DOI 10.15302/J-SSCAE-2016.06.021

国外 ICT 供应链安全管理研究及建议

倪光南[1]，陈晓桦[2]，尚燕敏[3]，王海龙[1]，徐克付[3]

（1. 中国科学院计算技术研究所，北京 100190；2. 中国网络空间研究院，北京 100010；
3. 中国科学院信息工程研究所，北京 100093）

摘要：鉴于国家关键基础设施和关键资源（CIKR）对信息通信技术（ICT）的依赖，识别和控制 ICT 供应链风险已成为保障国家安全的重要手段。美国作为 ICT 供应链管理的先行者，在提升战略地位、开展风险管理、确保软硬件安全、监管政府采购等方面为各国提供了丰富经验；欧盟、俄罗斯也加强了 ICT 供应链的安全管理。在分析上述国外情况的基础上，给出了完善我国 ICT 供应链安全管理的相关建议。

关键词：供应链风险管理；硬件供应链；软件供应链；采购安全

中图分类号：TP393.08　　**文献标识码：**A

Research on Foreign ICT Supply Chain Security Management with Suggestions

Ni Guangnan[1], Chen Xiaohua[2], Shang Yanmin[3], Wang Hailong[1], Xu Kefu[3]

(1. Institute of Computer Technology, Chinese Academy of Sciences, Beijing 100190, China; 2. Chinese Academy of Cyberspace Studies, Beijing 100010, China; 3. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: Given the nation's critical infrastructure and key resources (CIKR) reliance on information and communication technology (ICT), identifying and controlling the ICT supply chain risk has become an important factor when protecting national security. As the forerunner of ICT supply chain management, the US provides rich experience in enhancing the strategic position of the ICT supply chain, establishing the standards of ICT supply chain management, ensuring the security of software and hardware in the ICT supply chain, and supervising the procurement of ICT supply chains. In addition, the EU and Russia also specifically strengthen the security management of the ICT supply chain. Based on the above research, this paper provides some suggestions on the security management of the ICT supply chain in China.

Key words: supply chain risk management; hardware supply chain; software supply chain; procurement security

一、前言

信息通信技术（ICT）供应链包括硬件供应链和软件供应链，通常涵盖采购、开发、外包、集成等环节。其最终的安全很大程度上取决于这些中间环节，涉及到采购方、系统集成方、网络提供方以及软硬件供应商等[1]。ICT 供应链是所有其他供应链的基础，是“供应链的供应链”[2]。在 ICT 采购全球化的态势下，ICT 供应链安全与国家安全间的关系愈发密切。ICT 产品在原料采购、生产、运输

收稿日期：2016-10-20；**修回日期：**2016-10-25

作者简介：倪光南，中国工程院，院士，中国科学院计算技术研究所，研究员，研究方向为多媒体技术；E-mail: ngn@public.bta.net.cn

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

本刊网址：www.enginsci.cn

直至交付给最终客户的过程中，任何一个环节都有可能存在影响 ICT 产品安全性的因素。如果考虑到信息安全的对抗性质，来自国外的 ICT 产品供应商完全有可能、有条件在产品中设置恶意功能，如在软硬件中嵌入恶意程序、突然中断关键 ICT 产品或后续服务等。

鉴于国家关键基础设施和关键资源（CIKR）对 ICT 技术的依赖，识别和控制 ICT 供应链风险，加强 ICT 供应链安全管理已经成为保障国家安全的重要手段。在国家战略以及标准制定层面，美国、欧盟、俄罗斯等都提升了 ICT 供应链安全管理的地位，本文将从上述两方面深入研究国外的相关政策制度。在管理活动层面，本文将对国际现行的 ICT 硬件安全管理和软件安全管理进行探讨；并进一步以美国为例，对软硬件安全中涉及的采购环节的安全管理进行分析。本文旨在参考各国经验，为加强我国 ICT 供应链安全管理、建立我国 ICT 供应链安全评估制度提供建议。

二、国外 ICT 供应链安全管理政策

（一）ICT 供应链安全战略定位

长期以来，美国非常注重 ICT 供应链安全。2008 年布什政府提出国家网络安全综合计划（CNCI），提出建立全方位的措施来实施全球供应链风险管理 [3]。在此基础上，2009 年奥巴马政府指出不应局限于仅谴责国外产品和服务供应商，同时提出了新的供应链风险管理方法已经势在必行。2011 年美国在发布的《网络空间国际战略》中将“与工业部门磋商，加强高科技供应链的安全性”作为保护网络空间安全的优先政策，该项政策将 ICT 供应链安全提升至保障网络空间安全的高度 [4]。

欧盟、俄罗斯和中国同样将 ICT 供应链安全上升到国家安全的战略高度。欧盟《供应链完整性》报告指出，ICT 供应链完整性是国家经济发展的关键因素，提高供应链完整度对公共和私营部门意义重大 [5]。中俄共同提交联合国的《信息安全国际行为准则》强调，应当努力确保信息技术产品和服务供应链的安全，防止他国利用自身资源、关键设施、核心技术及其他优势，削弱落后国家对信息技术的自主控制权，或威胁落后国家的政治、经济和社会安全 [6]。

（二）ICT 供应链风险管理

1. 美国国家标准与技术研究院（NIST）

NIST 为保护非国家安全的联邦信息和通信基础设施，负责开发标准、指南、测试和度量指标。NIST 已经与公共和私营部门的利益相关者合作，研究和开发 ICT 供应链风险管理（SCRM）的工具与指标，以及有关 ICT 供应链风险的缓解措施和实施方法的指南。

2. ICT SCRM 项目及相关资源

（1）CNCI#11

2008 年，为响应 CNCI#11“建立全方位的方法来实施全球供应链风险管理”，布什政府启动了非国家安全信息系统供应链风险管理实践开发计划，即 ICT SCRM。

CNCI#11 为美国联邦机构信息系统的供应链风险管理提供了全面的方法。CNCI#11 第二工作组（WG2）通过提供与采购决策相关的威胁、漏洞和后果的高度评估，同时识别并减轻整个产品和服务生命周期中资源的风险，来促进 SCRM 的提升。

（2）NIST SP800-161

NIST SP800-161《联邦信息系统和组织供应链风险管理实践》为联邦机构制定相应的政策、程序，为有效管理 ICT 供应链风险提供指导 [7]。针对 ICT 产品的整个系统开发生命周期，NIST SP 800-161 可为其提供开发 ICT SCRM 计划的模板。该模板详细介绍了一套评估和管理供应链风险的程序，并列出了适用的威胁事件和可供参考的风险框架，用于评估威胁和确定缓解对策（即评价事件的相关性和潜在影响的方法）。这些程序被集成到 NIST SP800-39 的风险管理过程（架构、评估、响应和监控）中，作为联邦机构整体风险管理活动的一部分来实施 [8]。

（3）NIST IR7622

NIST IR7622《联邦信息系统供应链风险管理实践理论》是 NIST 发布的网络供应链风险管理指南，旨在消除购买、开发和运营过程中高影响联合信息系统面临的生命周期供应链风险 [9]；该标准同时介绍了 ICT SCRM 的方法和做法。

NIST IR7622（NIST 7622-2）第二版阐述了供应链风险管理在 ICT 领域中的应用，提供了一套实例可直接应用于那些级别达到联邦信息处理标准（FIPS）的采购或合同中。其涉及到信息系统采购方、采购团队、信息系统安全负责人和负责信息系统交

付的相关工程师，涵盖为政府和商业机构提供产品和信息安全服务的所有环节。

NIST IR7622-2 还给出了供应链风险管理的实施流程（见图 1）。对于 FIPS199 这样高影响的系统，ICT 供应链风险管理被明确嵌入到采购进程中来分析潜在的供应链风险，实施额外的安全控制以及供应链风险管理的实践；对中度影响的系统，授权机构应该做出是否实施 ICT 供应链风险管理的决策；低影响系统不需要实施大量的 ICT 供应链风险管理。

三、国外 ICT 供应链安全管理活动

（一）软 / 硬件供应链安全管理

1. 硬件供应链安全管理

ICT 硬件供应链是指 ICT 硬件采购、设计、制造、组装、维护到处理的一系列过程。

近年来 ICT 硬件供应链的长度、复杂性和脆弱性逐渐增加。全球范围内的政府部门都开始考虑 ICT 硬件供应链对 ICT 系统产生的威胁。在 ICT 硬件供应链系统与外部环境发生资源交换，以及在与供应链成员进行协调与合作的过程中，存在着各种内部或外部的不确定性风险因素。外部风险包括：自然灾害、恐怖事件、突发事件等；内部风险包括：供应中断，如攻击者中断制造和交付、错误的运输路线或延误交货、错误的订单（如数量或项目错误）、制造质量问题（如以硬件为基础引发的威胁）。

目前硬件供应链的风险管理主要针对三大硬件风险：硬件木马、恶意固件和硬件伪造。

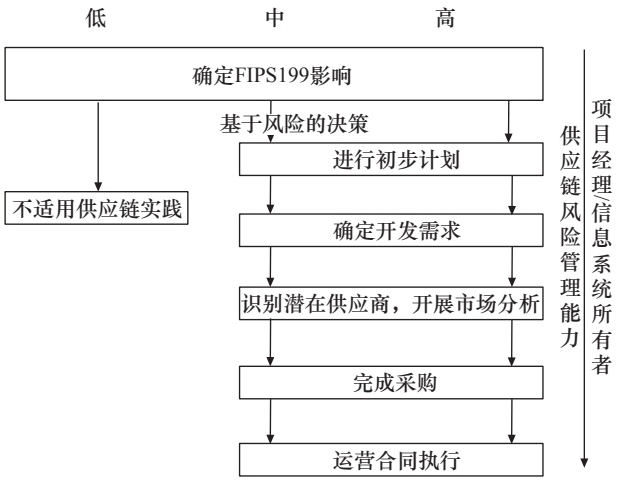

图 1　ICT SCRM 实施进程

2. 软件供应链安全管理

在关注硬件供应链安全的同时，切不可忽视软件供应链安全，因为任何一条供应链都不会脱离软件的使用。软件供应链可影响已交付系统的所有方面，只要供应链参与者能接触最终的软件代码或系统，那么危及软件供应链安全的风险就存在。参与者包括编写、加强和改变产品或系统内容的供应商、分销商、运输者和储存设施 [10]。

确保软件供应链安全的重要方法是软件供应链风险评估。风险评估是风险管理的一个基本方面，软件供应链风险评估是从风险管理角度，运用科学的方法和手段，系统分析软件供应链所面临的威胁及其存在的脆弱性，评估风险事件发生可能给整条供应链带来的影响或人们可能受到的损失程度，提出有针对性地抵御威胁的防护对策和更改措施。目前针对软件供应链的风险评估并不多，其中常用的是基于卡内基梅隆大学软件工程研究所（SEI）的风险评估方法。图 2 是 SEI 采用基于风险驱动的方法来评价系统化的软件供应链风险的原型。

（二）ICT 采购安全管理

1. 政府规章

20 世纪 90 年代末，美国已经意识到政府信息采购的安全性问题。1998 年 5 月 22 日，克林顿发布的第 63 号总统令中指出要确定大型采购任务中与其相关的信息安全。在布什执政期间，政府采购安全性被进一步明确，2002 年起草的国家安全战略中详细阐述了采购的步骤和过程，以及相关的标准。2008 年 12 月，在奥巴马上台之前，美国智库战略与国际研究中心（CSIS）发布了《在第 44 任总统任期内保护网络空间安全》的咨询报告，向新总统提出了若干重要建议，其中包括“通过采购规则提高安全性”，该条建议希望政府能与工业界合作，共同制定和执行 ICT 产品（软件居首要位置）采购安全指南 [11]。

除美国外，欧盟对 ICT 供应链采购安全也有明确规定。2016 年上半年，欧洲标准化机构——欧洲标准化委员会（CEN）、欧洲电工委员会（CENELEC）与欧洲电信标准协会（ETSI）对欧洲 ICT 产品和服务的政府采购所适用的可接入性提出了新的标

准。新标准是欧洲首次用法规和形式强调 ICT 产品和服务的政府采购所适用的可接入性，政府部门与其他公共机构在采购 ICT 产品和服务时，要确保服务、软件、电子设备与其他产品具有更好的可接入性。

2. 国防采购安全流程实例

对 ICT 产品和服务的采购主要分为国防采购和企业采购两类，其中国防采购的要求更高。下面以美国为例，简要介绍其在 ICT 产品和服务的安全采购方面的管理体系和采购系统，为我国 ICT 国防采购提供经验借鉴。

（1）ICT 采购管理

美国国防部的 ICT 采购实行国防部统一领导与军种分散实时结合的管理模式。所谓统一领导，是指在国防部设置专门负责采办、技术与后勤的副部长一职，统管全军 ICT 研发及采购事项；而分散实施，是按 ICT 项目的重要性及费用多少实行分类和分级管理。对于不同类别的 ICT 采购项目，负责采办、技术和后勤的副部长指派相应级别的里程碑决策当局进行监管（见图 3）。

（2）ICT 采购系统

美国国防部共有三个分系统来组织国防 ICT 采购，这三个系统互相配合，来完成军工产品的 ICT 采购。它们分别是规划、计划预算与执行系统（PPBE），联合能力集成与开发系统（JCIDS），采购运行系统（DAS）[12]。这三个系统在美国军工产

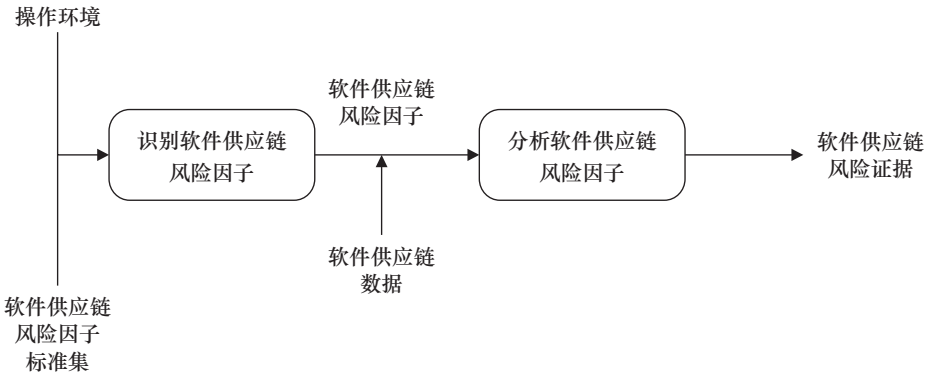

图 2　软件供应链风险评估

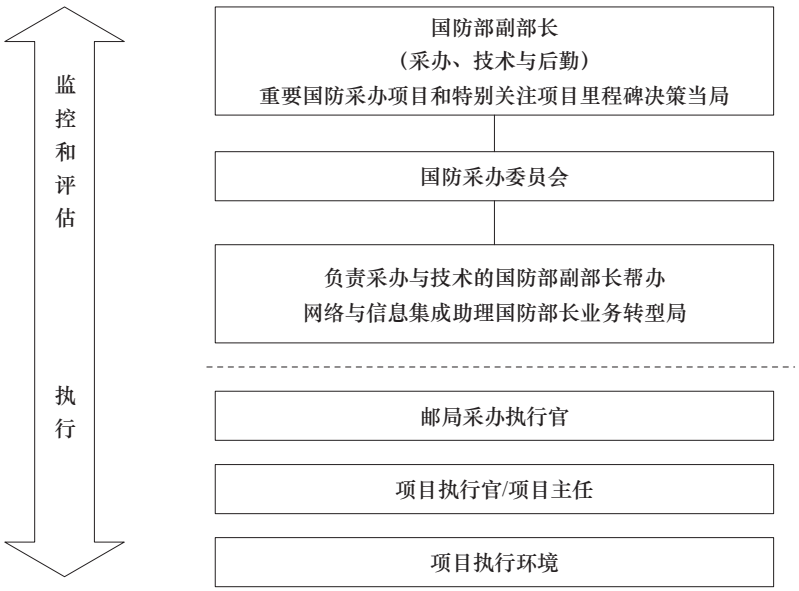

图 3　不同类别的 ICT 采办项目

品的 ICT 采购过程中相互支持，相互制约，确保 ICT 采购的安全。

四、对我国 ICT 供应链安全评估的建议

在我国 ICT 供应链处于劣势的背景下，根据《中华人民共和国国家安全法》要求，在国家网络安全审查工作中，加强 ICT 供应链安全评估管理、建立供应链安全评估制度是当务之急。在分析国外相关情况的基础上，给出我国 ICT 供应链安全管理和评估的几点建议。

（一）战略层面加强 ICT 供应链安全管理

从国家战略层面重视供应链安全管理，促进相应制度和标准的研究制定，加大探索研究与 ICT 供应链安全管理相关的核心技术。实施国家 ICT 供应链安全管理，使之作为国家网络安全保障的正当需求被国际社会所接受。建立供应链安全管理制度已成为国际通行做法，应在此基础上，进一步建立我国国家 ICT 供应链安全评估制度。

（二）将 ICT 供应链评估纳入网络安全审查

从加强国家供应链安全管理的角度出发，强化针对供应链的网络安全审查，对 ICT 产品和服务的设计、研发、制造、生产、分发、安装、运营、维护、采购等环节实施有效监督。将 ICT 供应链评估纳入网络安全审查，有利于澄清网络安全审查制度不是针对特定的国家或地区，可缓解外方对我国将该项制度当作贸易壁垒的担心和质疑。

（三）制定 ICT 供应链安全评估的法律法规

制定与完善国家政策、法律和标准，明确各方在 ICT 供应链安全评估中应当承担的责任和义务。ICT 供应链安全评估涉及多项法律的适用和协调，其中技术进出口管制、商用密码专控和认证许可都是与评估活动最为密切的法律制度，为了与网络安全审查的目的更加契合，需要进行适度调整。

（四）ICT 供应链安全评估的组织方式

改变分散的 ICT 供应链安全评估方式，设立统一的评估机构。评估机构可以是现有的与 ICT 供应链安全相关的管理部门，也可以建立专门的评估机构。评估机构负责统一部署和协调 ICT 供应链的安全管理与审查工作。

（五）建立 ICT 供应链安全评估程序

借鉴国际现有的信息安全评估制度，评估机构可运用供应链安全评估标准对 ICT 产品和服务的安全性能进行评估，其程序包括评估准备、一次评估、二次评估、定期评估、再认证评估等阶段。

五、结语

纵观国际现行 ICT 供应链安全管理的特点，我国应在以下几个方面做好准备工作：加强 ICT 供应链安全管理的战略研究；制定通用的 ICT 供应链安全评估标准；加强 ICT 供应链安全评估与现有信息安全制度的衔接。

参考文献

[1] Boyson S, Rossman H. Developing a cyber-supply chain assurance reference model [R]. Maryland: Supply Chain Management Center (SCMC), Robert H. Smith School of Business University of Maryland, 2009.

[2] Booz Allen Hamilton. Managing risk in global ICT supply chains: Best practices and standards for acquiring ICT[R]. McLean, Virginia: Booz Allen Hamilton, 2012.

[3] The comprehensive national cyber security initiative [EB/OL]. (2008-01-01) [2016-10-12]. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[4] Schmidt H A. International strategy for cyberspace [R]. Washington, DC: White House, 2011.

[5] Cadzow S, Giannopoulos G, Merle A, et al. Supply chain integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward (2015) [R/OL].(2015-09-11) [2016-10-15]. https://www.enisa.europa.eu/publications/sci-2015.

[6] The Embassy of the People's Republic of China in New Zealand (Cook Islands, Niue). China, Russia and other countries submit the document of international code of conduct for information security to the United Nations International code of conduct for information security [EB/OL].(2011-09-12) [2016-10-15]. http://www.chinaembassy.org.nz/eng/zgyw/t858978.htm

[7] Boyens J, Paulsen C, Moorthy R, et al. NIST special publication 800-161: Supply chain risk management practices for federal information systems and organizations [S]. Gaithersburg: National Institute of Standards and Technology, 2015.

[8] Ross R S. NIST special publication 800-39, managing information security risk: Organization, mission, and information system view [S] Gaithersburg: National Institute of Standards and Technology, 2011.

[9] Boyens J. NIST IR7622: Notional supply chain risk management

practices for federal information systems [S]. Gaithersburg: National Institute of Standards and Technology, 2012.

[10] Simpson S, Reddy D, Minnis B, et al. The software supply chain integrity framework: Defining risks and responsibilities for securing software in the global supply chain [S]. SAFECode, 2009.

[11] Langevin J R, McCaul M T, Charney S, et al. Securing cyberspace for the 44th presidency: A report of the CSIS commission on cybersecurity for the 44th presidency [R]. Washington, DC: Center for Strategic and International Studies, 2008.

[12] Chadwick S H. Defense acquisition: Overview, issues, and options for congress [R]. Washington, DC: Congressional Research Service, the Library of Congress, 2007.