查列表本身可能需要修改。如果检查列表包含要应用于系统的脚本或模板，则这种情况尤其可能。

此时，应将所有与检查表中设置的偏差记录下来供将来参考。 文件应包括每个偏差背后的原因，包括保持设置的影响和偏离设置的影响。 本文档有助于管理被保护产品生命周期中对检查列表的更改。 对检查列表的反馈可以发送给 NIST 以及检查列表开发人员。 对于开发人员来说，反馈对于评估检查列表编写是否正确以及设置是否适用于目标环境尤其重要。

在应用将用于更改产品设置的检查列表之前，用户应首先在非关键系统上进行测试，最好在受控的非操作环境中进行测试。对于没有用于测试目的的额外系统和网络的家庭或小型企业用户来说，这样的测试可能是困难的。 NIST 检查列表存储库中的每个检查列表都经过了开发人员的测试，但开发人员的测试环境和组织的运行环境之间经常存在显着差异，其中一些差异可能会影响检查列表部署。 IT 产品的测试配置应与部署配置相匹配。在某些情况下，安全控制修改会对产品的功能和可用性或其他产品或安全控制产生负面影响。例如，安装补丁程序可能会无意中破坏另一个补丁程序，或者使防火墙可能无意中阻止防病毒软件更新其签名或中断补丁管理软件。因此，执行测试以确定对系统安全性，功能和可用性的影响非常重要;记录测试结果;并采取适当措施解决任何重大问题。第 4.4 节包含有关执行备份和其他建议的建议，以防止或避免应用未经测试的检查列表时可能发生的潜在损害或不良影响。

在使用检查列表验证产品设置而不更改它们之前，用户应该对其进行测试。如果检查列表是自动的，用户还应该测试将与检查列表一起使用的工具或工具，以确保它们不会无意中破坏系统的功能或改变产品的配置。应执行核查检查列表测试，以确定预期和实际设置之间的差异，这可能表明核查检查列表中存在错误，例如核查检查列表未被修改的环境特定特征。

4.4 将检查列表应用于 IT 产品

检查列表可以通过以下两种方式之一应用于 IT 产品：修改产品设置或验证现有设置。以下提供了两种应用检查列表的建议：

- 设置修改

- 即使在审查和测试检查列表之后，用户也应仔细处理部署，以尽量减少应用检查列表可能产生的任何问题。
- 对于无法在非操作环境中测试检查列表的用户（例如，家庭用户），重要的是仔细核查检查列表文档并确定是否需要初始备份。 检查列表描述中的回滚能力字段将指示是否可以颠倒应用检查列表的结果以将产品返回到其原始配置。无论如何设置，强烈建议用户在安装核对检查列表建议之前备份 IT 产品的配置。

- 至少，用户应备份计算环境中的所有关键数据文件。如有可能，用户应对系统进行完整备份，以确保系统在必要时可恢复到其预检表状态。（在进行任何重大系统更改之前，建议进行完全备份;它不仅适用于实施检查列表。）大型组织也应遵循此程序，并且如果可能，首先选择若干操作系统作为试点以提供“现实世界”在企业级部署之前测试检查列表。
- 设置验证
  - 即使在审查和测试检查列表后，用户也应仔细处理验证，以确保产品设置不会被无意中改变。

在最初应用检查列表后，组织可能需要在将来获取并应用检查列表的修订版本。 根据所保护的产品，可能会根据设定的时间表定期更新检查列表，或者根据需要频繁或不经常更新检查列表。 对于选定的检查列表，NIST 可以维护用户的邮件地址列表，订阅检查列表的用户将收到更新通知或与检查列表相关的其他问题。 有关订阅邮寄地址列表的说明将包含在检查列表存储库中所选检查列表的说明中。 获取更新检查列表的组织将执行本节已经描述的相同步骤，同时利用从检查列表应用先前版本获得的知识和记录。

4.5 对检查列表提供反馈意见

NIST 欢迎来自检查列表用户的关于单个检查列表或存储库本身的所有“缺陷”报告，评审和建议。 此类反馈信息应发送至 checklists@nist.gov[13]

检查列表用户在评估检查列表时可能需要考虑的一些问题包括：

- 文件
  - 它是否解释安全目标？
  - 它是否包含检查列表设置的完整，清晰和简洁的描述？

- 推荐做法
  - 检查列表设置是否与推荐做法一致？
  - 检查列表设置是否考虑到最近的漏洞？
- 配置的影响
  - 检查列表开发人员是否在操作仿真环境中测试了产品的检查列表设置，并确定检查列表设置的应用会使产品符合检查列表的安全目标？
  - 执行任何检查列表设置会导致产品无法使用或不稳定？
  - 执行任何检查列表设置是否会降低产品功能？ 如果是这样记录他？
- 易于实施
  - 检查检查列表是否适用？
  - 说明简明扼要，完整？
  - 是否确定了所需的技能水平？
  - 包含验证安装是否成功的程序？
  - 在安装前是否有卸载检查列表或将产品恢复到初始状态的指导？
  - 如果检查列表无法回滚，文档是否建议其他准备措施，如备份？
- 帮助
  - 与检查列表相关的帮助是否可用？
  - 如果发生错误或检查列表设置导致产品操作不正确，文档是否包含用于故障排除的信息？
  - 有没有对产品的合格用户提供帮助？
- 如果检查列表开发者不是 IT 产品的供应商，文档是否指明检查列表是否已经被 IT 产品供应商赞助或认可？

5. 开发检查列表

本节介绍开发安全配置检查列表并将其提交给 NCP 的一般过程。 它包括 NIST 将遵循的过程概述，以筛选提交检查列表并将其发布到其存储库中，并且 NIST 和开发人员将遵循过程来更新检查列表或存档检查列表。 希望向 NIST 提交检查列表的个人开发者和组织应审查本文件的附录，其中包含参与 NCP 的行政要求。 在向 NIST 提交检查列表之前，开发人

员应确保他们拥有本文档的最新版本。 最新版本可在 https://nvd.nist.gov/ncp/participation 上单独获取。

检查列表生命周期包括以下步骤：

1. **初始检查列表开发**：开发人员[14]熟悉检查列表程序的程序和要求，然后执行检查列表的初始开发，包括选择目标环境。

2. **检查列表测试**：开发人员测试目标环境中的检查列表并纠正检查列表中的任何问题。

3. **核查检查列表记录**：开发人员根据程序的准则记录检查列表。

4. **提交已核查检查列表给 NIST**：开发人员将核查检查列表和文档包提交给 NIST 进行筛查和公开审查。

5. **NIST 筛选**：NIST 将筛选检查列表包的信息，并确认任何 SCAP 数据流内容格式正确，然后在公开审核之前解决与开发人员有关的任何问题。

6. **公众评审和反馈**：NIST 对候选人检查列表进行为期 30 天的公开评审，然后开发人员根据需要处理评论。

7. **检查列表存储库最终列表**：NIST 列出存储库最终检查列表并宣布检查检查列表的可用性。

8. **检查列表维护和存档**：任何人都可以在检查检查列表的整个生命周期内提供反馈。开发人员会根据需要定期更新检查列表。检查列表在不再被维护或不再需要时被归档。

应该执行每个步骤以确保检查列表在其开发和随后的发布，更新或存档期间的准确性，测试和记录。 以下各节介绍了每个步骤的注意事项。 USGCB 美国政府环境检查列表遵循本节中的步骤，但它们必须满足附录 D 中详述的附加要求。

5.1 开发创建，测试和提交检查列表步骤

上面列出的开发方法的前四个步骤涉及开发人员创建，测试，记录和提交检查列表。5.1.1 至 5.1.4 节更详细地描述了每个步骤。

5.1.1 初始检查列表开发

在初始检查列表开发期间，开发人员熟悉核对检查列表程序的要求以及检查列表生命周期中涉及的所有程序（如本节所述）。

此时，开发人员可能会同意参与 NCP 的要求，然后再继续制定检查列表。本文档中描述

了参与要求，但在附录 B 中以行政和程序化术语呈现，这对于技术开发人员来说并不那么明显，对于那些必须正式同意 NCP 要求的开发人员组织来说则更少。参与协议载于附录 C.[15]

在同意 NCP 要求后，开发人员决定应该在哪个操作环境（参见第 3 节）中执行核对检查列表，并相应地建立核对检查列表。此步骤的输出是产品的初始检查列表。

NIST 认识到，详细的检查列表开发不能在本文中广泛涉及。开发人员可能会在 NIST SP 800-53 [7]和 NIST SP 800-27（信息技术安全工程原理（实现安全基准）[5]）中编制目录，查找普遍接受的技术安全原则和实践的出版物开发检查列表时有帮助。在 https://scap.nist.gov/上也有许多与 SCAP 有关的出版物。

就漏洞覆盖率而言，安全目标应考虑到最新的漏洞，并且通常与公认的漏洞相关信息来源相一致，其中包括美国国土安全部（DHS）美国计算机应急准备小组 美国 CERT），计算机应急响应小组/协调中心（CERT / CC）和 NIST 的 NVD。[16]

联邦政府使用的产品检查列表开发人员应参考 FISMA 相关的安全控制要求。NIST SP 800-53 [7]提供了一个安全控制目录，使用控件组来为联邦信息系统创建三个最低安全控制集 - 低，中，高影响，如 FIPS 199“安全分类标准 联邦信息和信息系统[9]。 鼓励将在联邦信息系统中使用的 IT 产品开发人员通过创建检查表来帮助联邦机构满足 FISMA 的强制性要求，该检查表在各种运营环境或不同影响级别的信息系统中提供推荐的配置设置，如 FIPS 199 和 SP 800-53。 还鼓励开发人员考虑健康保险流通与责任法案（HIPAA）和其他来源强加的要求。

5.1.2 检查表测试

在将检查列表提交给 NIST 之前，应该在满足目标环境和平台的配置中对其进行全面测试。 如果适用，该检查列表应该用各种应用程序和硬件平台进行测试。 理想情况下，至少应该在生产或镜像生产环境中执行一些测试。 测试数据不需要提交给 NIST; 但是，开发人员应保留数据以供适当审查。

选择最合适的一组安全控制可能是一项艰巨的任务，因为许多安全控制具有有限的系统功能和可用性。 在某些情况下，安全控制可能会对其他安全控制产生负面影响。 例如，安装补丁可能会无意中破坏另一个补丁。 因此，对所有安全控制执行测试以确定它们对系统安全性，功能和可用性的影响并采取适当步骤解决任何重大问题非常重要。

NIST 制定了 SP 800-115，信息安全测试和评估技术指南[8]，帮助管理员测试系统中的

漏洞和配置问题。 尽管本出版物更侧重于测试系统而不是测试单个 IT 产品，但它对于检查列表开发人员可能很有用。

5.1.3 记录检查列表

检查列表文件的质量通常会使检查检查列表的有效性发生重大变化。 检查列表文件应清楚地说明如何使用检查列表，并提供简明，完善和完整的说明。 应该确定使用检查列表所需的技能水平以及目标环境。文档还应解释个别设置的重要性，包括产品功能的任何更改。如果适用，文档还应包括验证检查列表安装是否成功的程序，以及在安装检查列表之前卸载检查列表或将产品恢复到其状态的指导。在某些情况下，可能无法回滚检查列表设置，在这种情况下，检查列表文档应根据实际情况推荐备份和系统恢复等程序。

应该记录测试方法，例如检查检查列表的测试方式和使用的平台。 检查列表文档还应包含故障排除信息或检查列表设置导致产品操作不正确的信息。 理想情况下，如果出现问题，可以为产品的（注册）用户提供帮助。

检查列表开发人员必须完成每个检查列表的在线检查列表说明表格。[17] 表 1 显示了开发人员要完成的检查列表说明表格中的字段。

表 1：检查列表说明表单域

字段名称	说明
检查列表名称	检查列表的名称。
版本	检查列表的版本或版本号。
发布日期	指定实际检查列表文件发布的日期，格式为 MM / DD / YYYY。
产品分类	IT 产品的主要产品类别（例如，防火墙，IDS，操作系统，Web 服务器）。
目标	一系列创建了检查列表的特定 IT 系统或应用程序。
CPE 名称	特定目标的 CPE 表示。
检查列表角色	检查列表所描述的 IT 产品的主要用途或功能（例如，客户端桌面主机，Web 服务器，堡垒主机，网络边界保护，入侵检测）。
检查列表摘要	总结检查列表及其设置的目的。
已知的问题	总结应用检查列表后可能出现的问题，以帮助用户查明检查列表引起的任何功能和操作问题。

受众	目标受众应该能够安装，测试和使用检查列表，包括正确使用检查列表所需的最低技能和知识。
目标操作环境	IT 产品的操作环境，如独立，管理或自定义（带有说明，如专用安全限制功能，Legacy 或美国政府）。 一般只适用于安全合规/漏洞检查列表。
检查列表类型	核对检查列表的类型，如合规性，漏洞和专业化。
检查列表安装工具	介绍使用检查列表配置系统所需的功能工具，如果它们不包含在检查列表中。
符合 FIPS 140-2	产品是否可以在 FIPS 140-2 验证模式下运行（是或否）。
合规性	该检查列表是否符合各种法规和标准（例如，健康信息可移植性和责任法案[HIPAA]，Gramm-Leach-Bliley Act [GLBA]，FISMA [例如映射到 NIST SP 800-53 控件]，ISO 27001，萨班斯-奥克斯利法案，国防部[DoD] 8500，联邦风险和授权管理计划[FedRAMP]，国家安全系统指令委员会[CNSSI] 1253，信息和相关技术控制目标[COBIT] 5，NIST 网络安全框架，互联网安全中心[CIS]控制）。
权威	负责生成检查列表所代表的原始安全配置指导的组织。当局根据其“权限类型”进行排序。在 NCP 网站内，权限通过权限类型：权限的语法与其权限类型分组。
作者	负责按当前格式创建检查列表的组织。在大多数情况下，组织将代表检查列表的作者和权威，但事实并非如此。例如，如果组织为 NIST 出版物生成经过验证的 SCAP 内容，则创建 SCAP 内容的组织将被列为作者，但 NIST 将仍然是该权威。
回滚	功能是否可以回滚通过应用检查列表所做的产品配置更改，如果是这样，还可以回滚更改。
测试信息	检查检查列表被测试的平台。 可以包含任何其他与测试相关的信息，例如所用测试程序的摘要。 应指定在生产或镜像生产环境中执行的任何操作测试。
审核，警告，杂项	检查列表开发者希望传达给用户的任何附加信息。
免责声明	有关检查列表的法律声明。

产品支持	供应商将接受已在其 IT 产品上应用此检查列表的用户的支持电话；IT 产品的保修没有受到影响。如果提交者是产品供应商，则需要使用 NCP 徽标。 如果提交者不是产品供应商，提交者应该描述他们可能与产品供应商达成的任何协议。
接触点	一个电子邮件地址，可以参考检查列表发送问题，意见，建议和问题报告。 联系点应该是检查列表开发者监控检查列表问题报告的电子邮件地址。
赞助	如果由第三方实体提交，赞助提交的检查列表的 IT 产品制造商组织和个人的名称。
许可	说明许可协议（例如，检查列表是受版权保护的，开源的，通用公共许可证[GPL]，免费软件，共享软件）。
SCAP	内容指向代表配置指南的机器可读内容的链接。 本指南使用 SCAP 表示。
支持资源	与指南相关的任何支持信息或内容的链接。 该字段可以包含从实际指导的英文散文表示到应用指标特定设置的目标配置脚本之间的数据。
依赖/要求	指出需要使用其他检查列表或指南才能正确使用和实施当前检查列表。
参考	开发人员选择的任何支持参考文献，用于生成检查列表或检查列表文档。

开发人员需要按照指示填写字段以准确描述核对检查列表，并最大限度地减少用户对核对检查列表完成的混淆。

总之，结构清晰的检查列表文档包括以下内容：

- 安全目标声明，包括产品在应用检查列表之后的预期行为
- 目标受众（例如最终用户，系统管理员）以及使用检查列表所需的技术水平
- 检查表设置的说明，包括每个设置对产品操作的影响以及设置启用或禁用的任何功能
- 备份程序或在应用检查列表之前需要的其他初始步骤
- 根据情况，应用检查列表的分步说明（例如屏幕截图，图解说明的程序）并验证安

装是否成功

- 故障排除说明或其他信息和参考。

5.1.4 核对检查列表并提交 NIST

此时，检查列表开发人员已完成测试并记录检查列表。 开发人员现在将材料包提交给 NIST。 该软件包包括以下内容：

- 检查列表和配置文件，模板，脚本等
- 完成检查列表说明
- 检查列表文件
- 确定开发者的联络点
- 签署参与协议。

附录 B 详细列出了参与协议和其他要求，其中还包括相应的 NIST 联系信息。

核对检查列表包通过 NCP 提交网站提交给 NIST。 该网站通过一系列屏幕页面来引导核对检查列表开发人员，收集检查列表提交所需的所有信息和材料。 此外，该网站允许检查列表开发人员查看他们已提交的检查列表，查看已分配给他们的任务（例如修复先前提交的检查列表中的错误），更新现有检查列表并执行其他操作。NIST 还提供用于提交，提取和维护检查列表的 Web 服务。 要请求访问 NCP 提交网站或相关网络服务，请发送电子邮件至 checklists@nist.gov。

5.2 NIST 发布审查和完成出版物检查列表步骤

在下面的章节中将介绍 NIST 筛选和发布检查列表的过程，该检查列表对应于检查列表生命周期中的第 5 步到第 8 步。

5.2.1 NIST 筛查检查列表包

这一步涉及确定合适的检查列表材料是否足够准确和完整以进行公开审查。 NIST 筛选检查列表信息的完整性和准确性，并确保检查检查列表内容是 SCAP 表达的良好结构。 在筛选期间，NIST 可能会联系开发人员提交有关提交材料的问题。

5.2.2 候选检查列表的公众审核和反馈

在筛选检查列表包并且开发者已经解决了任何问题之后，NIST 将把它作为候选草案发布并公布审核及为期 30 天公开审核。 这允许公众检查和测试核对检查列表，并向核对检查列表开发人员和 NIST 提供评论和反馈。来自评论和反馈的信息可以包含在检查列表的修订中以提高其质量。 当候选检查列表完成审核流程时，其信息将添加到检查列表存储库。

检查列表审查人员发电子邮件 checklists@nist.gov 提供审核以及有关审核人员测试环境，程序和其他相关信息的其他信息。 根据审查结果，检查列表开发人员可能需要回复审核。 NIST 也可以酌情咨询独立专家评审员。使用独立审阅者的典型原因包括以下内容：

- NIST 可能会决定它不具备确定评论是否得到满意解决的专业知识。
- NIST 可能会不同意提议的问题决议，并寻求第三方的评论以获得更多观点。

在公众审查期结束时，NIST 将给开发者 30 天的时间回复审核。

5.2.3 检查列表存储库的最终列表

在解决任何未解决的问题后，NIST 会列出最终检查检查列表并宣布检查检查列表现在已列在资源库中。 此时，如果开发者为检查列表提供帮助，则开发者（例如，IT 产品供应商）可以有资格使用 IT 产品的宣传材料上的检查列表标志。 附录 C 描述了使用该标志的要求。

5.2.4 检查列表维护和档案

在整个检查表的生命周期中,任何人都可以通过邮寄 checklists@nist.gov 提供关于检查表的意见或问题。 NIST 将把反馈传递给检查列表开发人员。 根据产品和更新的频率，NIST 可能会保留相关检查列表的邮寄地址。 订阅邮件列表的用户可以收到更新通知或与检查列表相关的其他问题。 所选检查列表的说明（检查列表存储库中）将包含订阅邮寄地址列表的说明。

在列出最终检查检查列表后，NIST 将定期检查检查检查列表，以确定它是否仍然相关或是否需要对其进行更改。 如果开发人员决定随时更新检查列表，NIST 将宣布检查列表正在更新。 如果修订后的检查列表包含重大变更，则将被视为新提交，并且将被要求接受与新提交相同的审核流程。

根据 NIST 或开发人员的判断，检查列表可从存储库中删除或标记为存档。 这种行为的典型原因是产品不再被支持或已经过时，或者开发者不再希望为检查列表提供支持。

附录 A.参考文献

本附录包含本出版物引用的文件列表。

[1]	联邦采购法规（FAR）第 39 部分 https://www.acquisition.gov/sites/default/files/current/far/html/FARTOCP39.html
[2]	2014 年联邦信息安全现代化法（FISMA），公法 113-283 https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[3]	2002 年网络安全研究与发展法，公法 107-305,116 Stat.2367 http://www.gpo.gov/fdsys/pkg/PLAW-107publ305/pdf/PLAW-107publ305.pdf
[4]	NIST 特别出版物（SP）800-126，安全内容自动化协议技术规范（SCAP），所有版本均可用: https://csrc.nist.gov/publications/sp800
[5]	NIST 特别出版物（SP）800-27 修订版 A，信息技术安全工程原理（实现安全基准），2004 年 6 月: https://doi.org/10.6028/NIST.SP.800-27rA
[6]	美国国家标准和技术研究所特别出版物（SP）800-37 修订版 1，应用联邦信息系统风险管理框架指南 :安全生命周期方法, 2010 年 2 月 (2014 年 6 月 5 日更新) : https://doi.org/10.6028/NIST.SP.800-37r1
[7]	NIST 特别出版物（SP）800-53 修订版 4，联邦信息系统和组织的安全和隐私控制, 2013 年 4 月 (更新于 2015 年 1 月 22 日) : https://doi.org/10.6028/NIST.SP.800-53r4
[8]	NIST 特别出版物（SP）800-115，信息安全测试和评估技术指南，2008 年 9 月: https://doi.org/10.6028/NIST.SP.800-115
[9]	联邦信息处理标准（FIPS）199，联邦信息和信息系统安全分类标准，2004 年 2 月: https://doi.org/10.6028/NIST.FIPS.199
[10]	国家安全系统委员会（CNSS）第 4009 号指令，国家安全系统委员会（CNSS）术语表, 2015 年 4 月 6 日: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

附录 B.检查列表程序操作过程

National Institute of Standards and Technology

信息技术产品 NIST 国家检查检查列表计划的操作程序

版本 1.4

本文件规定了 NIST 信息技术产品检查检查列表计划的政策，程序和一般要求。本文件适用于组织中开发人员需要正式同意计划要求的个人。

本文件的结构如下：

- 第 1 部分- NIST 国家检查检查列表计划的一般考虑事项
- 第 2 部分- 在公众审查前初步筛选检查列表的程序
- 第 3 部分- 候选检查列表的公开审查程序
- 第 4 部分 - 最终验收程序
- 第 5 部分- 维护和除名程序
- 第 6 部分- 记录保存

本附录使用以下术语：

- **候选人**是经 NIST 筛选并批准的公众评估检查列表。
- **FCL :**最终检查列表检查列表 - NIST 存储库上所有最终核查检查列表的检查列表。
- **Final :**是已完成公开评审的检查列表，已包含检查列表开发人员和 NIST 处理的所有问题，并已根据本节的程序批准在存储库中列出。
- **检查列表：**是指特定产品和版本的检查列表。
- **检查列表开发人员或开发人员** :是开发和拥有检查列表并将其提交给国家检查列表计划的个人或组织。
- **独立资格审查人员**：由 NIST 负责向 NIST 提供关于公共审查或检查列表检查列表的建议。 他们独立于其他审阅者工作，并被视为检查列表所代表的技术专家。
- **商标：**是指 NIST 国家检查表程序标志。

- **国家检查检查列表计划：**计划或 NCP 用于取代 NIST 信息技术产品国家检查检查列表计划。
- **NIST 检查列表存储库或存储库**是指维护检查列表，网站检查列表描述以及有关国家检查列表计划的其他信息的网站。
- **公共审阅者**是任何公众审阅候选检查列表并向 NIST 发送的审核成员。
- **操作环境**是指本文档中概述的操作环境。

参考文件为此计划的要求奠定基础如下：

- FIPS 199，联邦信息和信息系统安全分类标准，https://doi.org/10.6028/NIST.FIPS.199
- NIST SP 800-27 修订版 A，信息技术安全工程原理（实现安全基准），https://doi.org/10.6028/NIST.SP.800-27rA
- NIST SP 800-53 修订版 4，联邦信息系统和组织的安全和隐私控制，https://doi.org/10.6028/NIST.SP.800-53r4
- NIST SP 800-70 Revision 4，IT 产品国家检查列表计划 - 检查列表用户和开发人员指南，https://doi.org/10.6028/NIST.SP.800-70r4

1. 概述和一般注意事项

本节重点介绍国家检查表计划各个部分的一般考虑事项。

（a）**检查列表生命周期概述：**检查列表通常具有以下生命周期：

1. 检查列表开发者询问有关程序并下载提交包。开发人员随后与 NIST 联系一份经过测试的检查列表，支持信息以及签署的有关 NCP 要求的协议。检查列表提交要求和程序在第 2 节中讨论。
2. NIST 验证所有信息是否完整，并对检查列表包进行高级筛选。符合列名要求的检查列表得到进一步考虑并被称为“候选检查列表”。第 2 节讨论筛选标准和程序。
3. 如第 3 节所述，NIST 将候选检查列表列入存储库供公众审查 30 天。
4. NIST 将公共评论者的意见转发给开发者。开发人员根据情况解决问题，并在 FCL 上列出检查检查列表，如第 4 节所述。
5. NIST 定期审查每个最终检查列表，以确定其检查列表是否应该继续，更新或存档，如第 5 节所述。

（b）**知识产权：**开发人员保留其检查检查列表的知识产权。

（c）**保密信息：**NIST 预计不需要从检查列表开发者处接收保密信息。 如果有必要向 NIST 披露机密信息，NIST 和开发者必须在披露之前签订单独的保密协议。

（d）**独立合格评审人员：**NIST 可决定向独立合格专家寻求技术建议，他们将审核提交的提交检查列表，以确定他们是否符合计划要求。 评审员的任务是向 NIST 提供关于随后的公开评审或检查列表最终检查列表的建议。典型的但不排斥使用独立审稿人的理由包括以下内容：

1. NIST 不具备确定问题是否得到满意解决的专业知识。
2. NIST 不同意提议的问题决议。

（e）**终止审议检查列表提交：**NIST 或开发人员可随时终止审查检查列表提交。 如果 NIST 终止审议，则要求联系人在 10 个工作日内作出回应。 典型的但不排除考虑检查列表提交的理由包括以下内容：

1. 提交包不符合筛选标准。
2. 开发人员未能解决其他时间引发的问题。
3. 开发者违反参与该计划的条款和条件。

2. 检查列表提交和筛选

本节概述向 NIST 提交检查列表的过程和要求，以及 NIST 确定检查列表是否适合公开审核的过程。 当检查列表符合筛选标准时，他们将在公共审查中得到进一步的考虑并被称为“候选检查列表”。然后 NIST 遵循后续程序。

（a）**检查列表程序要求的通知：**NIST 在存储库上为开发人员维护一套完整的信息。 这些信息概括了参与计划的要求，并描述了材料和时间表。

（b）**开发人员所需材料：**开发人员提供以下信息：

1. 来自提交组织的个人的联系信息，该联系人将作为与检查列表有关的问题和意见的联系点，以及备份或副联系人的联系信息。 信息必须包括邮政地址，直接电话号码和电子邮件地址。
2. 检查列表，文档和说明模板。
3. 参与协议必须打印，签名并发送给 NIST。 NIST 接受通过普通邮件发送的参与协议，传真或副本的电子邮件 PDF 副本。

4. 参加费用。 目前，检查列表开发人员不收费。 NIST 保留收取未来参与费用的权利。 费用不具追溯力。

（c）**初步筛选检查检查列表内容：**NIST 进行初步筛选，以核实检查列表包是否符合基本计划要求。 虽然 NIST 保留这样做的权利，但 NIST 通常不会对检查列表内容进行深入分析，例如对建议的安全和工程实践的反映。

3. 候选检查列表公众评论

在列出候选检查列表供公众审查时，NIST 遵循后续程序。

a. 公共评审期：NIST 列出 30 天评论期的候选检查列表。 NIST 保留延长审查周期的权利，特别是对于冗长或复杂的检查列表。 NIST 与候选检查列表一起使用以下免责声明（或非常相似的词）：

NIST 不保证或保证检查列表的准确性或完整性。 NIST 不对使用该检查列表可能导致的损失，损坏或问题负责。

b. 接受审核者的评论：公众审核者通过电子邮件 checklists@nist.gov 发表评论以及有关他们的测试环境，程序和其他相关信息的信息。这些电子邮件的内容被视为公共记录。

c. 维护记录：通过为每个检查列表创建一个唯一的电子邮件地址，NIST 可以维护公众和开发人员之间的通信和反馈副本。 如果是这样 NIST 将存档信息。

d. 处理意见：在公众审查期结束后，开发人员有 30 天的时间来回复评论。

4. 最终检查列表列表

在 NIST 确定检查列表和相关开发人员符合最终检查列表的所有要求之后，NIST 在 FCL 中列出检查检查列表并将它们称为“最终检查检查列表”。 然后 NIST 遵循后续程序。

a. **完成检查列表：**NIST 列出 FCL 中的检查列表。NIST 可能会将通告发送到由 NIST 或其他组织维护的各种电子邮件列表。 NIST 对最终检查列表使用以下免责声明（或非常相似的词）：

NIST 不保证或保证检查列表的准确性或完整性。 NIST 不对使用该检查列表可能导致的损失，损坏或问题负责。

b. **处理意见：**NIST 继续接受有关最终检查列表的审核，方法是在存储库中维护一个中央电子邮件地址 checklists@nist.gov。NIST 列出了用于联系开发人员的过程以及开发人

员的联系信息，例如电子邮件地址或 URL。 如果在任何时候联系点发生变化，都必须立即通知 NIST。

5. 最终检查列表更新，存档和删除

NIST 遵循随后的定期更新，存档和删除最终检查检查列表的程序。

a. **定期审查：**NIST 定期审查每个检查列表，以确定其状态的变化。 NIST 可能会联系开发人员酌情确定检查列表状态是否发生变化，在这种情况下，开发人员需要 30 天的时间才能做出响应，并指出是否应更新，存档或撤销检查列表。

b. **更新：**当检查列表正在审核时，NIST 可能在 FCL 上指明。 开发者在审核后 60 天将更新后的材料提交给 NIST。 根据更新的规模，NIST 可能会筛选检查列表并安排公开审核。

c. **存档：**开发人员可能不再希望为检查检查列表提供支持，产品可能不再受支持，或者可能有其他理由来存档检查检查列表。 根据开发人员或 NIST 的判断，检查列表可以保留在存储库中，但它将被重新归类为存档。

d. **撤销：**当撤销发生时，例如当开发商未能响应 NIST 对查询检查列表状态的询问时，NIST 会从 FCL 中移除检查列表。 NIST 可能会将通告发送到由 NIST 或其他组织维护的各种电子邮件列表。

6. 记录保存

NIST 维护与该程序相关的信息，并要求检查列表程序中的参与者也维护某些记录，如下所示。

a. **NIST 记录**：在检查列表提交给 NIST 的期间，以及检查列表在 FCL 上作为最终或归档检查列表列出的期间以及以后三年期间 [18]，NIST 将保留以下内容：

1. 存储库中列出的检查列表描述模板
2. 存储库中列出的检查列表和检查列表说明
3. 作为公众评论的一部分提交的所有意见
4. 所有关于检查列表提交给 NIST 的意见。

b. **开发人员记录**：在检查列表提交给 NIST 的过程中，以及检查列表在 FCL 上作为最终或归档检查列表列出的时间段内，开发人员将维护以下内容：

1. 存储库中列出的检查列表描述模板
2. 存储库中列出的检查列表和检查列表说明
3. 测试报告和其他检查列表测试的证据。

附录 C.参与和徽标使用协议表

本附录包含参与 NIST 国家检查检查列表计划（NCP）和使用 NIST 国家检查检查列表计划标识的条款和要求。 在向 NIST 提交检查列表之前，开发者应确保他们拥有本附录的最新版本。 最新版本可在 https://nvd.nist.gov/ncp/participation 上单独获取。

信息技术产品 NIST 国家检查检查列表计划的参与和徽标使用协议表

版本 1.5 2018 年 2 月 15 日

“NIST 信息技术产品国家检查检查列表计划”和 NIST 国家检查检查列表计划标识旨在与特定版本的信息技术（IT）产品结合使用，该检查列表已创建并已符合国家标准与技术研究院（NIST）信息技术产品国家检查列表计划，以便在检查列表库中实施最终检查列表。您可以参加 NIST National Checklist Program 并使用短语和标识，前提是您同意书面遵守以下条款和条件：

1.您将按照 NIST 国家检查表计划 NIST 操作程序（NIST SP 800-70 Revision 4 的附录 B）中所述的规则和要求遵循该计划。

2.您将在公众审查期结束后的 30 天内回复公众对您提交的检查列表提交的评论和问题。评论者的任何评论和您的回复可能会公开。

3.您同意维护检查列表并及时（在 10 个工作日内）回复 NIST 提供的关于检查列表内容的信息或协助的请求。

4.您同意按照NIST SP 800-70 Revision 4附录B中列出的NIST National Checklist Program的要求维护与检查列表相关的记录。

5.您将在涉及提交检查列表的任何后续诉讼中保持NIST无害。

6.您可以随时终止参加NIST国家检查表计划。您将向NIST提供两个营业周的通知，告知您终止参与的意图。NIST 可随时终止对检查列表提交的审议或您参与 NIST National Checklist计划。NIST将在两个工作日之前与您联系，以便终止您的参与。您可以在一个工作周内对拒绝提出上诉并提供支持性证据。

7.您不得在与本协议直接或间接相关的任何广告，产品或服务中使用NIST或商务部的名称。通过接受本协议，NIST不会直接或间接支持您，您的继任者，受让人或许可证持有者提供或将提供的任何产品或服务。您不得以任何方式暗示此协议是对任何此类产品或服务的认可。您不得将标志的使用与其他标志，短语或标志结合使用，以暗示NIST的认可。

8.“NIST信息技术产品国家检查检查列表计划”和NIST国家检查检查列表计划标识是NIST的注册商标，该商标保留其使用的专有权。 NIST保留控制使用“NIST信息技术产品国家检查检查列表计划”和NIST国家检查检查列表计划标识的质量的权利。

9.您对广告参与NIST国家检查检查列表计划以及使用徽标的许可仅限于那些产品以及NIST通过NIST国家检查检查列表计划在其最终版本上提供检查列表的具体产品版本检查列表列表。

10.您对广告参与NIST National Checklist计划以及使用徽标的许可仅限于那些向检查列表用户提供关于正确使用检查列表的用户的帮助和帮助的检查列表开发人员，产品和特定产品版本不会通过使用检查列表来更改。

11.您在产品报告，信头纸，小册子，营销材料和产品包装上使用标识时，必须附上以下内容：“TM：NIST的注册标志，并不意味着NIST或美国政府对产品的认可。”

12.标志的尺寸，位置，颜色和其他方面的尺寸要求在NIST SP 800-70 Revision 4中规定。

13. NIST保留将来收取参与费的权利。不需要任何费用

14. NIST可以自行决定终止NIST National Checklist Program。 对于任何违反本计划的条款和条件或出于法定或监管原因，NIST可能会终止您对本计划的参与。

通过下面的签名，开发人员同意此处包含的条款和条件。

组织或公司名称：

组织授权人的名称和标题：

签名：

日期：

附录 D. USGCB 基线的附加要求

正如第 5 节介绍中所述，USGCB 基线还有补充要求，以补充第 5 节中提出的要求。本附录详细介绍了这些附加要求,并根据 5.1 节和 5.2 节中的 NCP 检查列表开发步骤进行了介绍。

D.1 开发人员创建，测试和提交 USGCB 基线的步骤

USGCB 基准线的新发展由任何美国联邦机构领导，该机构在本附录中称为候选机构。

附录的这一部分列出了候选机构创建，测试和提交必须遵循的 USGCB 基线的额外要求。有关基本要求，请参见第 5.1 节。

D.1.1 初始基线开发

每个基线都来自国家检查列表计划（NCP）网站上公布的现有 SCAP 合规性和漏洞最终检查列表。 根据此检查列表，代理机构可以将这些设置定制到其企业环境。 如果这些设置可能适用于广泛的联邦制度，该机构应考虑派一名代表前往 USGCB 的联邦 CIO 治理委员会讨论将设置推广到 USGCB 基准。 USGCB 基线应符合 NIST SP 800-53 修订版 4 的指导原则，该指导原则指出“根据 FIPS 出版物 199 和 FIPS 出版物 200 分别确定的信息系统的安全类别和相关影响级别分别选择基线”。

USGCB 设置由平台编译;单个平台可以包括一个或多个版本（例如，Windows 7 32 位和 Windows 7 64 位）。候选机构必须确保为每个基准配置定义一个离散设置。提供一般指导不符合 USGCB 候选人的设置要求。NIST 认识到，某些配置可能是特定于站点的，并且定义可能为所有联邦机构强制执行的离散设置不是一项简单的任务。在创建候选设置的过程中，候选机构应该记住，这些设置旨在供所有联邦机构使用;因此，USGCB 设置可能被认为是适用

于所有人的通用子集。 USGCB 候选人应该反映适用于所有联邦机构的最低配置或核心配置。使用 USGCB 基准的机构可能会对其进行定制，使设置更具限制性或附加其他设置。在配置适用于广泛的环境但不适合所有人的情况下，USGCB 引入了“有条件”状态的概念。例如，某些站点可能允许使用无线技术，但其他站点不允许使用无线技术。基线将提供独立的无线配置，仅适用于允许使用无线技术的站点。

开发一个可行的 USGCB 基线需要 IT 产品的专业知识和平衡安全和运营需求的能力。在基线开发期间，定义，审查和测试离散设置的目标是达到提供保护的基准，同时允许运行功能。在开发基线设置时，候选机构应该利用现场经验和可用的安全配置资源，例如政府安全指导方针，产品安全指导方针和行业建议。每个基线都应参考安全指南，例如 DISA STIG / 检查列表，NSA 安全配置指南或供应商安全指南。候选机构还应该在基线创建阶段参与产品供应商，以确保可支持性和适用性。选择设置后，候选机构会考虑每个设置的功能（例如注册表值或文件版本），并确定用于评估合规性或确定设置值的可用方法。在创建基线时，开发人员将测试系统在更改设置时的行为（例如，检查注册表值，守护进程或服务状态）。

每个USGCB候选人都必须表达为SCAP内容。NIST建议在当前版本的SCAP上生成SCAP，以利用最新的规范功能和 SCAP 产品验证。[19]如果 SCAP 内容是在最新版本以外的版本中生成的，则 SCAP 内容必须符合与相应 SCAP 版本相对应的 NIST SP 800-126 修订版的要求，并且 SCAP 内容必须通过使用当前版本的 NIST SCAP 内容验证工具（SCAPVal）。

使用最新版本的 SCAP 通常是有利的，因为基线可以利用较新的规范来进行更精确的检查，但不一定要使用最新的 SCAP 版本。候选机构应确定所有没有开放式漏洞评估语言（OVAL）检查的基准设置，然后与产品供应商合作确保未来版本的 OVAL 支持这些检查。 同样，候选机构应该确定所有没有 CCE 标识符的配置，并与 NIST 和内容提供商合作，以确保每个配置设置都有一个已填充的 CCE。[20] 如果自动化 OVAL 检查不可能或者 CCE 标识符不能合理提供，那么每个实例都应由候选机构在 USGCB 候选人提交中包含的已知问题文档中注明。

除配置检查外，候选机构应该包含最新的补丁内容，候选机构应该在基准提交之前，期间和之后继续更新补丁内容。

D.1.2 基线测试

USGCB 候选人测试有两个主要方面：验证 SCAP 内容是否符合 SCAP 技术要求，并评估运营环境中的基准设置。

候选机构应使用 NIST SCAP 内容验证工具（SCAPVal）验证和测试所有 SCAP 内容。 随着 SCAP 规格的更新，SCAPVal 会定期修订。 SCAP 内容测试还必须包含至少一个经过验证的 SCAP 验证产品； 所选产品由候选机构酌情决定。 如果可能，经过验证的产品测试应模拟 USGCB 消费者将体验的环境。 可以在 https://scap.nist.gov/validation/index.html 找到当前的 SCAP 验证产品列表。

使用经过 SCAP 验证的产品进行测试应该包括评估三种配置的系统：

- 完全符合性：配置设置等于基线中定义的离散设置。
- 合规性降低：配置设置的限制性低于基准中定义的限制。
- 增强的合规性：配置设置比基准中定义的更具限制性。

除了验证基准符合 SCAP 要求外，候选机构还应该在具有相当规模的运营企业环境中测试基准，这是典型的联邦机构运营企业环境的代表。 此测试可确保在运营环境中的基线的可行性。 NIST 建议测试基线至少三个月。 应记录现场测试的证据，并包括有关系统的位置，持续时间，系统数量，确定的问题以及成功解决已知问题的信息。 附录 D.3 提供了现场测试报告模板。

在测试期间，基线将得到完善，并达到一个可行的 USGCB 候选基线，该基线在满足运营要求的同时是安全的。 利用经过现场测试的配置在运营环境中提供安全优势而不会产生负面影响的概念对 USGCB 流程至关重要。 如果需要进行基线调整以满足特派团需求，则应更新基准并重新部署到同一组运行系统以进行其他现场测试。

配置方法和材料将用于自动配置测试系统。 配置材料的预期用途是便于在部署到运营系统之前测试基线的 USGCB 最终用户的实验室设置。这些配置材料的格式可能因产品而异。例如，Microsoft 提供组策略对象（GPO），而 Red Hat 可能提供 kickstart 脚本。

候选机构应在基线开发期间与供应商和内容的作者合作，并确保配置自动化材料生成符合 USGCB 的系统。 NIST 建议供应商选择配置支持的方法和材料。 如果可能，在现场测试活动期间，USGCB 候选软件包中的所有配置方法和材料都应该进行全面测试，并包括最终用户说明。 至少，测试用例应确保方法和材料按预期运行，并生成符合 USGCB 候选人的系统。这些材料最好由产品供应商支持。

应审查 USGCB 候选设置，并将结果记录在位于 D.3 的现场测试报告模板中。 在审查过程中，测试人员确定基线是否会产生运营影响，解决现场测试期间发现的已知问题，并确定如何使用 OVAL 评估每项设置。 如果产品供应商参与设置审核和 SCAP 内容细化，则鼓励供应商执行以下操作：

- 突出显示可能对系统产生操作影响的设置
- 确定如何使用 SCAP 检查语言来最准确地评估每个配置设置（例如，OVAL，Open Checklist Interactive Language [OCIL]）

D.1.3 记录基线

除了已经提到的基准文件（如 SCAP 内容和自动配置材料）外，USGCB 基线还需要其他文件。

每个基准都必须以人们可读的格式记录，例如设置电子表格，其中列出了基准中每个配置的离散设置。 NIST 认识到产品的固有差异将决定设置文档的变化; 但是，以下字段是必需的：

- CCE 标识符 - 列出与此设置相对应的 CCE 标识符（如果可用）
- 设置描述 - 包含手动配置或评估所需的信息。 这会因产品而异。 例如，Windows 文档定义策略路径和策略设置名称，而红帽文档定义技术机制和配置详细信息。
- 设置 - 列出为基准建议的离散设置
- 类别 - 如果适用，请使用此列来指示“条件”设置

设置电子表格中可能包含其他信息，以提供有关设置的说明或技术细节。 有关完整的设置电子表格，请参阅 https://usgcb.nist.gov。

D.1.4 提交基线给 NIST

一旦定义了配置基线，开发了 SCAP 内容，并且现场测试完成后，候选机构将把 USGCB 候选包提交给 NIST 检查列表存储库。 完整的 USGCB 候选人提交材料必须包括以下内容：

- 基线设置电子表格
- SCAP 内容：带有经验证的 SCAP 数据流的自动化检查列表
- 已知问题电子表格，其中列出了设置或 SCAP 数据流的所有问题
- 解决基准消费者最有可能存在的问题的常见问题解答（FAQ）文件
- 自动配置材料（下面讨论）
- 现场测试报告

D.2NIST 审查和完成 USGCB 发布基线的步骤

附录的这一部分列出了与 NIST 筛选和发布 USGCB 基线有关的附加要求。基本要求参见第 5.2 节。

D.2.1 NIST 筛选基线包

NIST 审核 USGCB 候选人提交的内容，并确定提交的内容是否符合所有候选资格要求，即所有 NCP 提交内容所需的要素以及附录 D.1.4 中列出的 USGCB 要素。 如果提交的文件符合要求，NIST 将根据 NIST 开放文件审查流程发布 USGCB 候选人，这类似于在 CSRC 上发布其他内容（csrc.nist.gov）。 公众审核期结束后，NIST 将进行审核裁决，然后将候选 USGCB 基准以及裁决意见提交给联邦 CIO 治理委员会供最终审议。 遵循第 5.2 节中定义的步骤。

D.2.2 检查列表存储库，维护和存档的最终列表

在联邦 CIO 治理委员会 CCB 批准最终配置后，OMB、ISIMC 和 CIO 理事会正式发布 USGCB 最终版本，并可能提供强制执行日期。最终的 USGCB 已发布到 https://usgcb.nist.gov。该最终软件包包括必要的设置文档，SCAP 内容，自动配置脚本或虚拟磁盘映像，常见问题解答文档和已知问题文档。

在维护期间，NIST 与产品供应商协调，确保所有自动配置文件保持最新状态，符合供应商的更新周期，如附录 B 第 5a 项所述。

D.3 现场测试报告模板

以下是所有 USGCB 候选人提交所需的现场测试报告模板。

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

本现场测试报告验证在操作环境中成功测试 USGCB 候选配置。 该报告必须包含在提交给 NIST National Checklist Program 的 USGCB 候选包中。

候选人机构	
候选人机构联系人姓名	

POC 电子邮件	
POC 电话	
现场测试站点位置（组织机构和场所）	
现场测试技术联系人姓名	
POC 电子邮件	
POC 电话	
现场测试的日期	
现场测试的系统数量	
问题基线确认	
解决问题	

附录 E. 缩略语

本指南中使用的缩写词和缩写定义如下。

AIC	架构与基础设施
CCB	变更控制委员会
CCE	通用配置枚举
CERT / CC	计算机应急响应小组/协调中心
CMVP	加密模块验证程序
CNSSI	国家安全系统指令委员会
COBIT	信息和相关技术控制目标
CPE	通用平台枚举
CSRDA	2002 年网络安全研究与发展法案
CVE	通用漏洞和披露
CVSS	通用漏洞评分系统
DHCP	动态主机配置协议
DHS	国土安全部
DISA	国防信息系统局
DNS	域名系统

DoD	国防部
FAQ	常见问题
FCL	最终检查检查列表
FDCC	联邦桌面核心配置
FedRAMP	联邦风险和授权管理计划
FIPS	联邦信息处理标准
FISMA	联邦信息安全现代化法案
GLBA	Gramm-Leach-Bliley 法案
GPL	通用公共许可证组
GPO	策略对象
HIPPA	健康保险流通与责任法案
IA	信息保障
IATF	信息保障技术框架
IDS	入侵检测系统
IP	互联网协议
IR	机构间报告
IT	信息技术
ITL	信息技术实验室
NCP	国家检查表计划
NIST	国家标准与技术研究院
NSA	国家安全局
NVD	国家漏洞数据库
OCIL	开放检查列表交互式语言
OMB	管理和预算办公室
OVAL	开放漏洞和评估语言
SCAP	安全内容自动化协议
SCAPVAL	安全内容自动化协议验证工具
SMTP	简单邮件传输协议
SNMP	简单网络管理协议

SP	特别出版物
SSLF	专业安全限制功能
STIG	安全技术实施指南
TIS	技术基础设施小组委员会
US-CERT	美国计算机应急准备小组
USGCB	美国政府配置基线
VPN	虚拟专用网络
XCCDF	可扩展配置检查列表说明格式
XML	可扩展标记语言

附录 F. 术语

本指南中使用的选定术语定义如下。 有些术语的定义已经改编自【10】

听众

目标受众应该能够安装，测试和使用检查列表，包括正确使用检查列表所需的最低技能和知识。

作者

负责按当前格式创建检查列表的组织。在大多数情况下，组织将代表检查列表的作者和权威，但事实并非如此。例如，如果组织为 NIST 出版物生成经过验证的 SCAP 内容，则创建 SCAP 内容的组织将被列为作者，但 NIST 将仍然是权威。

权威

负责生成检查列表所代表的原始安全配置指导的组织。

权限类型

作为检查列表权限的组织类型。这三种类型是政府机构，软件供应商和第三方（例如安全机构）。

自动检查列表

通过一个或多个工具使用的检查列表，可根据检查检查列表的内容自动更改或验证设置。自动检查列表以机器可读格式记录其安全设置，无论是标准还是专有。

候选检查列表

核查检查列表已经过 NIST 筛选和批准，供公众审查。

检查列表

包含用于将 IT 产品配置到操作环境中的指令或过程的文档，用于验证产品是否已正确配置，和/或用于识别产品未经授权的配置更改。也称为安全配置检查列表，锁定指南，强化指南，安全指南，安全技术实施指南（STIG）或基准测试。

检查列表开发人员

开发并拥有检查列表并将其提交给国家检查列表计划的个人或组织。

检查列表组

代表基于常见原始素材的检查列表分组。如果一个组织在同一个名称下包装多套产品指南，则通常使用这种方法。

检查列表修订

代表对检查列表内容的更改，不影响内容提出的基础规则/值配置指导。需要新检查表修订的情景是当为过程检查列表创建 SCAP 内容时。此修订将会将检查单的内容类型从“单调”更改为“SCAP 内容”。为了适应这种变化，将创建新的检查检查列表修订版，同时仍然维护感兴趣方的过程检查列表修订版。

检查列表角色

检查列表所描述的 IT 产品的主要用途或功能（例如，客户端桌面主机，Web 服务器，堡垒主机，网络边界保护，入侵检测）。

检查列表类型

核对检查列表的类型，如合规性，漏洞和专业化。

内容类型

自动化和标准化程度上的检查列表内容的形式。 示例包括过程，自动化和 SCAP 内容。

自定义环境

包含系统的环境，其功能和安全程度不适合其他类型的环境。

最终检查列表

已完成公开评审的检查列表已包含检查列表开发人员和 NIST 处理的所有问题，并已获得 NIST 批准在存储库中列出。

最终检查列表列表（FCL）

NIST 存储库中所有最终检查列表的列表。

独立合格评审员

评审人员由 NIST 负责就公众评论或检查列表检查列表向 NIST 提出建议。

传统环境

包含旧系统或应用程序的自定义环境，可能需要进行安全保护才能应付当前的威胁，但通常使用旧的，安全性较低的通信机制，并且需要能够与其他系统通信。

商标

NIST 国家核对检查列表计划标志。

管理环境

环境包含集中管理的 IT 产品，从服务器和打印机到台式机，笔记本电脑，智能手机和平板电脑等各种应用。

NIST 检查列表存储库

维护检查列表的网站，检查列表描述以及有关国家检查列表计划的其他信息。 也称为存储库。https://checklists.nist.gov

非自动检查列表

一个旨在手动使用的检查列表，例如描述管理员应采取哪些步骤来保护系统或验证其安全设置的英文散文说明。

运营环境

打算应用检查列表的环境类型。 运营环境的类型有独立，管理和自定义（包括专业安全限制功能，遗留和美国政府）。

产品分类

IT 产品的主要产品类别（例如，防火墙，IDS，操作系统，Web 服务器）。

过程检查列表

检查列表提供了人员如何手动更改产品配置的叙述性描述。

公众评审员

一位公众谁审查候选人检查列表并发送评审给 NIST 的成员。

查看状态

核查检查列表在内部 NCP 审查过程中的状态。 可能的状态选项包括：候选，最终，存档或审阅中。 “最终”状态表示 NCP 已经审查了检查列表并已接受它在计划中发布。

SCAP 内容检查列表

一个自动检查列表，符合 NIST SP 800-126 中的 SCAP 规范，以机器可读的标准化 SCAP 格式记录安全设置。

专用安全有限功能（SSLF）环境

一个高度限制和安全的自定义环境；它通常保留给具有最高威胁和相关影响的系统。

独立环境

包含单独管理设备的环境（例如台式机，笔记本电脑，智能手机，平板电脑）。

目标

一系列创建了检查列表的特定 IT 系统或应用程序。

目标操作环境

IT 产品的操作环境，如独立，管理或自定义（带有说明，如专用安全限制功能，传统或美国政府）。 一般只适用于安全合规/漏洞检查列表。

美国政府环境

包含联邦政府系统的定制环境，根据政策规定的规定配置进行保护。

附录 G. 变更日志

修订 4 第 1 版 - 2018 年 2 月 15 日

- 在整个文件中做了一个较小的编辑修改。

版本 4 发布 0 - 2017 年 8 月 1 日

- 修改文件的前置事项。
- 在整个文件中做了小小的编辑修改。
- 在整个文档中删除了“层”和“SCAP 表达式”概念检查列表。包括从第 5.1.3 节中的表 1 中删除几个字段，其中列出了开发人员要完成的检查列表描述表单字段。
- 修改了第 4.2 节中核对检查列表内容类型的描述（比如：单调，自动化和 SCAP 内容）。
- 将“目标产品”检查列表说明表单字段更名为“目标”，并在第 5.1.3 节的表 1 中将“目标受众”重命名为“受众”。
- 更新了附录 B，以引用 NIST SP 800-70 修订版 4 而不是修订版 3，使用更新的 URL 并放宽了 5（c）中的要求。
- 更新了附录 C，以引用 NIST SP 800-70 修订版 4 而不是修订版 3。
- 重新编译术语表。

修订版 3 第 1 版 – 2016 年 12 月 8 日

- 修订了执行摘要和第 4.2 节，以反映联邦民政机构应该使用政府授权或授权的检查列表（如果有的话）。
- 用美国政府环境描述替换了特定部门环境第 3.5 节中的描述。 在整个出版物中更改了此环境的名称。
- 所选参考 URL 已在附录 A 和整个出版物中更新。

注释

1 鼓励组织将他们的信息包含在支持映射到其他需求的检查列表中，例如 HIPAA。

2 SCAPVal 可在 SCAP 规范网站上的每个 SCAP 版本下载，网址为 https://scap.nist.gov/revision/index.html。

3 从本文档中的这一点开始，术语检查列表（根据 CSRDA 术语使用）用于描述安全配置列表。

4 有关 SCAP 的更多信息，请访问 https://scap.nist.gov/和所有版本的 NIST 特别出版物（SP）800126，安全内容自动化协议技术规范（SCAP）[4]。

5 可扩展核对表配置描述格式（XCCDF）是一种基于 XML 的格式，用于自动化工具使用并消除解释问题。 XCCDF XML 格式可用于技术检查列表（例如，操作系统，软件应用程序和硬件配置）和非技术检查列表（例如 IT 系统的物理安全性）。有关 XCCDF 的更多信息，请参阅 NIST 机构间报告（IR）7275 修订版 4，可扩展配置检查表说明格式（XCCDF）版本 1.2 的规范，可从 https://doi.org/10.6028/NIST.IR 下载。 .7275r4。用于检查列表的另一种基于 XML 的格式是开放漏洞和评估语言（OVAL），该语言用于交换关于如何检查系统中是否存在漏洞和配置问题的技术细节。有关 OVAL 的更多信息，请访问 https://oval.cisecurity.org。

6 有关产品 SCAP 支持验证和 SCAP 验证产品列表的更多信息，请参阅 https://scap.nist.gov/validation/index.html。

7 随着新信息的发布，NIST 可能会更新操作环境的标准和信息以及本文档中包含的其他标准。

8 这并不意味着不应在托管环境中自定义检查列表。例如，对于特定需要偏离特定检查列表设置的用户组进行例外处理可能比较谨慎，而不是因为部分用户的需要而导致整个企业背离设置，或者阻止用户履行子集职责。

9 https://nvd.nist.gov/

10 SCAPVal 可在 SCAP 规范网站 https://scap.nist.gov/revision/index.html 上的每个 SCAP 版本下载。 该工具根据相应版本的 SP 800-126 [4]中指定的 SCAP 版本验证 SCAP 数据流的正确性。

11 如果同一产品有多个检查列表可用，则检查列表用户可能希望将所选检查列表中的

设置或步骤与其他检查列表进行比较，以查看哪些设置或步骤不同，并确定是否应使用这些备用建议中的任何一个。

12 这可能不适用于组织必须采用的检查表。

13 希望公布其自己版本检查列表的用户可以担任检查列表开发人员角色，并将其提交给 NIST 检查列表存储库，前提是原始检查列表上没有知识产权禁止这样做的限制。

14 为了简单起见，本文档的其余部分使用术语“开发人员”来指代正在开发核对检查列表的个人，个人或机构。

15 有关这些部分和此文档的最新更新，请访问 https://nvd.nist.gov/ncp/participation。 在正式同意参加该计划之前，应该咨询更新的材料。

16 US-CERT 网站是 https://www.us-cert.gov/。CERT / CC 网站是 https://www.cert.org/。NVD 位于 https://nvd.nist.gov/。

17 核对检查列表描述表格的离线版本可以从核对检查列表存储库的 NCP 参与材料网站下载，网址为 https://nvd.nist.gov/ncp/participation。

18 这是最近更新检查列表后的三年。

19 有关 SCAP 产品验证的更多信息，请参阅 https://scap.nist.gov/validation/faq.html 上的常见问题解答。

20 有关 CCE 的更多信息，请访问 https://nvd.nist.gov/config/cce。