美国软件供应链安全政策发展研究及启示

Research on Development and Implications of Software Supply Chain Security Policies in the United States

杨文钰[1]，赵相楠[1]，胡　方[2]，乔　雅[1]（1. 中国信息通信研究院安全研究所，北京 100083；2. 外交学院，北京 100037）
Yang Wenyu[1]，Zhao Xiangnan[1]，Hu Fang[2]，Qiao Ya[1]（1. Security Research Institute，China Academy of Information and Communications Technology，Beijing 100083，China；2. China Foreign Affairs University，Beijing 100037，China）

摘　要：
近年来，针对软件供应链的网络攻击日渐增多，其影响范围和程度不断扩大，软件供应链安全已成为全球性的挑战。为应对日益上升的威胁和挑战，美国政府对软件供应链风险管理工作做了全面的规划和部署。迄今为止，各项工作稳步推进，取得了一系列成果，也存在一定的局限性。对美国软件供应链安全相关工作进展和具体成果开展跟踪研究，梳理了美国政府机构的软件供应链安全职责和监管举措，分析其优点和局限性，以期为我国软件供应链安全治理提供借鉴。

关键词：
软件供应链；安全政策；软件安全；风险管理；透明度
doi：10.12045/j.issn.1007-3043.2025.12.015
文章编号：1007-3043（2025）12-0083-06
中图分类号：TP309
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In recent years，cyber attacks on the software supply chain have grown in frequency and scope，making software supply chain security a global challenge. To address the rising threats and challenges，the United States government has undertaken comprehensive planning and deployment of software supply chain risk management. So far，the work has progressed well，and a number of outcomes have been obtained，but there are also certain limitations. It conducts a tracking research on the progress of initiatives related to the security of the US software supply chain，outlines the responsibilities and regulatory measures of US government agencies，and analyzes their advantages and limitations to provide references for the secure development of China's software supply chain.

Keywords：
Software supply chain；Security policy；Software security；Risk management；Transparency

引用格式：杨文钰，赵相楠，胡方，等. 美国软件供应链安全政策发展研究及启示[J]. 邮电设计技术，2025（12）：83-88.

0 引言

当前，软件已成为支撑人类社会运转的基础设施之一，与个人生活、社会民生、国家发展紧密相关[1]。随着软件产业的蓬勃发展，软件供应链结构也越发错综复杂。在当今高度互联的时代背景下，软件供应链面临的威胁和风险正变得严峻[2-3]。恶意软件注入、代码非法篡改、数据泄露等问题屡见不鲜，针对软件供应链的网络攻击事件频发。这些安全风险不仅会严重损害公众信任，给企业带来巨大的经济损失，甚至可能会对国家安全构成威胁[4]。

美国是网络信息技术的发源地，对全球网络信息技术和产业的发展产生了较大的影响，在全球软件供应链治理秩序的形成过程中也发挥了重要的作用[5]。基于此，本文梳理了美国政府在软件供应链安全方面

通讯作者：赵相楠，zhaoxiangnan@caict.ac.cn
收稿日期：2025-11-05

的职责和管理举措，总结其经验，并基于我国国情，提出针对我国软件供应链安全建设的建议，以推动构建一个更安全、可靠的软件供应链生态系统。

1 美国软件供应链安全监管举措发展历程

1.1 初期监管措施

美国对供应链安全的关注最早可追溯到21世纪初。“9·11”事件后，为进一步打击恐怖活动，小布什提出诸多网络安全政策，并对政府组织架构进行调整[6]。布什政府发布的《确保网络空间安全国家战略》要求相关部门对供应链与信息安全风险的关系展开研究，这表明美国政府已经开始认识到供应链安全的重要性。

2008年，美国启动了“国家网络安全综合倡议”，其中包含对“开发全球供应链风险管理的多维手段”的倡议，强调需在产品、服务的全生命周期内综合应对国内和全球供应链风险。次年，奥巴马政府发布《网络空间政策评估——保障可信和强健的信息和通信基础设施》报告，全面审视了全球化背景下的供应链安全问题，ICT供应链安全随即被提升至国家安全的高度[6]。

随着网络全球化的深入发展，美国开始出台细化举措，聚焦政府部门的软件供应链风险评估和完整性保障。如美国国会于2014年提出《网络供应链管理和透明度法案》，旨在保障美国政府开发或购买的各类包含第三方或开源组件的软件、固件或产品的完整性。美国国家标准与技术研究院（NIST）又于次年发布了《联邦信息系统和组织供应链风险管理方法》（NIST SP800-161），用于指导美国联邦政府机构管理ICT供应链的安全风险，包括识别、评估和缓解ICT供应链风险等。

总之，在早期，由于尚未出现大规模的软件供应链攻击事件，美国软件供应链安全举措基本被包含在IT或者ICT供应链举措之下，政府的关注点由宏观向细分概念逐渐聚焦，但学界和业界对软件供应链的关注有限[1]。2020年底，“太阳风”事件爆发，美国政府对软件供应链安全的重视进一步提升[7]，开始出台专门针对软件供应链安全的举措。

1.2 拜登政府的软件供应链安全措施

在软件供应链攻击愈演愈烈的形势下，2021年，美国总统拜登签署了《保护美国供应链》（EO 14017）和《改善国家网络安全》（EO 14028）这2份行政命令，标志着美国政府在软件供应链安全方面采取了更加系统和前瞻性的行动[8-9]。

具体来看，2021年2月发布的EO 14017旨在强化供应链的弹性，并集合所有相关政府机构的力量对重要领域进行供应链审查，其中涉及ICT软件、数据和相关服务。而EO 14028第4章“提高软件供应链安全性”指出，在政府所使用软件的开发和部署过程中，需实行更严格和可预测的机制，确保软件产品的安全运行。此外，该行政令还对NIST、管理和预算办公室（OMB）、网络安全和基础设施安全局（CISA）等机构提出了具体工作要点。近年来，与美国软件供应链安全相关的工作内容大多可追溯到这项行政命令。

1.3 美国软件供应链安全管理体系

美国软件供应链安全相关机构的举措如图1所示。

由图1可知，美国的软件供应链安全管理由多个政府部门配合完成，这些部门在软件供应链安全中承担的工作各有侧重。商务部重点关注软件供应链的透明度，研究了软件物料清单的组成和实践。国防部从技术角度出发，致力于提升供应链透明度。国土安全部则在基础设施方面进行重点保护，为重要系统的软件供应商和需求方提供实践操作指南。以上部门的实际工作通常由各部门下属的机构执行，如NIST、CISA和NSA等。

综合来看，美国的软件供应链安全管理涵盖了多个方面，各部门各司其职，为软件供应链的安全管理提供了全方位的支持。

2 美国政府机构主要职责与举措分析

2.1 美国国家标准与技术研究院

根据行政命令EO 14028的要求，NIST工作主要集中在关键软件的定义以及软件的开发、测试等全生命周期的安全。

在关键软件的使用层面，NIST于2021年6月发布了《关键软件定义》文件。该文件首先介绍了关于“关键软件”中“关键”的定义，其次说明了“关键软件”的定义并给出了初步的软件分类，最后要求所有政府实体的“关键软件”都遵循严格的安全标准。在此基础上，NIST进一步发布了《根据EO 14028使用“关键软件”的安全措施——指导目的和范围》，该指南规范了美国政府对“关键软件”采取的安全措施以及测试其源代码的最低标准，提出了保护软件所用数据的机密

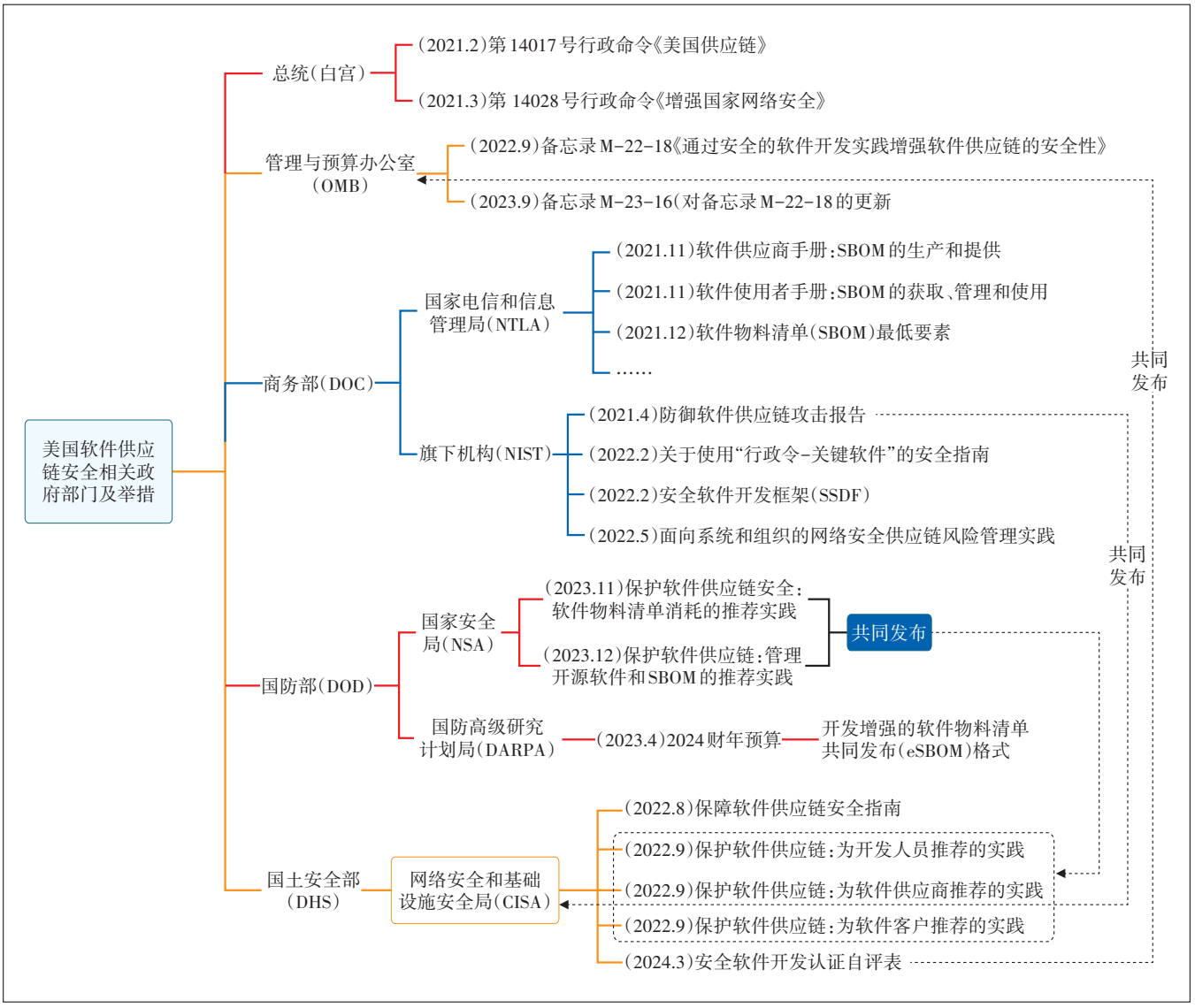

图1　美国软件供应链安全管理相关部门及举措

性、完整性和可用性，建立和维护数据清单等要求。

在软件安全开发层面，2022年2月，NIST更新了安全软件开发框架（SSDF），该框架概述了在软件开发过程中，为确保软件安全性而遵循的基本实践。该框架本身并不属于监管或合同要求，而是从软件开发者和供应商的角度提出要求，为行业内的企业和从业者提供了参考，旨在从源头减少软件漏洞和安全风险，从而保障美国的软件供应链安全。

在软件安全测试层面，NIST于2021年10月发布了《开发者软件验证最低标准指南》，概述了关键软件应采取的安全措施，并设定了供应商测试其软件源代码的最低标准的指南。该指南提出11条关于软件验证的建议，明确指出为确保软件质量和安全性，开发人员需要遵循的最低标准。该指南的特点在于从开发者及供应商的角度出发提供指导，有利于提高软件开发人员的专业化水平。

2.2　美国网络安全与基础设施安全局

CISA隶属于美国国土安全部（DHS），在关键基础设施安全方面扮演关键的角色，在软件供应链安全管理方面发挥着至关重要的作用。在其他机构的配合下，该机构从攻防角度出发，为开发人员、供应商和用户3个主要角色提供指导。

具体来看，为贯彻《国家网络安全战略》，CISA发布了《2024—2026财年网络安全战略计划》，强调软件

供应商应提高软件供应链的透明度，并提出了采用软件物料清单（SBOM）和严格的漏洞披露实践等措施。CISA也关注软件供应链安全开发层面的工作，与OMB共同更新了安全软件开发证明表。该证明表与NIST发布的SSDF相辅相成，为联邦政府提供软件的供应商会被要求提交其软件的安全性证明。

在实践指南方面，2022年，CISA和美国国家安全局（NSA）共同发布了一系列保护软件供应链安全的指南，分别为开发人员、软件供应商和软件用户推荐了实践方法，为其应对软件供应链的安全风险提供参考。

面向开发人员的实践指南强调了软件安全开发的重要性，从安全代码开发、验证第三方组件、开发环境加固和代码交付等角度出发，分析可能出现的威胁场景并提供缓解措施；面向软件供应商的实践指南指出了软件供应商需要承担的责任和改进举措，强调了供应商在软件交付过程中需对代码进行数字签名，以保护软件的完整性；面向软件用户的指南则从产品的获取与评估、产品的部署与验收测试和软件产品的操作更新等方面出发，帮助使用者检验产品的安全性。

2.3 其他机构

除NIST和CISA之外，还有多个部门积极采取了相关举措，具体如下。

美国政府管理与预算办公室（OMB）主要负责协助总统协调各政府部门的工作，扩大机构间的合作。在软件供应链安全方面，该部门的工作旨在强化美国软件供应链安全政策的连贯性，敦促既有标准规范和部署的实施。例如，OMB发布了2份备忘录（M-22-18和M-23-16），要求所有为联邦政府提供软件产品及服务的供应商提供软件安全证明，还在附录部分给出了各政府机构开展行动的时间表，并对EO 14028行政命令的部署进行了进一步的明确。2023年9月，OMB发布的备忘录M-23-16更新了M-22-18的部分条例和要求，重申了软件安全开发环境的重要性，敦促相关软件供应商了解新的认证要求，确定其提供给联邦政府的软件的合规性。

国家电信与信息管理局（NTIA）隶属于商务部，该机构长期关注软件组件的透明度，于2021年7月发布了SBOM的最小要素，而全面推进SBOM的应用是提升软件透明度的关键行动[9]。NIST、CISA等美国政府机构都将SBOM视为推进软件供应链风险管理的首要任务，并将其作为多项政策和标准的基础理念。自2021年11月起，NTIA还相继发布了《软件供应商手册：SBOM生成和提供》和《软件使用者手册：SBOM的获取、管理和使用》等系列文件，强调了SBOM对于软件供应链安全的重要性。

NSA旨在保障美国政府通信和信息系统的安全，防范和应对各种网络威胁和攻击。在软件供应链安全领域，该机构重点关注软件供应链透明度。2023年11月，在OMB备忘录M-23-16的部署下，NSA发布《保护软件供应链：SBOM使用的推荐实践》，该指南旨在帮助软件开发者、供应商和使用者通过合同的形式，传递软件组件和漏洞信息，降低软件供应链受到恶意攻击的风险。次月，该机构发布了《保护软件供应链：管理开源软件和SBOM的推荐实践》，为软件开发人员的开发活动提供指导性建议，旨在提高相关人员对软件安全性的认识。

国防高级研究计划局（DARPA）是美国国防部的下属机构，其使命是确保美国在技术和科学研究方面占据领先地位，主要通过资助尖端技术研发的方式来增强国家安全。2024年3月，DARPA发布了财年预算，计划在2024年开发增强的软件物料清单（eSBOM）格式，在原有要素的基础上基于安全需求进行丰富，并启动网络推理算法和相关工具的开发，旨在运用eSBOM发现软件开发过程中的潜在缺陷并进行防御，对软件开发、测试和维护过程进行全面改进。

3 美国软件供应链安全相关举措的亮点与局限性

3.1 管理措施的亮点

软件供应链攻击可能发生在软件的开发环节、交付环节和使用环节，不同环节建议采取的措施如表1所示。

由表1可知，美国在软件生命周期安全管理、责任分配和协作机制、系统化的漏洞管理、透明的SBOM机制等方面具有以下突出优势。

a）分阶段管理。从软件的开发、交付到使用过程，各个阶段都有明确的管理措施和责任分配。这种分阶段管理体系确保了每个环节的责任人都能有效识别和应对软件安全风险，并及时采取应对措施。

b）标准化流程。通过实施SSDF和其他标准，确立了统一的安全开发流程。这种标准化流程有助于保证软件开发的一致性，确保安全措施的全面落实。

c）持续性改进。美国软件供应链安全管理体系

表1　美国软件供应链安全亮点内容

环节	内容	来源
开发环节	供应商作为开发商和客户之间的联络人，应承担以下责任。 a）保持安全交付的软件的完整性； b）验证软件包和更新； c）保持对已知漏洞的认识； d）接收客户对问题或新发现的漏洞的报告，并通知开发人员进行补救	《面向开发者的保护软件供应链安全实践指南》
	提出开发者在软件开发生命周期应经常、全面地进行验证，这是保证软件安全的一个重要因素	《开发者软件验证最低标准指南》
	提供了4类实践： a）组织准备：组织应确保人员、流程和技术都能在组织级别执行安全软件开发； b）保护软件：组织应保护其软件的所有组件免受篡改和未经授权的访问； c）生产安全可靠的软件：组织应生产安全可靠的软件，尽量减少安全漏洞； d）应对漏洞：组织应识别、响应并解决其软件版本中的残余漏洞，防止将来发生类似的漏洞	安全软件开发框架（SSDF）
	SBOM的最小要素：数据字段、自动化支持、实践和流程	软件物料清单（SBOM）的“最小元素”
交付环节	供应商需承担的责任： a）保持安全交付的软件的完整性； b）验证软件包和更新； c）保持对已知漏洞的认识； d）接受客户对问题或新发现的漏洞的报告，并通知开发人员进行补救	《面向供应商的供应链安全实践指南》
	责任分配：当软件供应商实施行业领先的开发实践时，他们的责任包括将来自第三方代码的风险最小化，计算安全软件开发实践的责任由最终软件产品的生产者承担，而不是联邦机构	备忘录M-22-18、M-23-16
	描述了在软件构建前、构建时和构建后的不同时间阶段，构造SBOM时可使用的方法工具、应考虑的信息类型、相应的特点和注意事项等	《软件供应商手册：SBOM生成和提供》
使用环节	建议用户在收到产品时进行全面检查、执行功能测试并从安全角度验证产品、设立负责产品生命周期的配置控制委员会、确保产品与现有环境集成以及监控更新等	《面向客户的软件供应链安全实践指南》
	为提高软件使用者在软件资产管理和漏洞管理过程中的透明度，供应商的SBOM必须完整，列举所有运用至产品中的第三方软件信息（包括开源和自研软件），以及运行时所需的所有安装包	《软件使用者手册：SBOM的获取、管理和使用》

强调对漏洞的持续监控和及时修复，确保软件安全措施能够不断适应新的威胁和挑战。

3.2 管理措施的局限性

美国部分软件供应链安全工作因历史沿革、联邦与各州之间政策存在差异等因素，在实施过程中存在局限性。

例如，EO 14028中提到应“消除共享威胁信息的障碍”，联邦政府应与服务提供商签订合同，后者需共享网络事件相关的数据、信息及报告。然而，由于部分企业对用户隐私的顾虑，加之美国各州的用户数据隐私和法律要求存在差异，此类合作倡议较难形成强制的要求[10]。

此外，美国软件供应链安全强调源头治理，关注从开发侧降低安全风险，因此要求供应商提交软件物料清单、安全软件开发证明表等。但在实际落实的过程中，许多供应商不希望暴露其软件产品的问题，或是出于担心知识产权受到侵犯等考量，不愿意配合以上措施[11]。

最后，软件安全性自证方面也存在公正性、有效性问题。供应商出于商业目的往往倾向于隐藏其产品的安全缺陷，存在脆弱性不被发现的侥幸心理，无法证明其填写的安全软件开发证明表是否与实际情况一致，因而该措施的有效性仍需通过实践检验，并不断调整。

4 对我国软件供应链工作的启示

目前，我国已出台了部分标准，如《信息安全技术-ICT供应链安全风险管理指南》《网络安全技术 软件供应链安全要求》等，标准规范正在不断完善。部分行业在国家标准的指导下加紧制定、出台细化要求、方法及实践。以信息通信行业为例，中国通信标准化协会已制定电信和互联网行业的软件供应链安全系列标准框架，涵盖13项行业标准，旨在对软件供应全链条治理要素开展精细化治理，重点治理要素包括供方、需方、软件产品、软件服务、开源软件、供应链服务等。

但目前我国涉及软件供应链安全的标准多侧重于符合性评估，缺少对供应链的系统性安全要求[12]。且与国外相比，我国仍较为缺乏针对软件供应链的法律法规，软件供应链安全管理水平仍有待继续提升[13]。为提升我国的软件供应链安全管理水平，从软件供方、需方及第三方专业机构的角度出发，提出以下建议。

4.1 软件供应商

软件供应商作为软件供应链上游和对软件具有最深入了解的实体，其安全治理具有最佳的正外部性，应严格控制软件产品安全性。一是将SBOM与软件开发的生命周期相结合，包括在生成阶段合理设置字段元素，在运维阶段结合自动化工具、关联威胁情报及漏洞可利用性信息等，使SBOM的生成、更新、验证逐步融入软件全生命周期过程[14]，提高软件供应链

透明度并提高风险定位及溯源效率。二是增强安全开发意识和安全责任意识,在安全开发、安全测试、安全审查等方面明确责任人员及岗位职责,定期开展安全管理培训,全面提升团队成员的安全意识和技能。三是建立明确的软件供应链安全管理体系,制定标准化的操作程序,践行法规要求和行业最佳实践,为已交付软件提供安全运维,及时响应安全事件,积极与需求方、安全服务提供方联动,降低安全事件发生的可能性以及造成的负面影响。

4.2 软件需求方

软件需求方应关注软件的交付阶段与使用运维阶段的工作,并增强对供应商在安全软件开发方面的要求和审查。一是在采购软件时,除关注软件的功能契合度和易用性外,还应关注软件的安全性,充分评估软件供应商的安全能力,如要求软件供应商提供安全证明表及软件产品检测报告。关键信息基础设施相关需求方还可针对拟采购产品,进一步开展软件代码缺陷检测及漏洞分析等,确认软件的组成成分及安全风险状况。二是在使用软件的过程中,软件需求方应规范软件运维流程,跟踪软件及其组件相关的威胁情报,及时升级软件版本并安装补丁,降低未修复漏洞被利用的风险。三是对于外包开发的软件,在采购前应充分评估供应商安全软件开发流程,对供应商安全治理能力提出要求,并于外包开发完成、软件上线前开展综合安全测试,要求供应商处置完高风险项,确保高危漏洞不可被利用后再上线运营。

4.3 第三方专业机构

第三方专业机构可在标准制定、供应商能力评估、软件产品检测方面发挥积极作用,促进构建可信的软件产品及服务安全交付网络,为供应链安全管理提供支持。一是开展软件供应商安全能力评估相关标准的研制,建立合理化的评估流程,评估软件供应商的安全管理实践、安全要求和控制措施的合理性和有效性。二是建立科学合理的软件产品测试评估流程,综合使用软件成分分析、静态应用安全测试、交互式应用安全测试、动态应用安全测试、模糊测试等先进的软件产品检测技术,分析代码安全性,为安全评估提供重要的手段支撑[15]。三是加强对相关专业人员的能力培训,打造安全专家团队和系列精品课程,开展依托真实攻防场景、服务实战的软件供应链安全竞赛,提高安全服务实施人员的水平,切实提升软件供应链安全测试评估质量。

参考文献:

[1] 何熙巽,张玉清,刘奇旭. 软件供应链安全综述[J]. 信息安全学报,2020,5(1):57-73.
[2] 肖广娣,叶润国,焦程鹏. 我国软件供应链安全问题分析及对策研究[J]. 信息技术与标准化,2020(6):49-52.
[3] FERRAIUOLO A, RAZIEH B, TIZIANO S, et al. Policy transparency: authorization logic meets general transparency to prove software supply chain integrity[C]//Proceedings of the 2022 ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses. Los Angeles: Association for Computing Machinery, 2022: 3-13.
[4] SHAHMEHRI N, MAMMAR A, MONTES DE OCA E, et al. An advanced approach for modeling and detecting software vulnerabilities [J]. Information and Software Technology, 2012, 54(9): 997-1013.
[5] 李建伟. 美国网络安全监控战略与法制变迁及其启示[J]. 北京航空航天大学学报(社会科学版),2020,33(3):25-34.
[6] 左晓栋. 美国政府IT供应链安全政策和措施分析[J]. 信息网络安全,2010(5):10-12.
[7] ANDREOLI A, LOUNIS A, DEBBABI M, et al. On the prevalence of software supply chain attacks: empirical study and investigative framework[J]. Forensic Science International: Digital Investigation, 2023, 44(Supplement): 301508.
[8] 左晓栋. 美软件供应链安全工作进展及对我启示[J]. 保密科学技术,2022(12):32-39.
[9] 苏俐竹,徐雷,郭新海,等. 国内外软件供应链安全现状分析与对策建议[J]. 邮电设计技术,2022(9):24-26.
[10] 张晓玉. 美国《关于加强国家网络安全行政命令》解读[J]. 信息安全与通信保密,2022(1):32-37.
[11] 张烨阳,刘蔚,方时. 美国《改善国家网络安全的行政命令》执行情况分析及启示[J]. 全球科技经济瞭望,2023,38(1):69-76.
[12] 黄文波. 软件供应链攻击风险分析及应对措施[J]. 技术与市场,2020,27(6):44-47.
[13] 董国伟. 软件供应链安全态势综述[J]. 保密科学技术,2021(12):23-28.
[14] 王颉,万振华,王厚奎. 从软件安全开发生命周期实践的角度保障软件供应链安全[J]. 网络空间安全,2019,10(6):19-24.
[15] 齐越,刘金芳,李宁. 开源软件供应链安全风险分析[J]. 信息安全研究,2021,7(9):790-794.

作者简介:
杨文钰,工程师,硕士,主要研究领域为软件供应链安全、开源软件安全等;赵相楠,高级工程师,学士,主要研究领域为网络安全防护体系及攻防技术、软件供应链安全等;胡方,硕士,主要研究领域为国际政策、国别与区域、外国语言学及应用语言学等;乔雅,工程师,学士,主要研究领域为网络安全技术、软件供应链安全等。