DOI 10.15302/J-SSCAE-2016.06.008

网络安全审查制度研究及建议

陈晓桦[1]，何德全[2]，王海龙[3]，尚燕敏[4]，徐克付[4]

（1. 中国网络空间研究院，北京 100010；2. 中国信息安全评测中心，北京 100085；
3. 中国科学院计算技术研究所，北京 100190；4. 中国科学院信息工程研究所，北京 100093）

摘要：网络安全作为国家安全的一部分，其安全检查与评估所依循的规章制度分布在国家安全审查或网络空间管理的政策制度中。本文着眼于国际上现行的网络安全审查相关制度，重点分析各国在信息技术产品和服务安全评估、关键信息基础设施安全评估与管理、供应链安全和背景安全调查等方面的做法，从法律法规、组织体系、运行模式、审查方法和支撑技术等方面研究建立我国的网络安全审查制度。

关键词：网络安全审查；信息技术产品和服务；关键信息基础设施；供应链安全；背景安全

中图分类号：TP393.08　　**文献标识码：**A

Research on a Cybersecurity Review System with Suggestions

Chen Xiaohua[1], He Dequan[2], Wang Hailong[3], Shang Yanmin[4], Xu Kefu[4]

(1. Chinese Academy of Cyberspace Studies, Beijing 100010, China; 2. China Information Technology Security Evaluation Center, Beijing 100085; 3. Institute of Computer Technology, Chinese Academy of Sciences, Beijing 100190, China; 4. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: Cybersecurity is part of national security. The rules and regulations for security testing and evaluation are distributed as policies for national security review or cyberspace management. This paper focuses on the current international systems related to cybersecurity review, and analyzes governments' practices in the aspects of information technology product and service security evaluation, critical information infrastructure security evaluation and management, information and communication technology (ICT) supply chain security, and background security investigation. Based on the above, this paper discusses how to establish a cybersecurity review system in the fields of law and regulation, organization framework, operation mode, review approach, and supporting technology.

Key words: cybersecurity review; information technology product and service; critical information infrastructure; supply chain security; background security

一、背景

当前，网络空间已成为国家间不见硝烟、激烈博弈的主战场，技术漏洞、产品后门等安全隐患可能给国家利益带来灾难性损失。根据美国国家安全情报机构前雇员斯诺登提供的文件曝光，美国某些

收稿日期：2016-10-12；**修回日期：**2016-10-17

作者简介：陈晓桦，中国网络空间研究院，副院长，研究员，研究方向为网络安全审查、网络安全评价与标准、云计算和大数据安全；E-mail: chenxhcn@263.net

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

著名的信息技术（IT）公司曾参与到“棱镜计划”中，协助美国情报机构窃取网络信息、监视多国政府和全球网民。而目前中国境内使用的芯片、操作系统、数据库、关键技术仍被国外公司垄断，存在严重安全威胁。同时，中国信息和通信技术（ICT）企业的产品则面临外国的严格审查，其在国际市场上进行收购等商业活动也屡次受到干预和阻止。

本文着眼于研究国外网络安全审查相关制度，为建立我国网络安全审查制度提供参考。

二、国外网络安全审查相关制度概述

美英等西方国家的国家安全审查制度较为成熟，并针对 ICT 产品纷纷设立了安全调查与评估制度，不仅涉及产品和服务，还包括产品和服务的提供商。目前，国外尚未见到针对网络安全专门设立审查制度的报道，但依据国家安全审查和信息安全管理制度，已开展严格的网络安全审查活动。

（一）美国网络安全审查相关法规政策

美国是世界上最早开展国家安全审查的国家，其法规主要包括《政府采购条例》（FAR）[1]、2007 年《外国投资和国家安全法案》（FINSA 2007）[2]、《埃克森 – 佛罗里奥修正案》[3] 等。

美国依托信息安全行业和专业测试机构的力量，凭借经济、技术优势，跟踪相关国家标准化战略和政策动向，控制国际标准主导权。通过国家安全审查，外国企业必须与美国的安全部门签署安全协议，协议包含公民隐私、数据和文件存储可靠性以及保证美国执法部门对网络实施有效监控等条款。

（二）美国联邦信息安全管理法案

美国在联邦信息安全管理法案（FISMA）[4] 的框架下对政府信息系统开展安全管理，表面上体现为一系列的标准、指南和报告要求。

FISMA 赋予各联邦机构、国家标准与技术研究院（NIST）[5] 以及白宫管理和预算办公室 [6] 保障信息系统安全的相应职责，要求每个联邦机构制定并实施相关文件，确保信息和信息系统的安全，以支持本机构的运行，保护联邦资产。

（三）美国国家安全审查机构

外国投资委员会（CFIUS）[7]，是一个跨部门的机构，代表们来自包括美国国防部、国务院以及国土安全部等，主席是美国的财政部部长。协调负责人是财政部投资安全办公室主管，负责接收、处理、协调并购申报。CFIUS 审查可能控制美国企业的外籍人士所进行的交易，以判定这类交易对美国国家安全的影响，但具体实施细节并不完全透明。

众议院特别情报委员会曾对华为和中兴公司开展了国家安全审查相关的调查工作 [8]，采取了访谈企业有关人员、查阅文件资料、召开听证会、现场调查等多种方式。其中，与政府、政党、军方、情报部门的关系是调查和质询的重点，收集企业高管及核心人员的言行和背景资料，结合企业的内部运营、外部经营、知识产权、研发情况等证据，达到最终证明存在引发国家安全问题的可能性。

（四）美国与英国的信息技术产品和服务安全评估

1. 美国信息技术安全认证

美国规定进入国家安全系统的、商业现货的信息安全产品及由信息安全功能使能的相关产品，必须通过美国国家信息保障联盟（NIAP）[9] 通用准则评估认证体系（CCEVS）的评估认证；政府部门采购该类产品时，必须从 NIAP 审查通过的产品清单中选择满足安全要求的产品 [10]。其中国家安全系统是指属于美国政府部门的，处理涉密信息及军事、情报等敏感信息的信息系统。

2. 英国信息产品技术检查

英国电子通信安全组（CESG）[11] 统筹负责关于信息产品的安全认证工作，源代码检查是实施认证的重要手段，具体的测试认证工作可由 CESG 认可的商业机构负责。

3. 美国云计算服务安全评估

美国联邦风险和授权管理项目（FedRAMP）[12] 提供了对云服务进行安全评估、使用授权和持续监测的标准方法。通过 FedRAMP 项目，联邦机构在部署其信息系统时可以使用由 FedRAMP 授权的云服务，做到“一次授权，多次使用”。

（五）关键信息基础设施安全管理与评估

关键信息基础设施安全是网络安全的重要构成

部分，可以将国家关键信息基础设施保护视为风险管理流程。美国强调如果这类系统或资产遭到破坏或丧失工作能力，将对国家安全、国家经济安全、国家公众健康或公共安全，或任何这些事项的集合产生削弱影响。

美国早期的关键基础设施保护政策协调主要由关键基础设施保障办公室和国家关键基础设施保护中心负责。2002 年由美国国土安全部 [13] 履行这两个机构的职能，同时还指定了特定机构，包括农业部、健康和公共服务部、环境保护局、能源部、财政部、国防部，并采取了多项措施 [14,15] 加强对国家关键基础设施以及国家关键信息基础设施的保护。

（六）供应链安全管理

美国一直非常关注供应链安全，相继发布了《增强国际供应链安全的国家战略》[16]《联邦网络安全和信息保障研发计划》[17]《国家网络安全综合计划》[18] 以及《美国网络空间安全政策评估报告》等有关供应链安全的政策性文件，已经将 IT 供应链安全问题上升到了国家威胁和国家对抗的层面。美国国家标准与技术研究院（NIST）负责为非国家安全的联邦信息和通信基础设施的保护开发标准、指南、测试和度量指标，同时已经在研究和开发 ICT 供应链风险管理工具和指标，以及有关缓解措施和实施方法的指南 [19~23]。

（七）人员背景调查

人员背景调查在美国也称忠诚调查，是一个涉及多个部门、多种环节和因素，包括大量案头工作和实地走访在内的系统工程。

人事管理局（OPM）[24] 是负责制定背景调查总体规则及通行管理办法的政府机构，涉及国家安全或涉密的领域必须进行背景调查 [25,26]。出于国家安全方面的考虑，OPM 将所有联邦机构以及绝大多数政府合同商的工作职位按敏感程度和风险性划分为 6 大类，对应 10 种管理标准和要求。OPM 制定发布了“标准表格 86——国家安全职位调查表”[27]，要求对可能接触密级信息的政府人员进行背景调查；还制定发布了“标准表格 85——非敏感职位调查表”[28]，要求对政府雇员或按照合同为政府工作的人员进行背景调查。

三、建立我国网络安全审查制度的思考与建议

（一）网络安全审查制度基本内涵

基本定义：网络安全审查，是指对关系国家安全和社会稳定信息系统中使用的信息技术产品与服务及其提供者的安全性、可控性与可信性进行评估、监测分析、持续监督。

直接目的：防范产品和服务的提供者利用提供产品或服务的途径，非法控制、甚至干扰和破坏用户系统，非法监视用户行为，包括非法获取和利用用户敏感信息，如非法收集、存储和处理用户有关信息。

关键作用：从维护国家安全利益出发，对影响到重要信息系统和关键基础设施的重点产品与服务的安全性、可控性与可信性把关，加强对信息技术产品与服务安全的管理。

（二）网络安全审查制度法规标准

法规标准是保证网络安全审查的正当性、合法性、强制性以及可执行性。目前，网络安全审查的法律依据主要包括：《国家安全法》和《网络安全法》；政府信息系统管理与采购、信息技术产品与服务、关键信息基础设施、供应链安全管理等法律法规；相应的网络安全审查管理办法及实施细则；WTO 等国际准则。

此外，还应该制定软件安全审查、设备安全审查、服务安全审查、开发过程安全审查、背景审查等相关技术与管理标准。

（三）网络安全审查制度组织体系

科学合理的组织体系是完成网络安全审查各项工作的重要保证。主要机构及职能如下：跨部门网络安全审查委员会，是网络安全审查工作的总体负责和协调组织机构，成员由国家相关部门的代表组成；专家咨询委员会，网络安全审查工作的咨询建议机构；管理办公室，网络安全审查工作的行政管理机构，负责组织实施；审查执行机构；技术支撑机构。

（四）网络安全审查制度运行模式

1. 审查对象

网络安全审查的对象是信息技术产品和服务及其提供者。审查对象适用范围包括：用于关键信息

基础设施；用于国家、政府机构的重要信息系统；危害政治、社会、经济；损害公共利益；侵害公众权益；其他使用多、影响大且存在威胁国家安全风险的对象。

2. 审查内容

针对信息技术产品和服务及其提供者，网络安全审查的内容包括安全性、可控性与可信性。

安全性包括物理安全、逻辑安全、管理安全。物理安全：相关系统设备及设施受到物理保护，使之免遭破坏或丢失；逻辑安全指相关系统中信息资源的安全，包括保密性、完整性、可用性；管理安全包括各种安全管理的政策和机制。

可控性是指为了确保信息技术产品和服务能够且仅能按照使用者的指令提供应有的服务，对产品和服务进行安全监管，实现信息技术风险可监控、可管理，过程可审计的目标，包括可追溯性、可确定性、可审计性以及可审查性。

可信性是指企业（包括供应链）及企业核心人员，在规定的时间和范围内，能够具备相应技术、符合管理要求、提供澄清材料、回答设定质询以及承受调查审查的能力，从而在影响信息技术产品和服务的安全性和可控性以及影响国家安全方面达到的信任程度，能够被审查工作收集的情报和证据所验证并达到预设的、可接受的信任标准。

3. 启动条件

网络安全审查工作的启动应符合下列条件之一：依据法律法规明确要求；针对投诉举报；按照市场调查或抽查结果；自愿申请；或其他必要条件。

4. 审查方法

针对信息技术产品和服务的背景审查，目的在于提升国家对其可信性的掌控能力。背景审查的主要方法涉及情报搜集、挖掘、分析及检索。

（1）针对企业背景的审查方法

针对企业背景的审查，可以重点关注以下方面：与政府、政党、军方、情报部门的关系；企业声誉；公司资质；运营状况；信用记录；犯罪记录；生产环境；管理和实施部门；人员配置等。

（2）针对企业供应链的审查方法

企业背景必须包括供应链，主要考虑供应商管理体系及其执行情况，可以重点关注技术、质量、响应、交付、成本、环境、社会责任、网络安全等方面。

（3）针对员工背景的审查方法

员工包括企业高管人员（例如创始人、董事会成员、首席等）、产品主要设计人员、产品主要开发人员（无论处在离职还是在职状态）。针对员工背景的审查，可以重点关注以下方面：政治履历；工作经历；犯罪记录；信用记录；身体状况；家庭状况；精神状态；反人类言行等。

（4）问卷调查的方法

问卷调查是开展背景调查的重要依据之一，是对调查对象的初步评价，需要与调查对象进行多轮次交互。问卷调查在使用和设计时应注意的问题如下：使用要慎重；题目设计注重系统性、针对性、通用性以及差异性；选择题与问答题相互配合；具备合理的评价原则。

5. 支撑技术

（1）面向背景审查的支撑技术

在背景审查方面（包括供应链），应充分搜集、处理、分析、评判各方情报，从情报中发现危害国家安全的隐患。该过程主要包括情报搜集、跟踪调查、证据挖掘、情报关联、大数据分析、知识 / 数据库、风险评估、需求评估、研判决策等支撑技术。这些技术虽然有的已经很成熟了，但运用在背景审查上还需要进一步的改进和优化，才能满足实际应用的需求。

大数据分析是背景审查的核心支撑技术，由于背景审查需要源源不断地对国内外信息技术企业的全面状况进行跟踪调查，存储、整理、核查、更新、维护调查所得的各种证据信息，为之后的审查工作提供持续的历史资料和数据支持。

（2）面向技术审查的支撑技术

安全隐患分析是支撑技术审查的主要手段，包括源代码审计、逆向工程、渗透性测试等技术。

四、结语

目前，俄罗斯、日本、澳大利亚、印度等国家主要从信息产业外资并购安全审查、信息产品市场准入、信息产品安全认证等方面构建并完善与网络安全审查相关的制度体系。

借鉴上述各国经验，我国建立网络安全审查制度应注重以下方面：加强宣传，提高对网络安全审查的正确认识；制定措施，从政策支持、机制建立、

队伍建设、人才培养等方面进行考虑；重视背景审查和技术，开发配套的网络安全审查信息系统。

参考文献

[1] General Services Administration (GSA), U.S. Department of Defense (DoD), National Aeronautics and Space Administration (NASA). Federal acquisition regulation (FAR), FAC 2005_91 [Z/OL]. (2016-09-29) [2016-10-12]. https://www.acquisition.gov/?q=browsefar.

[2] U.S. Congress. Public law 110–49：Foreign investment and national security act of 2007(FINSA) [Z/OL]. Washington, DC: U.S. Government Printing Office, (2007-07-26) [2016-10-12]. https://www.gpo.gov/fdsys/pkg/STATUTE-121/pdf/STATUTE-121-Pg246.pdf.

[3] Peterson Institute for International Economics. The Exon-Florio amendment [Z/OL]. Washington, DC: Peterson Institute for International Economics. (2016-04-25) [2016-10-12]. https://piie.com/publications/chapters_preview/3918/02iie3918.pdf.

[4] U.S. Department of Homeland Security. Federal information security management act (FISMA) [Z/OL]. (2016-10-03) [2016-10-12]. https://www.dhs.gov/fisma.

[5] National Institute of Standards and Technology (NIST) [EB/OL]. [2016-10-12]. http://www.nist.gov/.

[6] Office of Management and Budget (OMB) [EB/OL]. [2016-10-12]. https://www.whitehouse.gov/omb.

[7] The committee on foreign investment in the United States (CFIUS) [EB/OL]. [2016-10-12]. https://www.treasury.gov/resource-center/international/Pages/Committee-on-Foreign-Investment-in-US.aspx.

[8] Rogers M, Ruppersberger D. Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE [J]. Journal of Current Issues in Media & Telecommunications, 2012,4(2):59.

[9] National Information Assurance Partnership (NIAP) [EB/OL]. [2016-10-12]. https://www.niap-ccevs.org/.

[10] NIAP. CCEVS objectives[EB/OL]. [2016-10-12]. https://www.niap-ccevs.org/Big_Picture/objectives.cfm.

[11] Communications-Electronics Security Group (CESG) [EB/OL]. (2012-05-14) [2016-10-12]. http://whatis.techtarget.com/definition/CESG.

[12] Federal Risk and Authorization Management Program (FedRAMP) [EB/OL]. (2016-10-05) [2016-10-12]. https://www.fedramp.gov/about-us/about/.

[13] U.S. Department of Homeland Security (DHS) [EB/OL]. [2016-10-12]. https://www.dhs.gov/.

[14] U.S. Department of Homeland Security. Homeland security presidential directive 7: critical infrastructure identification, prioritization, and protection [EB/OL]. (2015-09-22) [2016-10-12]. https://www.dhs.gov/homeland-security-presidential-directive-7.

[15] The White House. Executive order — Improving critical infrastructure cybersecurity [EB/OL]. (2013-02-12) [2016-10-12]. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[16] U.S. Department of Homeland Security. Strategy to enhance international supply chain security (July 2007)[EB/OL]. (2015-07-14) [2016-10-12]. https://www.dhs.gov/publication/international-supply-chain-security.

[17] Cyber Security and Information Assurance Interagency Working Group (CSIA IWG). Federal plan for cyber security and information assurance research and development [R]. Washington, DC: CSIA IWG, 2006.

[18] The White House. The comprehensive national cybersecurity initiative [EB/OL]. [2016-10-12]. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

[19] National Institute of Standard Technology. Standards for security categorization of federal information and information systems, FIPS PUB 199 [S]. Gaithersburg: NIST, 2004.

[20] National Institute of Standard Technology. Minimum security requirements for federal information and information systems, FIPS PUB 200[S]. Gaithersburg: NIST, 2006.

[21] National Institute of Standard Technology. Summary of NIST SP 800-53 revision 4, security and privacy controls for federal information systems and organizations[S]. Gaithersburg: NIST, 2014.

[22] National Institute of Standard Technology. Guideline for identifying an information system as a national security system, SP 800-59[S]. Gaithersburg: NIST, 2003.

[23] National Institute of Standard Technology. Guide for mapping types of information and information systems to security categories, SP 800-60 [S]. Gaithersburg: NIST, 2008.

[24] U.S. Office of Personnel Management (OPM) [EB/OL]. [2016-10-12]. https://www.opm.gov/.

[25] Farrell B S. Personal Security Clearances: Actions needed to ensure quality of background investigations and resulting decisions [R]. Washington, DC: U.S. Government Accountability Office, 2014.

[26] Federal Investigative Services. The security clearance and investigation process [R/OL]. Washington, DC: U.S. OPM. [2016-10-12]. http://www.brac.maryland.gov/documents/security%20clearance%20101%20pp%20presentation.pdf.

[27] U.S. Office of Personnel Management. Questionnaire for national security positions, OMB No. 3206 0005[Z/OL]. Washington, DC: U.S. OPM, 2010 [2016-10-12]. https://www.opm.gov/forms/pdf_fill/sf86.pdf.

[28] U.S. Office of Personnel Management. Questionnaire for non-sensitive positions, OMB No. 3206-0261 [Z/OL]. Washington, DC: U.S. OPM, 2013 [2016-10-12]. https://www.opm.gov/forms/pdf_fill/sf85.pdf.