

中国网络安全审查制度的建设

左晓栋 王石*

摘 要： 中国政府已经宣布，即将推出网络安全审查制度。本文研究了网络安全审查制度的重要意义，比较了国外网络安全审查制度的主要做法，对如何应对有关的贸易问题提出了建议，分析了我国网络安全审查制度的要点，并对继续推进网络安全审查制度建设做了展望。

关键词： 网络安全 审查制度 测评认证 贸易

2014年5月22日，新华社发布了一则重要消息：我国即将推出网络安全审查制度，凡事关国家安全和公共安全利益的系统所使用的重要信息技术产品和服务都应通过网络安全审查。新华社消息中还透露，该制度还将对进入我国市场的重要信息技术产品及其提供者进行网络安全审查，审查重点为该产品的安全性和可控性，旨在防止产品提供者利用提供产品的方便来非法控制、干扰、中断用户系统以及非法收集、存储、处理和利用用户信息，而不符合安全要求的产品和服务将不得在中国境内使用。

网络安全审查是我国网络安全工作中一项极为重要的管理制度，历经了多年的深入研究，也充分借鉴了国外的做法和经验。但这也是一项非常复杂的制度，涉及法规基础、产业支撑、技术保障、贸易博弈等多个方面。不断完善这项制度，充分发挥这项制度对保障国家网络安全乃至国家安全的重要作用，将任重而道远。

* 左晓栋，博士，高级工程师，中国信息安全研究院副院长，主要研究方向信息安全；王石，博士，中国信息安全研究院工程师，主要研究方向信息安全。



一 网络安全审查制度的意义

网络安全保障体系涉及很多方面的内容，例如法规、标准、人才、资金、技术、产业等。就保护网络与信息系统安全的过程而言，还包括预警、防护、检测、响应、恢复等环节。但归根结底，网络安全是高技术的对抗，信息技术产品和服务是决定网络与信息系统安全的根本。但信息技术产品和服务并非天然就是安全的。首先，产品中存在漏洞在所难免，虽然安全编程水平可以不断提升，但不可能彻底消除漏洞存在的可能性；其次，厂商有可能预设置后门便于开发、调试，但也不排除有厂商希望通过预设的后门来收集用户信息、控制用户系统以达到商业目的；再次，有些功能虽谈不上是后门，但不为用户所知或者超出了厂商的声明范围，尤以远程控制功能和数据回传功能为甚，厂商可以根据需要收集用户信息，必要时控制用户系统；最后，情报机构胁迫厂商预置间谍监听程序或通过攻击手段直接篡改厂商的出厂设备。

显然，在信息技术产品和服务进入使用环节前对安全性进行审查，以排除重大安全隐患，这应该成为一项基本的网络安全管理措施。但我国现有网络安全管理政策还远远不能满足国家安全的底线需求。从现实情况看，西方特别是美国的信息技术产品和服务已在我国呈全面渗透之势，而我国几乎对此未加防范。现在是必须采取行动的时候了。

二 国外网络安全审查制度的主要做法

（一）总体情况

各国尚未建立专门、独立且涵盖各领域的网络安全审查制度，但很多国家都已存在事实上的网络安全审查体系，往往由准入制度、采购制度、合格评定制度等组成，实质是对信息技术产品和服务的安全性进行评价，防止产品和服务带来网络安全风险。换言之，所谓的信息安全审查机制是广义的，是对具有安全审查功能的相关制度的统称。

总体而言，国外的网络安全审查制度主要有以下几类。



(1) 外资投资审查制度。外资并购境内企业或者在境内直接投资，需经政府相关主管部门审查通过后方可进行。审查的重点包括是否危害国家和社会公共利益，是否符合境内产业政策和环境保护政策，是否有利于促进竞争和不违背反垄断法律等。随着各国对国家安全问题的关注，不少国家建立了专门针对国家安全的外资投资特定审查制度。

(2) 重要领域或行业的业务准入审批制度。一些国家虽然将某些重要领域或行业向外资开放，但对相关的业务准入仍实行审批制，如电信、金融、电力、能源等。从事这些领域的相关业务需要经过政府审批，而不论是否含有外资成分。这类审批一般是出于对行业管理的需要，但有时也会涉及对网络安全的考虑。

(3) 对重要产品或服务的市场准入制度。一些国家对某些重要产品或服务的市场准入规定了较为严格的条件，包括安全管理要求，如电信设备的市场准入。由于信息技术的军民两用特性，世界上还没有哪个国家在市场准入环节对信息技术产品和服务实施专门的网络安全审查制度。

(4) 特定领域使用产品或服务的审查制度。对于某些部门或者涉及国防、军队、政府等重要单位使用的产品和服务，多数国家会从维护安全的角度对采购、使用相关信息技术产品和服务提出要求，制定更为严格的管理制度。

(二) 美国的典型做法

网络安全审查与贸易问题直接相关，各国对此都十分关注。由于 WTO 规则不涉及投资问题，故外资投资审查不违背 WTO 规则；重要领域或行业的业务准入审批制度以及重要产品或服务的市场准入制度虽然有时会涉及网络安全，但不以网络安全为主要目的，而是出于行业监管需求或遵循国际惯例；真正对信息技术产品和服务提出网络安全审查要求的，往往发生在产品和服务的使用环节。但针对不同的使用领域，国外一般采取不同的网络安全审查策略，美国最为典型。

1. 国家安全系统

(1) 对产品实施强制认证要求。自 2002 年 7 月起，美国已要求国家安全系统所使用的非密码类信息技术产品必须通过美国国家信息安全保障联盟 (NIAP) 通用准则 (CC) 认证。早在 2000 年，美国就宣布国家安全系统用于



保护非涉密信息的密码类信息技术产品必须通过国家标准和技术研究院（NIST）的 FIPS 140 认证。而国家安全系统中用于保护涉密信息的密码产品则一般由国家安全局（NSA）定制。

（2）对供应链实施全面安全风险。2013 年 11 月 18 日，美国国防部在《联邦采办条例国防部补充条例》中新增了网络安全临时政策——《供应链风险要求》，要求国防部对采购的信息产品和服务实施供应链安全风险评估。该政策规定，国防采购人可以针对已发现的供应链风险做出三种决定：一是拒绝采购不符合质量标准的产品和服务；二是拒绝采购未达到供应链安全评估等级的产品和服务；三是供应商不得采用不符合要求的下级供应商的产品和服务。这项信息技术供应链安全风险评估政策并没有公开任何流程和具体要求，且还规定国防采购人不得将不采购决策的部分或全部理由告知供应商。

2. 联邦信息系统

（1）总体要求。2002 年《联邦信息安全管理法》（FISMA）为美国联邦信息系统的保护确立了框架。根据 FISMA，如果合同商的系统存储了联邦机构的信息或者承接了联邦机构的业务，那么合同商的信息系统也必须满足 FISMA 的安全要求。

美国没有直接发布适用于政府信息系统的网络安全审查文件，但 FISMA 要求联邦信息系统应符合 NIST 制定的标准和指南的要求，实现最小的安全控制措施。这个最小的安全控制措施来自于 NIST 的特别出版物 SP 800-53，其中涉及网络安全审查的做法有以下两点。

①在 SP 800-53 的 17 类安全要求中专门列出了一类“系统和服务采办（SA）”安全要求。新版的 SP 800-53（2013 年 4 月发布）扩充了 SA 类下的“供应链保护”安全要求。而与供应链有关的安全要求均同时针对 3 类对象：联邦信息系统、信息系统组件、信息系统服务，即涵盖了系统、产品和服务。

②有针对性地提出了一些限制性安全要求，禁止采购和使用某些产品和服务。典型要求有：采用盲买机制，防止供应商知悉最终用户名单；供应商应进一步增强过程和安全措施的透明性；服务商应对下级供应商的过程和安全措施进行审查；从情报和执法机构处了解供应商的背景、声誉、履历等信息。SP 800-53 还特别要求“限制从特定供应商或国家采购”。

（2）云计算服务安全审查。2011 年，美国正式启动《联邦风险及授权管

理计划》(FedRAMP),标志着美国正式建立云计算服务安全审查制度。FedRAMP的基本思路是,由第三方评估机构根据FedRAMP云安全基线(来自于SP 800-53)对云计算服务进行安全风险评估,联合授权委员会根据评估结果对云服务商进行审查,对通过审查的云计算服务给予初始授权,联邦政府部门可在初始授权名单中根据自身需求选择通过审查的云计算服务商。FedRAMP明确要求联邦机构自2014年6月起必须采购和使用满足安全审查要求的云计算服务。

(3) 供应链风险管理措施。2014年7月,NIST发布SP 800-161《联邦信息系统和组织的供应链风险管理措施》草案,对信息技术产品和服务的风险防范提出了更系统、更专业的要求。供应链安全措施共分为16类,既需要对厂商进行细致的评估和审查,还需要在联邦信息系统中建立防范供应链风险的技术对策。

3. 重点行业信息系统

20世纪下半叶,鉴于各行业普遍高度依赖于信息技术,美国开始将关键基础设施(重点行业)的保护纳入政府的工作范畴。但美国有87%的关键基础设施掌握在私营业主手中,联邦政府不能干涉这些关键基础设施的运营。政府虽然希望获得监管私营关键基础设施网络安全的权力,包括对私营部门使用的信息技术产品和服务提出资质要求,但由于私营部门的反对,历次立法尝试均告失败。但美国还是为确保重点行业供应链安全而采取了一系列超常规的措施,特别是针对中国。

(1) 以个人而非组织名义对重点行业采购国外产品或服务的个案加以干涉。联想在美投资后,美国国务院受议员施压调整了对联想电脑的采购计划。2010年8月,华为与美国电信商Sprint价值60亿美元的电信合同在骆家辉等政界高官的警告下夭折。

(2) 抹黑竞争力强的中国企业。美国众议院情报委员会于2011年对中兴、华为发起特别调查并发布调查报告,以中国企业不透明、内设党委、有军工企业股份、企业负责人有军队履历等为由,认为中兴、华为对美国构成威胁,建议重点行业不要采购中兴、华为的产品和服务。此调查的直接后果是中兴、华为彻底退出美国的通信设备市场。

(3) 制造中国黑客威胁论,引发对中国的敌意。美国多年来连续炮制中



国黑客威胁论，污蔑中国政府和军方支持黑客实施网络攻击和窃取美国商业秘密。这为中国企业的国际化进程制造了极为不利的国际舆论，培养了用户对中国企业的敌视和防范心理，事实上设置了比采购禁令更为厚重的贸易壁垒。

(4) 直接入侵中国企业。自 2009 年起，美国国家安全局发起了针对华为的“狙击巨人”计划。最初目的是找到华为与中国军方之间联系的证据，同时监控华为高管的通信，并收集华为产品的信息，以竭力阻止华为电信设备在美国市场销售。但该计划随后升级为利用华为技术中的漏洞，通过入侵华为的设备来进行监控，还可以在获得总统许可的情况下发起攻击活动。

(三) 国外网络安全审查制度的主要特点

基于对美国网络安全审查做法的分析，并结合对其他国家网络安全审查制度的观察，可看出国外网络安全审查制度有如下特点。

1. 军队、情报领域以及涉密部门均设置了强制性网络安全审查

军队、情报领域以及涉密部门多被视为国家安全范畴，各国对此领域使用的信息技术产品和服务均施以严格的安全审查，国外的产品和服务几乎没有机会。这种审查的标准和流程很少公开，且一般都不接受供应商的申诉。

2. 政府信息系统的网络安全审查事实上是强制性的

政府信息系统不能笼统地直接归入国家安全范畴，为了与国家安全系统相区别，美国等国没有明文要求对政府采购国外信息技术产品和服务进行网络安全审查。但通过严密的制度设计和巧妙的操作手段，对政府信息系统的安全要求已经成为事实上的强制性审查要求，国外产品和服务难以绕过。

3. 未对重点行业设置强制性网络安全审查制度并不是出于 WTO 规则的约束

美国等国没对重点行业设置强制性网络安全审查制度，是受政治经济制度所限。但美国借此声称重点行业属于商用领域，不适用 WTO 的“国家安全例外”，以此来阻击其他国家的网络安全管理制度。

4. 看似公平的游戏规则隐含着巨大的不公平

西方国家一方面强调游戏规则开放性、公平性，另一方面在规则的实施流程中设置贸易壁垒。在我国企业按照国外所谓公开透明的政策、标准、合格评定制度送检产品时，对方往往在流程上制造障碍。比如：在申请国际认证时，以各种理由不接收企业递交的申请材料；不论实际申请的安全级别如何都

要求从最低级别的安全认证做起，而每一级别认证耗费的时间要以年计，逼企业知难而退；在检测和认证过程中对企业的任何问题不予回应，往往使之中途被迫搁置。

三 网络安全审查制度与贸易规则的关系

信息技术产品和服务本身是一种贸易对象，这就必然使我国网络安全审查制度受到国内外密切关注，并经受国际贸易规则的考验。网络安全贸易纠纷逐渐增多，各方围绕贸易规则的博弈正酣，迄今仍未达成共识。美、欧、日等国家和地区一方面以贸易规则为据抨击我国的网络安全管理政策，另一方面却以国家安全为由阻挠我国信息产业开拓国际市场。这成为网络安全审查制度构建无法回避的问题。

（一）美国对中国主要网络安全贸易诉求

以阻止我国实施无线局域网安全标准 WAPI 为开端，美国已联合欧、日等连续对我国多项网络安全政策提出异议，其核心诉求就是中国只能对军队和涉密系统使用产品和服务提出强制性要求，对其他领域则应放开管理，即使有合格评定制度也应基于国际标准。

（1）关于无线局域网安全标准 WAPI。有关部门原拟强制实施 WAPI 设备认证，在美国的交涉下宣布无限期推迟此制度。

（2）关于信息安全产品认证。有关部门原拟将此制度作为市场准入措施强制实施，后遭美、欧、日等国家和地区反对，该制度调整为仅在政府采购领域实施。

（3）关于信息安全等级保护制度。我国的制度要求第三级以上信息系统应使用本国生产的自主信息安全产品。而美国认为，根据 WTO 的国家安全例外，中国实施的任何强制性要求只能适用于军队和涉密信息系统，而重点行业属于商用系统，不能认定是国家安全范畴。

（4）商用密码管理制度。美国要求我国完全放开对商用密码的管理。

（5）信息安全标准。美国要求我国等同采用国际标准，反对我国自行制定国家标准。



(6) 互联网管理政策。先是欧洲议会投票声明网络审查是一项贸易壁垒,其后美国的互联网企业多次投诉,认为我国互联网管理政策有利于国内企业发展,对国外企业制造了不公平贸易环境。

(二) 美国对自身网络安全贸易措施的辩解

美国以网络安全为由先后采取了多种涉华贸易限制措施,如 CFIUS 对联想、华为在美投资启动国家安全审查,美国政府或国会对政府部门、重点行业采购中国 IT 产品进行直接干涉,美国众议院情报委员会对中兴、华为开展特别调查,在《2013 财年综合继续拨款法》中限制美 4 家政府部门购买中国的信息技术设备。辩解理由如下。

(1) CFIUS 的活动被中国人夸大了。统计表明,在外国公司并购美国公司的交易中,申请审查的只占 12.5%,最终开展审查的不到 1%,审查后撤销申报和遭总统否决的只占 0.6%。因此,CFIUS 对中国企业的审查不能真实反映美国的投资环境。

(2) 《2013 财年综合继续拨款法》确实要求限制采购中国的产品,但相关条款是法案投票前被某几位敌视中国的议员添加进去的,由于该法案长达 200 余页,正式投票前没有被人注意到,仅属个案。

(3) 美国政府从来没有出台限制采购中国产品的文件。虽然某些官员和议员对涉华采购案表示担心甚至否定,但纯属个人行为。

(4) 做出不采购决定的都是采购方,在法律上属于纯粹的商业合同行为,与政府无关。

(5) 美国国会对中兴和华为的调查是这两家公司自己请求的,美国没有这样的审查制度,且国会的行为与政府无关,政府无权干涉和约束。

(6) 在中兴、华为调查案中,国会只是发布了一个不具法律效力的普通报告,而不是行使立法权;报告也只是建议不采购中兴、华为设备,没有任何强制性。

(三) 网络安全贸易纠纷的性质和特点

综上所述,以下几点值得总结和思考。

(1) 中美网络安全贸易纠纷看似是经贸问题,实则是国家安全问题。自

2013 年起，中国对美投资已经超过美国对华投资，CFIUS 似乎不再对中国在美投资产生重大影响。但具体到信息技术领域，CFIUS 永远不会袖手旁观，因为这是涉及国家安全的“死生之地”。

(2) WTO 的“国家安全例外”条款往往被各国用来支持自己的管制政策。但 WTO 从未明确国家安全的范畴，这也造成了争议。美国要求我国将国家安全的范畴尽量缩小，而 CFIUS 的运作则表明，美国将国家安全范畴扩大到无所不包，随意性相当大。可以预见，美方对我国网络安全审查制度的重大质疑将是该项制度的范围问题，会让我国将重点行业排除在政府管制之外。

(3) 美国巧妙地规避了 WTO 的限制，但达到了同样的初衷。其制度设计十分精细，将政府摘得一干二净，难以在现有 WTO 规则下对其提出有效诉讼。美对自身网络安全贸易措施的说辞也充分证明了这一点。

(4) 网络安全贸易纠纷是围绕规则的一种对抗，但某种程度上又超越规则，是综合实力的较量。例如，美国一直在要求我加入 CC 互认协议，并要求我国认可国外认证机构颁发的 CC 证书，以使国外产品免于在我国接受检测或认证。但当我国企业在国外拿到 CC 证书并走出国门时，无论是美国还是其他国家此时都认为光 CC 证书是不够的，还要审查企业股东、企业透明度等并不见于国际标准的指标。这种双重标准的做法已经屡见不鲜，因此，我国企业必须熟悉规则、善用规则而不拘泥规则。^①

四 网络安全审查制度的要点

从我国实际情况出发，并借鉴国外先进经验，我国的网络安全审查制度需要把握好以下一些要点。

（一）紧密围绕国家安全的需要

不是所有领域使用的信息技术产品都要经过审查，而要限定在影响国家安全和公共利益的领域。事实上，金融、交通、通信、能源等这些涉及公共利益

^① 左晓栋：《近年中美网络安全贸易纠纷回顾及其对网络安全审查制度的启示》，《中国信息安全》2014 年第 8 期，第 63～72 页。



的领域本身也属于国家安全的范畴。但即便在上述领域，也不是所有的信息技术产品和服务都需要审查，而是要聚焦于重要产品和服务，也就是对网络安全有重大影响的产品和服务。

有人认为，有必要对存在隐患的产品和服务实施“先审后用”。这种看法的出发点是对的，但在 WTO 框架下，仅出发点正确并不够，还需有“必要性证明”，即必须证明所采取的措施是所有可能选项中对贸易影响最小的。我国已经加入 WTO，在不适用国家安全例外和一般安全例外的领域就没有必要以贸易措施来实现管理目标，这里有个平衡的问题。例如，把商用和一般领域内产品和服务的网络安全问题交由合同法、消费者权益保护法等去解决，不失为一种更妥善的办法。

美国在网络安全审查制度方面，当遇到某项制度涉及国家安全时，则完全在国家安全规则下议事，如美国 CFIUS 标准不完全公开，流程由内部掌握。这种安全审查流程的策略值得我们借鉴。

（二）将国家安全需求体现在供求合同中

网络安全审查制度面向的是国家安全需求，是“小众”，因此不能设计成市场准入制度。此外，政府没有必要为了维护产品和服务采购方的安全而将网络安全设计成行政许可，而是应将其融入采购方对产品和服务的招标要求之中，让网络安全审查要求更多地通过采购方去落实。以采购活动为名而行国家安全之实，这是国外的重要经验。

国家安全审查作为一种制度需要保持强大威慑力，平时少用慎用，用即见效。

（三）平衡与原有测评认证制度的关系

我国以前有多项信息安全产品测评认证制度，这些制度针对的也是产品和服务。在建立网络安全审查制度时，要充分采信已有制度的测试结果，避免重复工作。但传统的测评认证制度有两个不足，需要网络安全审查制度去补缺。

（1）传统制度只针对信息安全/网络安全产品，而不是所有的信息技术产品。信息安全/网络安全产品只是针对系统安全的附加产品，比如防火墙等，这只能保证外围安全，涉及系统本质安全的重要组件，包括服务器、操作系

统、数据库、应用软件等，都没有纳入认证制度。

(2) 传统制度主要是标准符合性验证，即测评时逐条对照标准，全部符合则表示通过测评。但标准是“死”的，不一定能及时反映供应链威胁的变化。更重要的是，标准主要关注产品和服务能够对外提供哪些安全功能，而网络安全审查制度有时是要防止攻击者“新增”某些恶意功能，角度有所不同。

(四) 突出对安全保障能力的考量

网络安全审查制度所关注的“安全”实质上可理解为“可信”，继而可分解为“可控”和“透明”。这正是美国国防部《可信计算机系统评估准则》(TCSEC)、欧洲《信息技术安全评价准则》(TCSEC)、国际标准 CC 提出“可信性”的目的所在。产品的安全功能再强大，如不能让用户放心使用，那其带来的风险有可能更大。反之，用户拒绝某个产品，并不一定意味着该产品功能太弱，而很可能是用户担心产品背后的厂商意图与攻击能力。

基于这样的考虑，网络安全审查制度应该关注厂商的背景、可靠性等因素。网络安全审查制度不分国内和国外，不是简单地把国外的产品拒之门外，而是要求产品体现出可控性和透明性。没有这两个方面，就不能保证产品的可信度。我们应该重视如下的问题，包括产品的远程控制功能、产品外传的信息、厂商收集的用户信息是否会应外国政府的要求而跨境流出等。

五 结束语

网络安全审查制度是国家信息安全的一道基本屏障，但这道屏障已缺失多年，这是因为我国自身的产业能力跟不上，长期受制于人。网络安全审查制度离不开合适的土壤，必须与自主创新政策同步推进。习近平总书记在 2014 年 6 月两院院士大会上指出，不能总是用别人的昨天来装扮自己的明天，不能总是指望依赖他人的科技成果来提高自己的科技水平，更不能做其他国家的技术附庸，永远跟在别人的后面亦步亦趋。这为创新我国的网络安全审查制度指明了方向。