美国人事管理中的信息安全审查制度及其启示

涂永前　　罗子越　　胡夏枫

摘　要　为了维护国家、组织安全与利益，信息安全审查成为重要岗位及行业从业者上岗前的重要流程。美国联邦政府公共行政管理领域安全保障体系完善，在信息安全审查程序与制度设计方面拥有丰富的历史经验并特点突出，如信息安全审查程序严格、雇佣双方权责统一。通过将美国公共部门与私人部门的安全审查进行深入对比，及其与中国政审制度进行比较，很明显中国政审制度在安全审查领域存在明显不足，如政审对象范围广、程序针对性差、内容狭窄、手段单一、延续性有待加强等，难以成为涉密人员安全审查的有效方式。美国在信息安全审查领域的经验是有益的借鉴，中国需要在原有的政审制度设计上进行改造和完善，在重要岗位和涉密人员安全审查方面探索具有中国特色的安全审查体系。

关键词　安全许可　组织安全　涉密人员　政审

作者涂永前，中国人民大学劳动人事学院研究员（北京 100872）；罗子越，中国人民大学劳动人事学院助理研究员（北京 100872）；胡夏枫，西南政法大学地方立法研究院研究员（重庆 401120）。

中图分类号 D73　　**文献标识码** A　　**文章编号** 0439-8041(2019)08-0065-13

在信息时代，窃密与反窃密斗争十分激烈，因此，许多国家（组织）将信息“安全审查”（security clearance）作为重要岗位及行业从业者上岗前的重要流程。当从业者工作涉及到国家（组织）安全、需要知悉国家（组织）涉密信息、接触重要设备资产、承担敏感职责、出入核心区域等时，通常需要接受比其他从业者更为严格的信息安全审查。行之有效的信息安全审查可以抑制雇佣双方利益不一致风险，具体作用于以下三个方面：（1）国家（组织）机制正常运行。个体的存在发展依赖于其在关系网的存在方式，国家（组织）机制的正常运行离不开公众和伙伴的作用，当涉密信息遭到泄露、重要设备资产受损、敏感职责履行不到位、核心区域曝光等事件发生时，国家（组织）信誉受损，机制的正常运行面临挑战。以斯诺登事件为例，斯诺登窃走 150 万份美国国家安全局（National Security Agency，简称 NSA）绝密文件并泄露了部分涉密信息，包括“棱镜计划”（监听美国以外地区使用参与该计划的公司产品服务的客户或任何与国外人士通信的美国公民，涉及国家包括美国部分“铁杆”盟友），美国因此受到了国际伙伴对于美国攻击他国通信网络，侵犯公民隐私权和言论自由权的谴责以及国内公民对于美国安全情报系统的质疑（因为斯诺登在上岗前曾接受信息安全审查，并获得绝密等级的安全许可）和对基本权利受损的批判，美国安全情报的部分项目被迫搁浅、改道，机制恢复正常运行耗费了大量的人力物力财力。（2）公众私密信息保

护。公众私密信息可能以多种形式储存于国家公共部门与私人部门。[①] 对于公共部门而言，信息安全审查有助于防范身份盗窃以及相关违法犯罪事件的发生，提升社会稳定性和公众幸福感。在 2013 年参议院财政委员会听证会上，美国卫生与公共服务部部长 Kathleen Sebelius 曾指出，美国存在着大量不需要进行刑事犯罪背景调查就可以在公众不知情的情况下凭借岗位特权获得并非法使用公众个人私密信息的雇员。[②] 无独有偶，近年来，我国因公民私密信息泄露而导致身份盗窃案发生频次大幅上升，领域多方扩展，严重侵犯了公民自然权利。而对于私人部门来说，上岗前信息安全审查和保密教育培训有助于客户隐私权的保护，在大数据时代以信息优势拓宽客户渠道、稳定客户流、建立长期信赖的客户关系，从而巩固企业核心竞争力。（3）部门和人员绩效提升。根据 Richard G Brody 的统计，企业面临的一件过失雇佣的诉讼成本大约为 100 万美元，并有 79% 的诉讼是企业败诉。[③] 部门规范信息安全审查程序与制度设计一方面有利于降低过失雇佣的机会成本，另一方面有利于提升雇员的“人”“岗”匹配度，优化岗位设置与人事安排，提高部门绩效。而对相关从业者而言，为了通过安全许可审查，获得和维系安全许可，在工作和生活中都需要积极培养政治意识、责任意识和忧患意识，牢固掌握接触涉密信息、设备、场所的相关规则，以高水平的工作效率和良好的工作态度自觉维护国家（组织）利益，提升组织绩效。

由此可见，重要岗位及行业从业者的信息安全审查对于国家、组织和个人都具有客观性和必要性。

一、信息安全审查的基本内涵

涉密人员管理包括上岗、在岗、离岗管理，重要岗位及行业从业者的信息安全审查归属于涉密人员管理的上岗管理环节。国内研究方面，王鸿杰提出中国应当建立接触国家秘密许可的可信任度审查制度，但未对可操作的建议进行具体阐述。[④] 韩慧云从科学划分审查等级、完善分级审查标准、严格确定禁止条件三个方面完善涉密人员资格审查标准体系，从明确审查主体、规范审查程序、建立审查档案三个方面健全涉密人员资格审查工作机制，对如何严格把控“入口”关进行了措施探索，但是对于该措施建议形成的因果逻辑未进行说明。[⑤] 孙琦从涉密人员定位和涉密人员资格审查两个方面介绍了美国、英国、法国、加拿大等国家的信息安全审查制度，但在程序上的介绍相对粗略，外国制度的引证资料不够详实，缺乏对中国借鉴意义的引申。[⑥] 彭志简述了美国涉密人员的三个主要类别——联邦政府、地方政府以及工业安全许可涉密人员，对美国的涉密人员安全许可程序进行了介绍，但是对美国流程主要集中于背景调查环节，对其他环节涉及较少。[⑦]

鉴于既有研究的不充分及粗疏，本文拟对该制度展开具有创新意义的研究，主要包含以下方面：一方面，立足以往研究，弥补前人对美国信息安全审查程序与制度设计介绍上详细度、完整度的不足；另一方面，着眼现实情况，基于美国公共部门与私人部门、美国公共部门与中国公共部门的安全审查比较视角，探索借鉴之处。

重要岗位及行业从业者的信息安全审查在美国公共部门和私人部门都十分普遍。

对于公共部门来说，重要岗位是指个人工作涉及国家安全、需要知悉国家涉密信息、接触关键性基础

---

① 本文对公共部门和私人部门的划分基于公共经济学定义。目前学界对于国有企业是否属于公共部门尚有争议，本文不做讨论。本文使用最为典型的政府部门作为公共部门的代表进行研究。

② Daniel Halper, “Sebelius: Obamacare Navigators Don’t Need Criminal Background Checks,” *The Weekly Standard*, November 6, 2013. https://www.weeklystandard.com/daniel-halper/sebelius-obamacare-navigators-dont-need-criminal-background-checks.

③ Richard G. Brody, Virginia L. Cox, “Background Investigations a Comparative Analysis of Background Checks and Federal, Security Clearance Investigations,” *Business Studies Journal*, 2015(1).

④ 王鸿杰：《我国接触国家秘密许可制度建立方法浅探》，《保密科学技术》2011 年第 3 期。

⑤ 韩慧云：《依法推进涉密人员资格审查》，《保密工作》2012 年第 2 期。

⑥ 孙琦：《国外涉密人员资格审查制度介绍》，《保密工作》2012 年第 2 期。

⑦ 彭志：《美国涉密人员安全许可制度简介》，《保密工作》2015 年第 7 期。

设施资产[①]、承担敏感职责、出入核心区域等等的岗位。重要岗位从业人员上岗前必须完成个人信息的一系列审查并获得安全许可通过裁决，以避免涉密信息泄露，设备资产损坏，核心区域被侵犯，危害国家利益与社会公共安全。

国家安全定义有狭义和广义之分。狭义国家安全是指以民族国家为主体、以政治安全和军事安全为主要内容、以确保国家生存为基本目标的国家安全，如美国的《分类信息程序法》（Classified Information Procedures act）；广义的国家安全从二元化向多元化外延拓展，覆盖国土、军事、经济、文化、信息、生态等多重领域，非传统安全在国家安全领域中的重要性不断凸显，如习近平总书记提出的覆盖 11 类安全的国家安全体系。总体上看，国家安全的定义正由狭义向广义发展。[②③]

国家涉密信息是依照法定程序划分的，在特定时效内对特定人群开放的涉及国家利益、安全的信息。关于国家涉密信息法定程序，各国制定了自己的划分标准和定密标识。以美国为例，美国信息保密监督办公室（Information Security Oversight Office）于 2010 年和 2014 年分别发布了第一、二版的《国家定密标识手册》（*Marking Classified National Security Information*），界定了国家安全信息的部分密级标识、整体密级标识（与整体文件内的最高部分密级一致）以及定密标识要素（如定密人员、定密理由、原始/派生[④]情况和解密指令等），将国家安全信息划分为涉密信息和未涉密信息，涉密信息按照它们对于美国公共社会安全的可能造成的危害程度分为“绝密”（Top Secret）、“机密”（Secret）、“秘密”（Confidential）三类，与之对应，安全许可也分为绝密、机密、秘密三个等级，根据《国家定密标识手册》中原始涉密信息的 8 项定密条件[⑤]，军事、外交、情报、核等涉及传统国家安全定义的行业和岗位的从业者接受信息安全审查更加普遍。[⑥]

对于私人部门而言，企业的商业秘密是由企业形成或拥有的不为公众所知悉、能为企业带来经济利益、具有实用性和潜在价值，经企业采取保密措施，一旦泄露可能使得企业的经济利益、运营安全和竞争优势遭受损害的经营信息和技术信息[⑦]。因此，涉及企业商业秘密产生、传导、管理、储存等环节的工作部门和岗位通常需要更加细致的背景调查。

二、美国公共部门信息安全许可的架构及其特征

（一）美国国家安全体系架构

美国政府国家安全部门实行“中央集权”和“部门分权”相结合的协调机制，主要包括决策、指挥、执行、咨询、监督等层面和环节。决策环节由总统直接领导下的国家安全委员会（National Security Council，简称 NSC）负责；指挥环节由国家情报主任（Director of National Intelligence，简称 DNI）负责，是总统、NSC 的首席情报顾问；执行机构由国家情报主任办公室（Office of Director Inelligence，简称 ODNI）以及下设的具体十几个部门组成，代表部门包括中央情报局（Central Intelligence Agency，简称 CIA）、联邦调查局（Federal Bureau of Investigation，简称 FBI）、国土安全部（Department of Homeland Security，简称 DHS）等；大量的咨询机构和多元监督机构共同助力组织体系的完整。

第二次世界大战以来，受冷战影响，美国在国家安全领域加快了法律体系的构建（见表 1）。

---

① 项安安：《国家安全审查制度立法的差异性及其国际协调》，《中国海洋大学学报》2018 年第 1 期。

② 任卫东：《传统国家安全观：界限、设定及其体系》，《中央社会主义学院学报》2004 年第 8 期。

③ 钟开斌：《中国国家安全体系的演进与发展：基于层次结构的分析》，《中国行政管理》2018 年第 5 期。

④ 派生定密文件是指对在已定密信息基础上的整合形成的文件，其标识与原始定密信息一致。

⑤ 根据第 13526 号行政命令《美国国家安全信息》，仅涉及以下 8 项的信息可以被标识为国家安全信息，具体包括：军事计划，武器或作战系统；外国政府信息；情报活动（包括秘密行动），情报来源及发现方法，以及秘密情报系统；美国政府的对外关系或外交活动，包括秘密来源；涉及国家安全的科学、技术以及经济事项；美国政府保护核材料及核设施的方案；与国家安全相关的系统、装置、基础设施、项目、计划或保护工作的优势或弱点；大规模杀伤性武器的开发、生产或使用。

⑥ 黄雪宜、陆明远：《美国国家定密标识的应用及其特点分析》，《保密科学技术》2018 年第 1 期。

⑦ 2010 年中国国务院颁发的《中央企业商业秘密保护暂行规定》。

表 1　第二次世界大战后美国国家主要安全立法一览表 ①

发布时间	英文名称	中文名称
1947年	National Security Act of 1947	1947年《国家安全法》
1949年	The Central Intelligence Agency Act of 1949	1949年《中央情报局法》
1959年	National Security Agency Act of 1959	1959年《国家安全局法》
1966年	Freedom of Information Act of 1966	1966年《情报自由法》
1978年	Foreign Intelligence Surveillance Act	1978年《外国情报监视法》
1980年	Intelligence Oversight Act of 1980	1980年《情报监督法》
1980年	Classified Information Procedure Act	1980年《机密信息程序法》
1982年	Intelligence Identities Protection Act	1982年《情报人员身份保护法》
1982年	Foreign Mission Act of 1982	1982年《外国使团法》
1985年	Military Espionage Punishment Act of 1982	1985年《军事间谍惩治法》
1991年	National Security Education Act of 1991	1991年《国家安全教育法》
1992年	Intelligence Organization Act of 1992	1992年《情报组织法》
1994年	Intelligence Services Act of 1994	1994年《情报法》
2001年	USA Patriot Act of 2001	2001年《美国爱国者法案》(即《美国捍卫本土安全、有效打击恐怖主义法》)
2002年	Enhanced Border Security and Visa Entry Reform Act of 2002	2002年《加强边境安全和入境签证改革法》
2002年	Homeland Security Act of 2002	2002年《国土安全法》
2002年	The Federal Information Security of 2002	2002年《联邦信息安全法》
2007年	The Protect American Act of 2007	2007年《美国保护法》
2010年	Intelligence Authorization Act for Fiscal Years 2010	2010年《情报授权法》
2015年	Cyber Security Act of 2015	2015年《美国网络安全法》

此外，一些著名的总统行政命令也丰富了美国的国家安全法律体系。

表 2　第二次世界大战后美国国家安全主要总统行政命令 ②

发布时间	中文名称	签署总统
1982年	12356号总统行政命令《美国国家安全信息》	里根
1995年	12958号总统行政命令《国家安全信息保密》	克林顿
1996年	12968号总统行政命令《接触秘密信息的规定》	克林顿
2005年	13381号总统行政命令《加强管理接触国家安全机密信息程序》	小布什
2010年	13549号总统行政命令《关于州、地区、部落和私人部门实体的国家安全信息分类计划》	奥巴马

美国联邦政府为建立健全涉密人员从业的信息安全审查程序和制度奠定了坚实的组织基础和法律保障。

（二）美国联邦政府安全许可程序

安全许可是联邦政府雇员访问涉密信息、接触设备资产、出入核心区域并担任一些敏感职责的所必须获得的前提条件。根据雇员岗位职责所需了解的涉密信息等级、敏感职责程度以及公众信任职位分类，判断雇员从业需要接受的安全许可审查等级，等级自高向低分为绝密等级安全许可、机密等级安全许可、秘密等级安全许可。各等级申请者所要求提交的背景资料涉及年限、详细程度，裁决过程的耗费以及再审等情况也有所差异。③ 高等级安全许可持有者可以行使低等级的权限。

涉密信息具备三大特征：第一，涉及到国家利益与安全问题，尤其是与外交和国防相关事项；第二，

① 倪峰：《国会与冷战后的美国安全政策》，北京：中国社会科学出版社，2004 年，第 72—164 页。

② 黄雪宜、陆明远：《美国国家定密标识的应用及其特点分析》，《保密科学技术》2018 年第 1 期。

③ Center for Development of Security Excellence, *Security Clearance Eligibility*, 2017.

非公开性，仅在一定时间内对一定人群公开；第三，涉密信息的界定由相关部门进行，未经授权的个人、组织以及所在的单位无权自行界定是否涉密以及涉密等级。根据《国家定密标识手册》规定，分为绝密、机密、秘密。

敏感职责是不局限于涉密信息的获取情况而与美国国家安全、利益高度相关的职责。美国公共部门职位根据其具体职责内容可以自高向低分为：特别敏感职位（Special Sensitive）、关键敏感职位（Critical Sensitive）、非关键敏感职位（Non-Critical Sensitive）、不敏感职位（Non-Sensitive），其中只有不敏感职位从业者不需要通过信息安全审查。以 DoD 举例，在 DoD 内，员工职位都可以划归以上类别，四种类别职位的具体职责分别如下。特别敏感职位的职责：获取敏感隔离信息（Sensitive Compartmented Information 简写为 SCI）；掌握重要或独特的情报来源、途径；知晓会对美国战略优势产生较大影响的技术、计划、程序。关键敏感职位的职责：获取绝密等级信息；需要获取公众最高程度信任；访问特殊访问程序（SAPs）；使用第一等级信息技术（IT-I）。非关键敏感职位职责：获取机密、秘密信息；需要获得公众信任；使用第二等级信息技术（IT-II）。不敏感职位的职责：其他。

公众信任职位（Public Trust Position）是指能对国家安全、社会稳定产生较大风险，对社会公众服务的效率和完整性造成极大影响的职位，通常包括以下职责:制定政策、维护社会稳定、维护公众健康、承担执法任务等。

本节基于美国联邦政府部分机构的安全许可文件、职业服务组织介绍和学者研究，总结了美国公务部门的安全许可一般性程序。

1.“需要知道”原则（need-to-know.）与安全许可的等级

“需要知道”原则包含两方面内容：一方面作为安全审查前提，指任何人都不应该仅仅因为职位等级、位置或已拥有安全许可而拥有访问涉密信息的权限，而应该由雇主组织根据该从业者工作所需要接触的涉密信息、承担的敏感职责、归属的公众信任职位类型确定从业者是否需要以及应当申请的安全许可等级；另一方面在获得安全许可后，只允许根据工作需要接触特定的涉密信息，设备资产、核心区域，禁止访问其他涉密信息、设备资产、核心区域，如安全许可权限范围内但不属于工作需要的情形。

2. 安全调查问卷

申请者须为获得雇佣部门的安全许可等级划分的联邦政府雇员或准雇员。[①] 申请首先需要填写一份 127 页的国家安全调查问卷（编号：SF-86）。人事管理办公室（Office of Personnel Management，简称 OPM ）于 2003 年启用了电子问卷调查处理系统（Electronic Questionnaires for Investigations Processing，简称 e-QIP），e-QIP 允许申请者通过安全的互联网连接、输入、编辑、提交问卷，旨在通过自动化方式检验、反馈填写不完整或格式不正确的问卷，从成本和效率的角度优化联邦调查服务部门（Federal Investigative Services，简称 FIS）[②] 的背景调查进程。

安全调查问卷通常涉及到以下领域的信息：公民身份、刑事犯罪与民事纠纷记录、教育背景、就业背景、兵役背景、社交关系（家人、朋友、邻居等）、与外国联系情况（如外国亲友）、海外定居与旅游背景、财务信用状况、心理咨询状况、非法药品史（如毒品）、酗酒史、网络安全事件（如黑客行为）以及其他具有颠覆性影响的重大活动。问卷详细程度、涉及时限根据安全许可等级有所不同，等级越高，问卷调查要求越为严谨细致；绝密等级覆盖过去 7—10 年信息，机密与秘密等级覆盖 5 年。如果存在一些负面记录（例如存在犯罪记录），审查将更为复杂。

问卷信息要求真实、完整、全面、一致、准确，否则将面对安全审查延缓或否决、罚款甚至监禁五年的判罚。完整性指覆盖时限要求内所有正面、负面以及不确定的信息，对于负面信息，可附个人情况说明。

---

① 已经收到联邦政府的书面聘用要约，并同意在收到要约日起 30 天内上任。

② OPM 下设机构。

问卷填写完成后，申请者需要签署问卷信息的隐私授权书，授权审查机构以信息安全审查为目的使用隐私信息，禁止提供给未经授权的个人、组织或活动使用。

问卷提交后，由所属部门的设备安全官员（Facility Security Officer，简称 FSO）审核，审核通过后将问卷提交至相关部门，经批准后，信息进入到调查机构[①]的背景调查阶段。

3. 背景调查

调查机构成立调查小组开展背景调查，核实信息的真实性、完整性、全面性、一致性、准确性，判断是否需要二次提交以及补充资料。补充资料通常比较常规，调查小组可以根据面试中的信息进行更新，或反馈至申请者处，由申请者自行提交补充资料。

背景小组工作如下：

首先，访问公共部门储存的的个人信息数据库，例如 FBI 犯罪信息记录，人事部的就业记录，移民局的移民记录[②]，国防部兵役记录，地方执法机关记录等。查询方式简单高效，获得个人信息授权与相关部门允许后，凭借社会安全号、ID 号、驾照号等身份识别信息便可快捷查询。美国公务部门信息安全审查尤其关注犯罪记录与海外记录。对于犯罪记录，FBI 数据库登记范围广，登记内容覆盖逮捕、羁押、起诉或其他正式的指控以及由此产生的判决结果全领域；互联共享程度高，“州际查询系统”的建立使得州际之间，地方与中央之间犯罪记录系统协调整合[③]，减少登记、储存、查询、封存等工作的冗余。对于海外记录，分散在全世界的美国安全与情报人员须及时提供海外相关信息。[④]

其次，与申请者以及申请者证明人的电话或面试沟通。按照法律规定，证明人需在某一领域了解申请者，如家人、同事、朋友、旧领导以及同样职位的其他候选人等，并对证词负责。证明人可由申请者自行推荐，而是否选择以及选择权在于调查小组。核心岗位的沟通环节设有测谎仪，根据机构和岗位差异主要分为两种测谎流程：持续时间较短的反间谍测谎和持续时间较长的生活测谎。

最后，根据背景调查情况提供详细调查报告至裁决小组。一般来说，根据调查类型和具体案例情况，调查时间从 2—9 个月不等。当申请者涉及以下情况，调查通常更为详细：高等级安全许可申请者；海外定居、就业、长期旅游记录；海外联系密切（如有海外亲友）；信息难以求证；需要补充资料等。

4. 裁决阶段

裁决小组遵守“完整人”原则（the Whole-Person Concept），审查所有的信息，并评估申请者的信息是否违反 2017 年颁布的最新《国家安全裁决指导》[⑤]（*The National Security Adjudicative Guidelines*），以向最终决定者建议申请者是否有资格获得安全许可，最终决定通常与此建议相一致。“完整人”原则是指安全许可的审查是基于提交的个人所有信息，既包括正面信息，也包括负面信息，既考虑现在信息，也考虑过去信息。裁决小组若对调查报告存疑，可以驳回，重新开始背景调查，等待新的调查报告反馈。

如果有负面信息或敏感信息引起了安全方面的关注，裁决小组根据《国家安全裁决指导》考虑减轻项，评估综合风险。如果出现严重的负面或敏感信息，该案件将被延缓或否决，延缓案件将在获得更多的有效信息后再裁决，否决案件当事人自行选择上诉，否则可能面临失去该工作或被调剂的情况。许可通过者，需要在正式工作前签署关于涉密信息的保密协议，同时接受安全教育培训，以培养政治意识、责任意识和忧患意识，掌握使用、传播、储存涉密信息、以及反间谍的程序规则。

---

① 根据 NSI 的最新安全许可简介，调查机构根据申请者部门不同，有所差异。例如国防部、FBI 可以自行调查，但是其他大多数部门的调查由 OPM 进行。

② 美国难民移民事务部，对赴美难民的安全许可审查，https://refugees.org/explore-the-issues/our-work-with-refugees/security-screening/.

③ 王跃：《系统模型与功能配置：刑事司法一体化视野下的犯罪记录制度构建》，《中国人民公安大学学报》2015 年第 2 期。

④ 王跃：《系统模型与功能配置：刑事司法一体化视野下的犯罪记录制度构建》，《中国人民公安大学学报》2015 年第 2 期。

⑤《国家安全裁决指导》涉密 13 大领域：美国忠诚度、受外国影响情况、外国偏好度、海外活动背景、个人日常行为情况、财务情况、酗酒情况、毒品情况、性行为情况、心理状态、刑事犯罪记录、涉密信息使用情况、网络安全行为。

5. 临时安全许可

雇佣组织有紧急的职位或工作需求，而安全审查尚处于裁决中或延缓裁决阶段时，雇佣组织可申请临时安全许可，裁决机构会在几周内人工审核安全问卷信息并进行初步背景调查以颁发临时安全许可，其权限与正式安全许可一致。获得临时许可后，信息安全审查通常会加速，如果在审查过程中或结束后裁定不适合拥有安全许可，则临时许可废止。

6. 定期再审查与连续评估

美国公务部门信息安全审查不是一个一次性的过程，雇员必须接受定期再审查和连续评估以维系或调整安全许可。定期再审查的间隔期均为 5 年，具体审查内容视等级以及具体情况而定。连续评估是为了弥补初始审查和再审查之间的空缺，对雇员进行不间断的监督与评估，当出现问题行为时,会被及时报告，未来，连续评估旨在建立一个自动化记录核查与监测系统，以提升监督效力。

7. 安全许可的降级、撤销、终止以及恢复

当组织员工不需要获取涉密信息时，安全许可降级或撤销；当组织员工离职时，安全许可终止。对于终止的许可不可恢复，而降级、撤销的许可在满足“需要知道”原则前提下，可在其安全审查有效期满前恢复。

（三）美国安全审查蕴含的权责统一特征[①]

美国对于信息安全审查的设置充分体现了雇佣关系双方的权责统一特征。

涉密部门雇主可以根据任职资格来招聘员工、根据岗位设置划分安全许可的等级要求、根据宏观指导健全保密规划、根据安全许可审查结果调整雇员人事安排、组织涉密培训、进行涉密监控和连续评估、实行定期再调查等，同时必须承担保障雇员有限知情权和隐私权、公众的质询权与监督权等义务。

雇员的隐私权、有限知情权、获得教育权、法定程序人等合法权利受到法律规章制度的保障，雇员必须自觉维护国家安全利益，积极配合信息安全审查程序，参与涉密信息培训，报告重大影响事件（譬如个人基本情况的改变、外国出行以及通信情况、财务信用问题、心理状况、药品使用状况、违法犯罪记录、不合理使用涉密信息、预发表审查等）对同事存在的安全隐患进行报告、帮助等。

为了减少劳资关系中因安全许可审查客观性产生的争议，美国设置了申请者的法定程序，即当申请者的安全许可申请被否决、撤销、降级时，申请者有权上诉，提供与被否决、撤销、降级决定相关的资料，对自己的负面信息进行解释说明，禁止无关资料。并且考虑该项上诉专业性强、数量庞大、影响广泛，美国诞生了专业的安全许可法定程序代理律师及事务所，以协助申请者法定程序。

三、美国公共部门安全审查实施现状及存在的问题

从国际上看，美国公共部门安全审查拥有坚实的法律制度基础、集权与分权的组织体系保障，严谨的程序设计，但是随着安全形势严峻化，美国快速扩张的安全审查建设也出现了一些问题。[②③④⑤]

（一）案件积压现象严重

根据 ODNI 发布的 2014 年和 NCSC 发布的 2015、2016、2017 年的安全许可决议报告可知，美国主要情报机构[⑥]存在着严重的安全许可案件积压现象。

统计 2013—2018 年美国联邦政府安全许可通过数见图 1。

① J. Michael Hannon, Security Clearances: Know Your Rights, FOREIGN SERVICE JOURNAL, 2005(9).

② Office of the Director of National Intelligence, 2014 Report on Security Clearance Determinations, 2015.

③ National Counterintelligence and Security Center, 2015 Annual Report on Security Clearance Determinations, 2016.

④ National Counterintelligence and Security Center, Fiscal Year 2016 Annual Report on Security Clearance Determinations, 2017.

⑤ National Counterintelligence and Security Center, Fiscal Year 2017 Annual Report on Security Clearance Determinations, 2018.

⑥ NSCS 报告的调查机构为 CIA、DIA、FBI、NGA、NRO、NSA、State（国务院）七大情报机构，ODNI 报告涉及十大情报机构，但报告中仅以数字代码表示机构，因而无法匹配数字代码与具体机构。

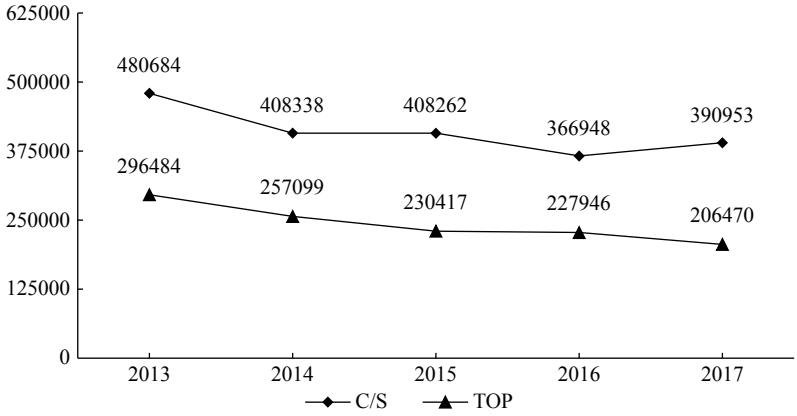

图 1　2013—2018 年美国联邦政府安全许可通过情况折线图 ①

DSCS 解释数据下降的一个重要因素是美国新实行了数据质量计划（DQI）（即在互联网后台自动限制数据格式，以提升问卷数据填写的准确性和完整性）和严格筛选计划（严格按照“需要知道”原则比对申请资格）。2015 财年报告显示，有资格申请的总人数和申请未通过的总人数都比 2014 年有着明显下降，提交信息完整度达到了 100%，意味着严格筛选计划和 DQI 发挥了重要作用。

但是这系列报告仍然明确指出，下降的通过率背后是愈发严重的积压现象，并对美国公务部门的案例积压进行了定量和定性分析。首先根据积压时间将积压案件分为 0—4 个月、4—8 个月、8—12 个月、12 个月以上案件，其次，分别统计了三个等级的对应分类情况，其中机密、绝密等级安全许可超过 4 个月的待定案件从 2014 财年的 1322 件，增加到了 2015 财年的 2526 件，增长率约为 91%，最后，报告对 12 个月以上的严重积压案例进行原因分析，“多重问题综合影响”被情报机构工作人员认为是导致 717 件（约占比 45%）案例发生严重延误的原因；“单一问题”中“外国问题”是最主要因素，国际背景多重语言从业者的安全审查需要更多的资源投入，并制定可供参考的规则，其次是“财务信用问题”，作为衡量从业者诚信度和利益风险的重要标准；此外，FBI 和 CIA 作为积压最为严重的部门，“原案件定期再审查等大量行政流程因素”造成积压的决定性因素之一，2017 年美国将秘密、机密等级的安全许可定期再审查缩短至 5 年，与绝密等级相同，使得积压现状在短期内更加难以改变。

财年报告中虽然没有对定期再审查问题进行具体说明，但从拥有安全许可雇员的实际涉密情况来看（见图 2），存在稳定数量的不符合“需要知道”原则的雇员人群，定期再审查环节必不可少。

安全审查不仅需要投入大量的人力，财力问题也不容忽视。早在 2003 年美国教育部就发现安全审查的成本负担问题，并通过结合对处理安全表格时间、背景调查时间、裁决时间等申请各环节流程平均时间的预估和美国平均薪资和福利水平的统计计算，计算出当年 8343 名现役和待定承包商雇员的审查费用约为 2777541 美元，远远超出他们的预期，因此建议部门通过密切与其他机构合作的方式降低成本。美国信息保密监督办公室（Information Security Oversight Office，简称 ICOO）在 2014—2016 财年保密工作报告中统计了 2013—2016 财年的经费开支情况（见表 2），年度保密经费开支逐年增长，增长幅度分别为 29%、8%、4.4%，其中“涉密信息系统保护和维护”一项长期居于首位，在 2014、2015 年的开支占据总开支的 50% 以上；“保密管理、监督、规划”一项在 2016 年增幅达到 73%，人员安全在这一期间相比较物理安全的增幅，以及教育培训上的花销等都可以看做美国对近年来频发的情报系统泄露、内部人员泄密事件的关注和应对。

资源紧缺导致案件积压，案件积压又产生衍生问题。第一，审查员工作压力可能引发审查的失职，使得原合格人群无法进入重要岗位工作或原不合格人群获得安全许可资格，接触到涉密信息、设备资产、核

① C/S 代表获得秘密和机密等级的安全许可通过数量，TOP 代表绝密等级的安全许可通过数量。

心区域，承担敏感职责，从而对国家安全埋下隐患。第二，新案例积压使得员工上岗存在长期等待，组织一方面需要为他支付工资，增加财政负担；另一方面岗位职责压力累积，影响组织机构正常运转和工作效率。第三，临时安全许可的潜在风险，临时许可仍然需要完成剩余审查裁决工作，没有解决资源紧缺亟待处理的矛盾，且临时许可授予者中如果出现不适宜授予许可的雇员，已经无法改变他在拥有临时许可期间已经接触到国家涉密信息事实，反而增加安全隐患。

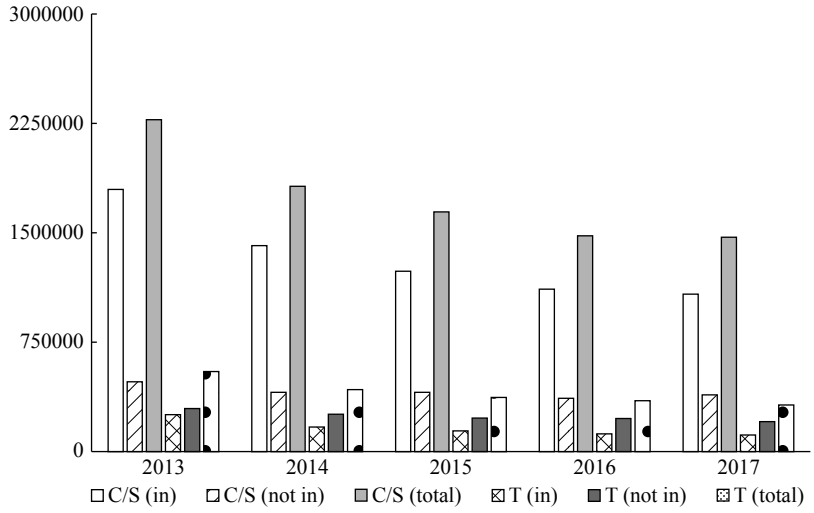

图 2　2013—2018 年美国联邦政府雇员安全许可持有者涉密情况柱状图 ①

表 3　2013—2016 年美国联邦政府保密工作经费开支表（单位：亿美元）

	2013	2014	2015	2016
涉密信息系统保护和维护	44	75.7	80.5	63.6
保密管理、监督、规划	21.7	24.2	24.7	42.7
物理安全	23.1	22	23.2	24.3
人员安全	15.2	14.9	19.5	23.8
教育培训	5.88	6.29	6.9	7.34
其他	6.42	6.71	7.1	7.16
总计	116.3	149.8	161.8	168.9

短期内，政府可以通过增加资源投入改善案件积压情况；长期来看，考虑到西方高昂的人力成本、紧张的财政负担以及培养、合格专业审查人员培养的时间与经济成本，安全许可流程以及流程实现方式的变革升级可能才是可行之路。

（二）安全审查具体计划空缺

美国公共部门安全审查是抽象和具体的结合，各组织机构在总体指导下出台具体安全审查计划，但是实际落地情况往往不尽如人意，重视程度的不足与具体案例实现方式的差异客观性使得安全审查具体计划空缺，外延性问题与抽象化困境使得具体计划的实操性不强。

申请者不清楚组织内部具体计划指导，影响申请准备，对于不合法、不正当的审查裁决过程因为缺乏上诉约束效力而轻视、忽视上诉，权利间接受损；对外合作首先需要明确内部规范，需要多方信息支持的背景调查小组受限于内部行为规范的乏力，外部合作摩擦不断，影响审查节奏；审查、裁决小组由于具体程序的空白，部分纠纷短期内难以解决；此外，国家安全体系布局受制于此，难以把控不同部门间实施审

① 各个年份柱状图从左至右（右侧图例从上至下）依次是实际涉密的机密和秘密等级安全许可持有者数量、实际未涉密的机密和秘密等级安全许可持有者数量、机密和秘密等级安全许可持有者总数、实际涉密的绝密等级安全许可持有者数量、实际未涉密的绝密等级安全许可持有者数量、绝密等级安全许可持有者总数。

查的松紧情况，构建自上而下的完整体系。

（三）其他势力介入

安全审查结果涉及到重要岗位的人员安排，利益相关者众多，政治势力可能会通过干预安全审查的方式干预部门核心人事安排，当权力“选定”从业者成功上位，容易相互勾结形成势力团体，破坏政治民主性和组织团结性；当多方政治势力均衡而局势僵持时，可能造成岗位人事安排悬而不决而职责压力过大，影响组织机构正常运转和理想职能的发挥，甚至波及其他机构和国家。因此，政治博弈而引发的安全审查公平性问题不容小觑。目前，从业者依法上诉的法定程序的实际效力不足，对权力监督制衡机制的科学改造可能是减小政治势力介入影响的有效之策，但具体方式还有待探索。

四、美国公共部门和私人部门安全审查对比

（一）程序对比

为了避免商业机密泄露或损害，私人部门通常在产生雇佣意向后，使用征信机构的征信报告获得当事人信用信息，判断是否符合其安全标准（也有少部分通过其他公共或私人的方式获得当事人的信用信息）。征信机构获取信息途径不同，提供产品与服务具有多样性，例如额外的指纹信息、信用检查以及毒品检测，对信息当事人社交媒体进行监控等。美国形成了发达的征信市场和征信监管制度，1970 年颁布了《公平信用报告法》（*Fair Credit Reporting Act*，简称 FCRA），为背景调查中的信息使用提供了强有力的法律约束，为法律规章体系的完善提供了强有力的借鉴。

在征信机构搜集、存储、使用、披露信息时，信息当事人拥有信息自主权，可以通过对征信机构全部授权或部分授权的方式允许征信机构行为，并在法律允许的范围内向第三方披露自己的私人信息。在信息使用者未授权或不知情的情况下，任何征信机构不得从事以上活动。同时，征信机构行为必须对信息当事人公开，确保其知情权。私人部门作为征信机构的信息使用者，首先，需要向征信机构提供自己的基本信息，对信息的使用目的，以及为了确保仅限该目的使用采取的程序措施和相关保证，否则若发生任何对信息当事人利益损害的事情，则由征信机构承担法律责任；反之，如果私人部门提供虚假信息、故意违反或过失违反程序规则的，则由私人部门担责。其次，私人部门需要向征信机构为使用征信产品与服务支付相关费用，征信机构会根据信息使用者对产品、服务的需求差异收取不同的费用。最后，私人部门对于信息当事人承担告知披露的义务，当使用了征信机构的征信报告但是做出不利于信息当事人或不符合信息当事人要求的决定时，必须以口头、书面或电子形式告知信息当事人该决定内容，决定缘由，征信报告和征信机构相关信息（2012 年 FCRA 的补充规定）。

公务部门同样需要遵守 FCRA，美国审计署（The United Stated Government Accountability Office，简称 GAO) 将背景调查分为四个阶段：问卷提交、调度和启动、调查、定期再审查，在这个过程中，背景调查员会约见从业者本人、证明人（同事、朋友、邻居等）。审查在书面文件中容易遗漏的关于个人性格、可信赖性和完整性的信息。公务部门调查程序通常比私人部门的调查更彻底。

（二）成本对比

成本是进行安全审查不可忽视的一项内容，公务部门需要考虑财政约束，私人部门需要考虑成本负担情况。成本通常来说难以界定，具体以直接成本和间接成本说明。

直接成本是指在安全审查流程中的花销，公务部门的直接成本主要涉及安全审查的员工数量、范围等级、方式方法以及后续的连续评估与定期再审查等，根据 GAO 发布的 2012 财年报告，OPM 进行的绝密等级安全许可底价为 4005 美元，其间再调查费用为 2711 美元；而私人部门的审查成本则与选择的征信机构、产品与服务要求相关，根据 Richard G. Brody 与 Virginia L. Cox（2015）的研究，私人部门基本审查费用为 50—150 美元，深度审查费用则是 200—500 美元不等，虽然私人部门的网络在线背景调查方式耗费极低，约 10 美元，但是由于网络在线信用报告不全面、不准确性，私人部门面临的诉讼可能性增加，所以未

全面推广使用。由此可见，公务部门的直接成本一般高于私人部门，但是具体的金额因案件而异，因此很难做出准确的估量。

间接成本是指背景调查中由于信息的误用为信息使用者增加的负担。这种间接成本来源于信息使用者审查失误而引发的诉讼成本以及信息当事人的欺诈行为（故意隐瞒、模糊说明等，违背信息真实性、完整性、全面性、一致性、准确性特征）。欺诈行为造成涉密信息、资产等的“失窃”。斯诺登的绝密等级的安全审查耗费几千美元，但是仍然窃取了大量绝密文件并泄露部分。美国《人力资源》杂志曾报道说，“每年大约有 75% 的员工会对公司进行盗窃”，员工盗窃不仅涉及财产，还包括时间。通常情况下欺诈行为可能性与安全审查成本呈现负相关，但审查成本、审查流程无法规避欺诈行为的发生，即安全审查有效性无法由成本决定。

（三）审查障碍对比

美国公共部门和私人部门的安全审查同时被信息欺诈行为、第三方势力干预、军方记录权限[①]等困扰，但又有所差异。

公共部门的安全审查障碍主要在于两方面：一方面，指导方针存在一定的指向性，容易引导倾向性信息提供与回答，尤其影响性格特征的考察；另一方面，则是时间限制、资源紧张、案例积压情况下审查人员工作压力巨大，联邦调查必须遵守 2004 年《情报改革与反恐怖主义法》（*The Intelligence Reform and Terrorism Act*）（IRTPA）中规定的时间要求，90% 的安全检查必须在 60 天内完成，其中调查环节在 40 天内完成，裁决环节在 20 天内完成，联邦政府的安全审查人员的工作强度曾被形容为“从萝卜里挤血”的程度，因此高强度、高压力下不免造成审查人员审查纰漏，甚至伪造报告。

私人部门使用征信机构的信用报告的安全审查障碍则主要是信息搜集渠道上。由于统一数据库建立复杂、管理难度大以及风险性高，目前并没有形成完整的全国信用数据库网络闭环，因此许多信息需要调查人员在州、县和直辖市的记录中进行搜索。在美国集权和分权体制下，州际之间的数据库规则并不一致，一些州为了帮助犯罪人员就业，明令禁止无条件向私人部门公布犯罪记录，或尝试在就业意向书发放后再提供。犯罪记录作为安全审查的重要组成部分，其缺失会影响征信报告的准确性、完整性，进而影响私人部门安全审查的有效性。

五、中美公共部门安全审查对比

（一）中国保密法制体系建设与政审制度

中国于 1988 年出台了《中华人民共和国保守国家秘密法》（简称《保密法》），2010 年对该法案进行了修订，新《保密法》新增了“涉密人员”为法律术语，其中第 35 条将涉密人员划分为一般涉密人员、重要涉密人员、核心涉密人员，并对涉密人员的甄选、培训、管理、监督进行了宏观抽象规定；2015 年国家保密局出台了《关于进一步加强涉密人员保密管理工作的意见》，进一步认可了“以岗定人”的原则，将涉密岗位分为了特定岗位（涉密特征明显的岗位，如涉密信息制作、传递、管理、储存岗位等）和量化定岗（工作中年产生、处理国家秘密达到一定数量的岗位）；2014 年《保密法实施条例》的出台对涉密人员管理和权益保障做出规定；此后，各个部门和地方层级也相应出台了一些规范性文件，建立了一个相对完整的涉密人员管理法律体系。但是中国的法律体系过于原则化和抽象化，尤其相对于“物”（涉密场所和涉密载体）的管理，对“人”的管理稍显不足，对审查标准、审查程序没有明确规定，因此目前对于涉密人员的甄选、政府尚没有具体的、操作性强的安全审查流程制度，政治审查（政审）还是政府主要的审查方式。

翟一帜将中国的政治审查制度历史划分为四大阶段。[②]新民主主义革命时期是政治审查的缘起和确

① 斯诺登安全审查过程中斯诺登未完成美国陆军预备役部队 5 个月服役时间这一记录如果被审查小组发现并考虑到，则会成为安全审查的重要危险信号。

② 翟一帜：《“政治审查”的历史演进考察》，《理论探索》2017 年第 2 期。

立，毛泽东在 1939 年《共产党人》发刊词中提出政治审查在党的建设上的重要地位，要在维护党组织纯洁性的前提条件下吸收党员，这一阶段确立了个人档案制度。中华人民共和国成立后至“文革”前是政治审查的广泛拓展时期，政治审查从党组织建设方式拓展到教育招生、企业招工、军队征兵等生活领域。“文革”期间，政治审查“唯成分论”，使得社会阶层固化，对国家政治、经济、文化发展产生负面影响。改革开放时期是政治审查的纠偏与发展，内容侧重点不再“唯成分论”，政治审查从许多领域中退出，聚焦在国家征兵和招聘政府公务人员的重要考核方式。

政治审查的基本流程主要分为：申请者确认自己通过基本筛选进入政审环节，自己填写政审表格汇报自己的思想政治、学习生活、家庭成员、社会关系、奖励惩处等，审查小组对申请者组织审查（通常由人事部门或组织部门组建两人以上的审查小组，对申请者基本情况查询相关档案、对申请者的同学或同事、老师或领导进行访谈以了解申请者的实际情况和他人评价，查询申请者的违法犯罪记录以及海外关系记录等），审查小组根据审查情况制定审查报告提出审查意见，由考核工作班子决定最终结果。

（二）中美对比视角下中国政审特征

中国政治审查和美国联邦政府安全许可审查相比，具有以下明显特征。

政审对象范围广泛，针对性差。政审对象不仅仅局限在需要知悉国家（组织）涉密信息、接触重要设备资产、出入核心区域、承担敏感职责，而是成为所有政府部门、事业单位、国有企业从业者上岗前一项基本环节。受限于政审对象的广泛，政审很难制定有涉密岗位针对性的程序环节。

政审内容狭窄，手段单一。美国公共部门从法律规章、组织体系到程序设计，包括 127 页安全问卷在内的多重审查工具，对个人的忠诚、品格、诚信和可靠性进行全方位考察，以确保从业者有资格获得国家涉密信息。我国政审的内容主要是政治审查和犯罪记录审查，对于从业者的信用情况、财务情况、生活习惯情况、海外关系情况等关注较少，审查手段依赖于访谈和档案查询。访谈有效性差：对政审对象相关其他人员的访谈具有引导性，且接受访谈人员受中国传统文化与社会风气的影响，大多回答中庸或者避开负面评价，作为第三方证明的真实性较低。档案查询中核心记录——犯罪记录具有查询对象封闭性和查询结果否决连带性，犯罪记录查询方式封闭性是指，虽然公安局建立了全国统一犯罪记录信息查询系统，但是仅对有办案需要的国家机关、需要查询本案犯罪嫌疑人或被告人犯罪记录的辩护律师、有必需目的的普通公民开放，且需要向公安机关申请，并获得审批，而材料准备、是否审批、审批速度则因案件具体情况而异，金钱、关系因素可能干预其中；犯罪记录查询结果否决连带性是指，犯罪记录不仅影响本人政审结果、还会影响部分亲属，如公务员政审明令禁止录用因犯罪受过刑事处罚的人员、直系亲属以及对成长过程有重大影响的旁系亲属存在严重刑事犯罪记录的人员，而涉密岗位的则更为严苛。

政治审查程序延续性弱。延续性弱体现在三个方面：首先，与美国的连续评估和定期再审查相比，中国政审具有一次性特征，当准从业者政审通过后，一般不会对其进行后续的审查，但是存在部分涉密人员是在入职之后的“叛变”问题，因而动态性审查不足导致安全风险大大增加；其次，许多审查仅限于工作时间，对于工作之外的社交活动并没有实行有效监督；最后，政审的一次性特征使得对于申请者的权益保护有待加强，美国用法定程序保障申请者对审查结果的监督权，而中国政审结果通常难以被质询、改变。

总体上来看，中国政审对象范围广，程序针对性差，内容狭窄手段单一，延续性还有待加强，无法成为涉密人员安全审查的有效方式，亟待出台新的安全审查程序规则来加强对国家涉密信息、重要设备资产、核心区域的保护，减少国家安全、社会稳定的潜在风险。

六、中国特色政审制度的完善建议

在复杂多变的国家环境下，中国的国家安全和国家利益受到日益严峻的威胁，美国联邦政府公共行政管理领域安全保障体系完善，在信息安全审查程序与制度设计方面拥有丰富的历史经验并特点突出，是中国探索有中国特色政审制度的有益借鉴。

（1）搭建自中央到地方的完整体系。法规建设搭建安全审查的基本框架和程序范式，各地方各部门在

宏观指导下根据具体情况规划各自的安全审查规则，进行从业人员的人事安排，健全宏观法规和具体安全审查计划相结合的制度支撑。

（2）重视安全审查程序的创新设计和程序实施的严谨性、科学性。传统政审方式过于依赖档案记录和访谈，但档案记录只涉及重大事项和人生经历，信息覆盖全面性不足，访谈的客观性、真实性、有效性有待加强，尤其对访谈对象的权利保护和责任明晰，访谈过程与访谈技巧的专业性，访谈内容的保密性。因此需要改进、创新程序设计和程序实施方式，进一步提升审查对象信息的真实性、完整性、全面性、一致性、准确性。

（3）加强安全审查的延伸性。由于单次审查难以规避不足，以及内外部环境变化可能引发关键改变，初次安全审查效力不能视为永久效力。定期再审查和连续评估可以弥补初次安全审查的不足，尤其对于高级别安全许可拥有者工作时间和非工作时间重大活动的监督，可以有效规避泄密风险。

（4）重视从业者基本权利的保护。美国公务部门注重雇佣双方的权责统一，保护安全审查对象的隐私权、有限知情权、获得教育权，并设置申请者法定程序巩固审查的公正性，针对法定程序环节形成了专业律师市场，中国在设计相关制度、程序时也需要立足公民的基本权利界定从业者合法权利。

（5）设计科学的安全审查工作人员绩效考核指标和绩效管理体系。美国公共部门资源紧张，审查人员在高强度、高压力背景下难免纰漏。中国对涉密岗位安全审查正处于初步建设阶段，在严谨化的程序构想下，安全审查人员如何避免环境作用下的“失职”需要重视。首先，是安全审查专业人员的培养，私人部门将员工上岗前普通背景调查工作归为人力部门的重要职责，而安全审查工作相较于普通背景调查更加强调专业性，因此，需要重视安全审查专业人员的培养。绩效考核与管理系统的建立一方面有助于检验人员的专业素质的培养效果，另一方面，通过绩效管理多环节避免审查人员工作过量，提升每个案例审查的有效性。

（6）提升安全审查小组的独立性和客观性。严肃对待小组人员组成，严格小组文化纪律建设，明确权力来源，监督权力使用。

（责任编辑：王胜强）

The Information Security Clearance System in America and Its Inspiration

TU Yongqian, LUO Ziyue, HU Xiafeng

Abstract: Information security clearance has become a significant process to safeguard classified national security information and/or occupy a national security sensitive position. The United States Federal Government has a excellent security system with historical experience and prominent characteristics in both procedure and system, such as strict clearance procedure and an integration of rights and responsibilities. This article makes an in-depth introduction of the security clearance of the public sector in America and compares it with which in the private sector and with Chinese political censor, revealing some obvious deficiencies of the censor in target definition, procedure effectiveness, content comprehensiveness, manner diversity and system continuity. With the useful experience of the United States in the field of information security clearance, we need to reform our political censor system and explore a security clearance system with Chinese characteristics.

Key words: security clearance, organization security, sensitive position, political censor