美国《改善国家网络安全的行政命令》执行情况分析及启示

张烨阳[1]，刘 蔚[1]，方 时[2]
（1. 中国科学技术信息研究所，北京 100038；
2. 北京大学，北京 100091）

摘 要： 2021 年太阳风供应链攻击（SolarWinds）事件曝光后，美国拜登政府发布的《改善国家网络安全的行政命令》，概述了美国联邦政府机构为提高其机构网络安全能力而需要采取的 55 项行动。此后，美国拜登政府根据其发布对美国网络安全相关领域具有重要影响的一系列重要文件，引起了美国联邦政府网络安全格局的重大变化。从该行政命令出台的背景出发，分析了其执行进展，对依照行政命令出台的重要政策、采取的重要措施做出了解读，总结了行政命令执行过程中存在的问题，最后提出了对中国信息安全领域的借鉴意义。

关键词： 网络安全；SolarWinds；行政命令；零信任架构；供应链安全
中图分类号： TN915.08 **文献标识码：** A DOI：10.3772/j.issn.1009-8623.2023.01.011

2020 年 12 月美国联邦调查局（FBI）、美国国家情报局局长办公室（ODNI）和美国国土安全部网络安全与基础设施安全局（CISA）联合发布声明，首次正式确认被黑客植入木马的 SolarWinds 软件造成多个美国联邦政府机构的网络遭受入侵。针对该事件的风险，美国国土安全部网络安全与基础设施安全局以“超出了容忍极限”的罕见字眼在官方通报中予以通告。为应对太阳风供应链攻击（SolarWinds）事件，以及后期发生的科洛尼尔输油攻击（Colonial Pipeline）事件等备受瞩目的网络攻击事件，美国总统拜登于 2021 年 5 月 12 日签署了《改善国家网络安全的行政命令》（Executive Order on Improving the Nation's Cybersecurity，以下简称《行政命令》）。这是美国当前在网络安全方面最详细的行政命令之一，概述了美国联邦政府机构为提高其机构网络安全能力而需要采取的 55 项行动。这些行动包括修订《联邦采购条例》（FAR）、为关键软件设计和使用制定标准、淘汰不符合安全标准的软件产品和平台，以及加快基于零信任架构的云技术应用等措施。该行政命令在提升美国文职机构网络安全的同时，旨在利用美国政府（全球最大的商品和服务单一购买者）的购买力，迫使美国软件产业提升其产品安全性，从而进一步引领整个美国信息产业向更高的安全标准迈进。《行政命令》发布之后，美国拜登政府根据其采取了多项举措，包括更新《联邦采购条例》，发布了“关键软件”定义指南，以及《软件物料清单（SBOM）最低要素白皮书》《安全软件开发框架》《推动美国政府走向零信任网络安全原则》[1] 等一系列重要文件，引起了美国联邦政府网络安全格局的重大变化。

自 2021 年美国遭受 SolarWinds 事件、Colonial Pipeline 事件、微软 Exchange 服务器攻击事件等多起网络攻击事件后，美国国防部（DOD）2022 财年追加了网络安全方面的预算，并自 2012 年以来首

第一作者简介： 张烨阳（1984—），男，硕士，工程师，主要研究方向为网络及网络安全。
收稿日期： 2022-11-27

次计划大幅增加其网络任务部队人员数量。这些部队人员一方面是防御性质的网络保护团队，另一方面是执行网络攻击以及为攻击行为提供情报收集、任务规划的团队。2021年国际战略研究所（IISS）的一份新报告称，美国是世界上唯一的一级网络强国，进攻性网络作战能力可能比任何其他国家都发达[2]。目前这支世界上网络作战能力最强的部队已将其矛头指向了中国。

本文拟从《行政命令》自2021年以来的执行情况出发，对美国相关机构落实该行政命令的进展进行研究，并对其理念、采取的措施及存在的问题进行深入分析，从而为中国网络安全技术发展路线及相关政策制定提供参考建议。

1　《行政命令》执行进展分析

《行政命令》从更新《联邦采购条例》、构建现代化的联邦文职机构网络安全体系、提升联邦政府软件安全性和建立网络安全审查委员会4个方面着手，加强美国联邦政府的网络安全。

1.1　更新《联邦采购条例》

《联邦采购条例》是美国联邦政府机构在使用财政拨款采购供应品和服务时遵循的主要法规，同时还包含采购所需的标准招标条款和合同条款，通常由美国国防部、美国总务署（GSA）和美国国家航空航天局（NASA）联合发布[3]。

为解决在SolarWinds事件中运营商与政府部门受合同条款约束、信息沟通不畅的问题，破除两者之间的信息共享障碍，提升美国联邦政府软件采购安全标准。《行政命令》一方面要求美国行政管理和预算局（OMB）及其他相关机构协商，在60天内向联邦采购监管委员会（FAR委员会）推荐关于网络事件报告和相关信息保存的合同条款。要求在该命令发布之日起60天内，美国行政管理和预算局主任应与国防部部长、司法部部长、国土安全部（DHS）部长和国家情报局局长协商，审查《联邦采购条例》和《国防联邦采购条例补编》中关于与信息技术（IT）和操作技术（OT）服务供应商签订合同的要求和条款，并向FAR委员会和其他适当机构建议更新这些要求和条款。另一方面要求在《行政命令》发布一年之内，美国国土安全部部长应与国防部部长、司法部部长、行政管理和预算局局长和电子政务办公室主任协商向FAR委员会提供合同语言方面的建议。

《行政命令》颁布后，在解决网络威胁事件报告与信息共享方面，美国FAR委员会开启了联邦采购条例编号为2021-017的案例，以制定合同语言和相关要求，并据此拟议FAR修正案。该案例涉及的拟议草案于2022年2月发布，并于2022年4月完成了向利益相关方及公众公开征求意见。2022年5月6日，FAR委员会的一个分支机构——美国国防采购条例委员会（DARC）同意了拟议的FAR规则草案。目前正由FAR下属的信息和监管事务办公室进行审查和批准。在拟议反映“关键软件”指南要求的合同条款方面，美国国家标准与技术研究院（NIST）于2022年2月发布了安全软件开发框架（SSDF），该框架将《行政命令》中对于增强关键软件供应链安全性的要求转化为具体安全实践的指南。随着安全软件开发框架的发布，美国国土安全部将向FAR委员会推荐涵盖框架指南内容的合同条款。

按照《行政命令》的规划，对于《联邦采购条例》的修改工作应在2022年5月12日前完成，但截至2022年10月，针对《联邦采购条例》的修订仍未完成。

1.2　构建现代化的联邦文职机构网络安全体系

为了弥补美国在SolarWinds事件及Colonial Pipeline事件等网络攻击事件中暴露出的网络安全短板，构建可应对新型威胁的网络安全体系，《行政命令》在推广基于零信任的云服务架构应用、加强网络威胁检测及处置工作、提高网络事件调查和补救能力方面给出了一系列指令，旨在改善美国联邦政府系统的网络安全态势。

根据《行政命令》的要求，在推广基于零信任的云服务构架方面，2021年6月，美国国土安全部网络安全与基础设施安全局根据《行政命令》发布了“零信任成熟度模型”，作为联邦政府向零信任架构过渡的路线图；同时为了指导美国联邦政府机构将现有系统向云端迁移，于2021年9月与相关机构合作发布了云安全技术参考架构指南（TRA）[4]。2022年1月26日，美国行政管理和预算局根据《行政命令》的要求于发布了《推动美国政府走向零信任网络安全原则》，阐述了美国联邦零信任架构

（ZTA）战略，提出各联邦政府机构2024财年在零信任技术应用方面应达到特定的标准和目标[1]。

在加强网络威胁检测及处置工作方面，2021年10月8日，美国行政管理和预算局根据《行政命令》向美国联邦各机构负责人发布了一份备忘录，就端点检测和响应（EDR）解决方案的实施提供了指导，详细说明了各机构在特定时间必须达到的目标[5]。2021年11月16日，美国国土安全部网络安全与基础设施安全局根据《行政命令》的要求发布了《网络安全事件和漏洞响应手册》（Cybersecurity Incident & Vulnerability Response Playbooks），旨在为美国联邦政府各机构应对网络安全事件建立标准的方案，确保采取统一的流程应对威胁，从而提升牵头机构全面分析安全事件的调查能力[6]。

在提高网络事件调查和补救能力方面，美国行政管理和预算局根据《行政命令》发布了《提高联邦政府网络安全事件的调查和补救能力》的备忘录，为美国联邦各机构建立了事件日志管理成熟度模型，对系统日志的记录、保留、管理提出了要求。

1.3 提升美国联邦政府软件安全性

在SolarWinds事件发生后，美国联邦政府意识到其软件供应链中存在严重的安全隐患，相关机构在获取、部署、使用软件方面面临网络安全风险，《行政命令》概述了一系列相关行动，主要围绕增强软件供应链安全和消费者标签计划两个方面开展。

在增强软件供应链安全方面，2021年7月，美国国家标准与技术研究院根据《行政命令》的要求发布了《关键软件安全使用指南》，对操作、部署关键软件的环境提出了要求，同时还发布了《软件供应商验证测试最低标准指南》。美国商务部发布了《软件物料清单（SBOM）的最低要素白皮书》，概述了软件物料清单应具备的内容。2022年2月，美国国家标准与技术研究院根据《行政命令》的要求发布了更新的《安全软件开发框架》，详细说明了安全软件开发最佳实践[7]。2022年3月，美国行政管理和预算局发布《根据行政命令（EO）14028第4（k）节实施软件供应链安全指南》，其中要求联邦政府机构开始将美国国家标准与技术研究院的软件供应链安全指南纳入软件维护和采购[8]。

在消费者标签计划方面，2021年8月，美国国家标准与技术研究院根据《行政命令》的要求发布了一份白皮书，就《物联网（IoT）设备安全能力标签计划草案》征求公众意见。2021年10月，再次就《消费者软件网络安全和标签标准草案》征求公众意见，并于2021年12月发布了修订后的文件草案。2022年2月4日，最终发布了《消费者物联网（IoT）产品网络安全标签的推荐标准》[9]和《消费者软件网络安全标签的推荐标准》[10]。

上述大部分工作未能按照《行政命令》的要求在2022年5月12日前完成，截至2022年10月大部分工作都已完成。尚未完成的部分包括对《联邦采购条例》进行修订，要求软件供应商向采购方提供已遵守《行政命令》相关安全要求的证明，以及根据《行政命令》的要求，在《联邦采购条例》完成最终修订后，删除采购清单中不符合要求的软件产品。

1.4 建立网络安全审查委员会（CSRB）

《行政命令》要求建立网络安全审查委员会，旨在审查重大网络事件发生之后的威胁活动、漏洞、缓解措施和机构响应措施。2022年2月3日，美国国土安全部成立网络安全审查委员会，成员由联邦政府公共权力部门官员和私营企业负责人组成。目前该委员会的首要任务聚焦于广泛存在的Log4shell漏洞①，包括对Log4j漏洞进行审查和评估，为解决漏洞和相关安全威胁、改进网络安全和事件响应提供建议。

2 重点政策及措施的制定思路分析

为了提升美国整体网络安全水平，根据《行政命令》，美国联邦政府采取了多项行动弥补近期安全事件中暴露的问题，本文从以下4个方面对此进行分析：

2.1 重视将所有利益相关者纳入政策及指导文件的制定过程

美国联邦政府认为在网络安全相关政策及指导文件的制定过程中，应重视听取其他机构和行业的利益相关者的意见。通过聚合分散的知识和相关信息，可以及早发现潜在的问题，并更好地制定政

① Log4shell是日志记录工具Log4j中的一个远程代码执行漏洞，允许攻击者在目标系统上安装恶意软件或勒索软件，该漏洞影响范围涉及全球数百万台在线运行的服务器。

策以建立有效的风险管理框架。美国联邦政府多个机构在制定政策及指导文件的过程中已采取了类似的做法。例如，美国国家标准与技术研究院在制定《系统和组织网络安全供应链风险管理实践》《安全软件开发框架》《消费者软件网络安全标签的推荐标准》时，采取召开研讨会、发布政策草案征询公众意见、直接与各类组织员工开展定期对话等多种方式，与来自政府组织、公司、行业协会、消费者协会、学术界的多方代表进行了广泛接触，涉及美国国内外的数百个组织、机构和个人。

2.2　使用新兴技术将网络安全政策从合规性转向安全性

《行政命令》的实施将美国的网络防御态势在终端检测与响应系统、零信任架构等新兴技术的配合下，从主要以合规驱动安全的角度转变为基于实际风险来考量安全的角度。根据以往经验，政府主要关注预防措施和合规性。这种向“破坏假定”思维方式转变的策略对于网络安全政策的成熟至关重要。鉴于目前的网络安全态势，美国应对威胁的预防措施存在一定的不足，《行政命令》拟将网络威胁作为管理对象，在美国联邦政府各机构关键系统全生命周期都假设威胁的存在并对其进行闭环管理，并在此基础上通过端点检测与响应系统、零信任架构等技术措施对系统进行持续的监控和检测，限制攻击者入侵，增强系统的安全弹性，防止灾难性后果的产生。如果美国联邦政府各机构通过一两年时间的努力，达到《行政命令》要求的安全标准，将显著提升其网络安全性。

2.3　注重零信任架构的推广与使用

在 SolarWinds 事件后，美国联邦政府将零信任视为实现网络现代化和加强政府网络防御能力的关键要素。在零信任政策方面，与 2022 年中国发布的《信息安全技术　零信任参考体系架构》以及 2021 年发布的《零信任系统技术规范》相比，美国的零信任架构战略在要求上更加丰富、清晰，例如，在通信加密方面，中国的《零信任系统技术规范》只要求控制通道和数据通道对数据传输进行加密，而美国的零信任架构战略在 DNS 流量加密、HTTP 流量加密、代理系统内部流量加密、电子邮件加密、云存储中敏感数据加密、日志加密、密钥管理等多个方面做出了详细的要求。

2.4　注重供应链安全政策的系统性

《行政命令》承认美国联邦政府通过其供应链获取并部署的软件存在网络安全风险，为了降低供应链风险，美国国家标准与技术研究院按照《行政命令》第 3 节的要求发布了一系列文件，包括指导机构从整体出发，在组织各个层面提供识别、评估和减轻供应链网络安全风险的《系统和组织网络安全供应链风险管理实践》；从软件生产者角度出发，降低软件全生命周期漏洞风险的安全软件开发框架；从机构采购者角度出发，指导美国联邦政府机构如何采购符合安全软件开发标准产品的《在行政命令 EO 140284e 节要求下的软件供应链安全指南》[11]（以下简称《指南》）；从普通消费者角度出发，提升消费者辨别物联网设备及软件网络安全性的《消费者物联网（IoT）产品网络安全标签的推荐标准》和《消费者软件网络安全标签的推荐标准》。这些文件涵盖了供应链安全的各个方面，不仅体现了美国联邦政府对供应链安全问题的重视，还展现了其为解决网络安全问题制定政策的系统性和全面性。

3　存在问题的分析

针对美国联邦政府机构存在的网络安全问题，《行政命令》采取了多方面的举措，力图在短期内大幅提高美国联邦政府机构网络安全水平，但部分网络安全问题涉及历史沿革、深层利益矛盾等无法在短时间内解决，因此，《行政命令》在执行过程中存在一些问题，以下就此进行分析。

3.1　在网络安全信息共享方面，难以取得供应商的信任

公私网络安全合作在美国历史上并非第一次出现，2003 年，美国发布《国家网络空间安全战略》（NSSC），该战略呼吁建立“公私合作伙伴关系”[12]。2015 年，奥巴马总统签署了《促进私营部门网络安全信息共享行政命令》，鼓励政府和私营企业之间共享信息[13]。2020 年，特朗普总统签署了《关于加强联邦政府网络和关键基础设施网络安全的行政命令》，呼吁关键基础设施行业与政府在网络安全信息方面进行数据共享[14]。但最终受到美国各州用户数据隐私和法律的影响，未能在国家层面形成强制的网络安全事件报告制度。此外，

与美国国土安全部、联邦调查局或国防部进行网络风险和违规信息共享的公司有可能成为政府调查的对象、原告诉讼的目标以及负面媒体报道的受害者。《行政命令》虽继续要求私营企业与政府自由、公开地共享网络事件数据，其中部分数据有可能涉及违规行为，但拜登政府对此没有提供免于法律责任的保护以及互惠信息共享的方式，只是呼吁为信息共享“消除合同障碍”，要求私营企业进行单向信息共享，并未规定实践中如何运作。且上述行为并不等同于真正的合作伙伴关系，因此难以取得很大的实效。

3.2 在供应链安全方面，部分内容尚存争议

3.2.1 由供应商自证安全的措施实施效果尚不确定

《行政命令》和美国国家标准与技术研究院制定的《指南》对美国联邦政府软件供应商（以下简称“软件供应商”）的生产、制造设定了一个较高的标准，同时在验证供应商符合安全软件开发框架实践要求方面，建议采用第一方证明，除非在基于网络安全风险的考虑下才需要第二方证明和第三方证明。这表明当软件供应商表示他们已经满足安全软件开发框架和其他指南的要求时，美国联邦政府作为软件购买者被敦促相信软件供应商“信守承诺”。这一做法在软件供应商刚开始接受安全软件开发框架、软件材料清单的概念时是积极有效的，可以促进相关安全措施的实施。但后期随着软件供应链威胁复杂性的提高和出于软件供应商自身利益的考量，这种做法的有效性有待确定。

3.2.2 供应链安全指南执行范围有限

2022 年 4 月，美国国家标准与技术研究院发布的《指南》中提到联邦机构开发的软件、使用的开源软件或者直接被联邦机构使用的软件，不在该文件指导范围内，即《行政命令》关于供应链安全的一系列安全措施只适用由软件供应商向美国联邦政府提供的软件。与此同时，美国联邦政府内部包括其关键基础设施上部署了大量使用开源代码、商业软件、商业开发工具自行开发的软件。如不将代码审查、开发环境保护、漏洞扫描等措施应用到此类软件中，将影响美国联邦政府的网络安全。

3.2.3 软件供应商是否愿意提供软件物料清单

要求美国联邦政府软件供应商在销售产品时提供软件物料清单是《行政命令》的一项重要举措，被美国国土安全部网络安全与基础设施安全局视为增强软件构成透明度、衡量组织软件产品安全制造能力的重要工具。对于开源软件供应链来说，较易实现软件组件及供应链透明度。但对于顶级闭源供应商来说，一方面希望保持其代码的专有权，另一方面不希望暴露其软件中的缺陷。目前已经有一些美国联邦政府主要软件供应商反对提供软件物料清单的措施，担心其知识产权受到侵犯。美国联邦政府需要出台更有力的政策才能说服闭源软件供应商支持此项措施。

3.3 在构建现代化网络安全体系方面，零信任技术的应用仍存挑战

目前美国联邦政府内还有大量使用时间较长的应用程序，在技术方面，这些应用程序一方面由于开发年代久远，维护工作已经停止。在美国政府问责署 2021 年发布的《政府机构需制定和实施关键遗留系统的现代化计划》中指出，联邦政府内部分遗留系统为联邦重要业务提供了关键支撑，其中使用时间最长的系统已达 51 年，其开发语言大多较为老旧，并且很多都存在已知且难以修补的漏洞。另一方面部分遗留程序并不具备现代化安全改造的条件，例如，部分程序对外接口在设计之初未提供任何类型的多因素认证支持，仍然需要终端仿真器和类似 Telnet、SSH、FTP、T27 等原始网络协议才能连接，只支持用户 ID 和密码的验证方式。在现代化改造所需的资金方面，该报告指出，美国联邦政府每年在互联网技术和网络方面的投资支出超过 1 000 亿美元，但 80% 的经费用于遗留系统的运营和维护，且这部分费用受缺乏传统编程语言技能人员的影响，随着时间推移有持续增长的趋势。在网络安全人力资源方面，2022 年美国网络安全公司 Trellix 对 900 名来自美国联邦政府、大型公司的网络安全专业人员进行了问卷调查，形成了一份《网络安全成熟度的调查报告》（以下简称《调查报告》），调查结果表明，尽管在当前的网络安全威胁形势下，大部分公司都有在网络安全建设方面投资的意愿，但网络安全人才的缺乏正在减缓现代化网络防御技术的实施进度，这项因素被认为是在实施网络现代化方面最常见的挑战。

4　对中国的经验借鉴

《行政命令》为解决 2021 年以 SolarWinds 事件为代表的多起网络安全事件所揭示的问题，在网络安全信息共享、加强供应链安全、推广零信任技术架构等方面采取了多项措施，这些措施在提升美国联邦政府网络安全性的同时也暴露出一些新的问题，对中国信息安全领域的工作有着借鉴意义。

（1）加快网络安全法规建设步伐，让网络安全工作由合规性向安全性转变。

在网络安全法规方面，面临日趋严峻的网络安全态势，中国先后出台了《信息安全技术网络安全等级保护基本要求》《国家电子政务标准体系建设指南》等相关政策标准，在合规性方面对信息系统做出了要求。2016 年中国颁布的《中华人民共和国网络安全法》，把网络安全提升到国家安全的高度，将网络安全由合规性驱动过渡到合规性和强制性驱动并重。

但现行的管理规定更侧重于被管理的信息系统在安全方面是否达标，并未过多地强调围绕信息系统网络安全开展持续的闭环管理。下一步中国应根据新的网络安全态势，将网络安全的要求由合规性、强制性向安全性转变，现有的网络安全防护措施无法应对未来新型的网络攻击，应将网络威胁作为管理对象，在信息系统全生命周期都假设威胁的存在，通过对信息系统、网络的持续监控发现网络威胁入侵的线索，利用零信任架构相关技术，增强信息系统安全弹性，防止灾难性后果的产生。这一切的实现都需要顶层设计与规划，制定或修订相应法规，要求中国重要基础信息系统的建设方、运维方在系统开发、测试、运行维护各个阶段将信息系统安全作为管理目标，适应不断变化的威胁环境，确保信息系统全生命周期的安全。

（2）政府主导，统一网络安全相关标准。

目前中国的网络安全一般会受到各级主管单位、公安部门和其他相关单位的共同管辖，当发生网络安全事件时，同一事件要按照不同的口径填报多份材料提交给相关部门，在处置网络安全事件方面缺乏统一的处置标准、流程。由于缺乏统一的网络安全信息报送标准、网络安全事件处置标准，在应对大规模网络攻击时，会影响上级决策部门对于事态的掌握，延缓事件处理进度，同时由于缺乏对相关系统运行信息的日常收集，难以做到对网络攻击事件的提前发现与预防。

建议中国在政府相关部门的主导下，建立政府、市场统一的网络安全相关标准，尽量减少由此带来的各种成本，使其更容易被各方所接受。在网络安全信息收集方面，要求关键基础设施的运营者必须采用自动化的方式，按照一定的标准及时间间隔向相关部门报送系统运行关键信息，由相关部门对信息进行分析及保存，争取做到对网络攻击事件的提前发现，当攻击事件发生后，也能通过本地留存的信息第一时间对其进行分析，同时相关部门在发现网络安全威胁时也要向关键基础设施运营者通报，形成良好的双向互动机制。在网络安全事件处置方面，要对信息安全处置流程进行标准化，使决策部门在应对大规模网络攻击时，能清晰掌握各单位处理网络安全事件的进度，进而更好地协调资源。在网络安全标准制定方面，相关政府部门应切实履行职责，承担起零信任技术标准、供应链安全相关标准的牵头制定工作，在此基础上广泛纳入各利益相关方，听取各行业代表的意见，制定切实可行的网络安全标准。避免相关标准由企业主导的现象，确保其客观性和公益性。

（3）制定中国零信任战略，逐步推进零信任技术应用。

《调查报告》表明，目前 29% 的美国关键基础设施提供商以及 40% 的美国政府机构已经在其系统中完全实施了零信任解决方案，而中国在这方面的进展相对缓慢。目前在中国大部分单位内部主管网络安全、系统开发的部门话语权较弱，而在零信任架构的实施过程中必然涉及对各单位现有业务信息系统的改造，需要单位内主管业务、网络安全、软件开发的相关部门密切配合，仅靠网络安全部门推动难以实现。为了积极推动零信任相关工作，中国应尽快制定零信任战略，改善关键基础系统的网络安全。

（4）依托政府采购市场，提升中国软件供应链安全。

目前在大多数软件的开发过程中，为了提升开发效率、降低成本，往往以功能的实现为目标导向，在开发过程中缺乏对供应链安全的管理。为此建议

中国制定关键基础设施软件标准，在项目管理层面要求软件产品供应商以安全为核心，组建安全风险框架，设定安全基线，对安全风险进行评估、应对、监控，对开源软件组件进行审查，建立开源组件可重用库。在具体开发层面，要求软件供应商将软件安全开发的最佳实践嵌入软件全生命周期的各个环节，通过维护安全的软件开发环境、建立软件发布完整性的验证机制、重用已有的安全代码模块、让开发人员在创建源代码时遵守安全编码实践等措施减少软件中的漏洞数量，消除潜在隐患。

上述措施的实施必然会带来开发成本的上升，为了提升软件供应商遵从相关安全标准的积极性，应要求进入关键基础设施软件采购名录或政府采购名录的软件必须符合这一标准。同时，在国家层面实施安全软件标识计划，对符合相关安全标准的软件予以标识，让机构及消费者在采购时可以对软件的安全性进行评估。借助政府和市场的力量，带动中国软件安全性全面提升。

（5）积极培养新形势下的网络安全人才。

随着零信任架构中各种安全技术的应用，网络安全要求系统业务模块与安全组件在应用层进行深度融合，对于网络安全人才的要求将侧重于安全开发能力。因此，社会各方面对同时掌握开发技术及网络安全知识的人才需求会明显增加。《调查报告》表明，100% 的政府背景受访者和 91% 的关键基础设施运营者表示，缺乏具备相应网络安全技能的员工，这是实施新型网络安全技术最大的阻碍。中国应提前布局，在大学开设相关专业，积极培养产业需求的网络安全人才，满足社会对于专业人才的需求。■

参考文献：

[1] Office of Management and Budget. Moving the U.S. government toward zero trust cybersecurity principles[EB/OL]. (2022-01-26)[2022-06-10]. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[2] International Institute for Strategic Studies. Cyber Capabilities and National Power: a net assessment[EB/OL]. (2021-06-28) [2022-06-10]. https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.

[3] U.S. General Services Administration. Federal acquisition regulation[EB/OL]. (2022-09-02)[2022-10-10]. https://www.gsa.gov/policy-regulations/regulations/federal-acquisition-regulation-far.

[4] Cybersecurity & Infrastructure Security Agency. Cloud security technical reference architecture[EB/OL]. (2021-09)[2022-06-05]. https://www.cisa.gov/cloud-security-technical-reference-architecture.

[5] Office of Management and Budget. Improving detection of cybersecurity vulnerabilities and incidents on federal government systems through endpoint detection and response[EB/OL]. (2021-10-08)[2022-07-09]. https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

[6] Cybersecurity & Infrastructure Security Agency. Cybersecurity incident & vulnerability response playbooks[EB/OL]. [2022-08-13]. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

[7] National Institute of Standards and Technology. Secure software development framework (SSDF) version 1.1[EB/OL]. [2022-05-10]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

[8] Office of Management and Budget. Implementation of software supply chain security guidance under executive order (EO) 14028 Section 4(k) [EB/OL]. (2022-03-07)[2022-09-10]. https://www.nist.gov/system/files/documents/2022/03/07/EO%204k%20implementation%20questions.pdf.

[9] National Institute of Standards and Technology. Recommended criteria for cybersecurity labeling for consumer internet of things (IoT) products[EB/OL].(2022-02-04)[2022-08-10]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.

[10] National Institute of Standards and Technology. Recommended criteria for cybersecurity labeling of consumer software[EB/OL]. (2022-02-04)[2022-08-10]. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-1.pdf.

[11] National Institute of Standards and Technology. Software supply chain security guidance under executive order (EO)

14028 section 4e[EB/OL]. (2022-03-07)[2022-09-10]. https://www.nist.gov/system/files/documents/2022/02/04/software-supply-chain-security-guidance-under-EO-14028-section-4e.pdf.

[12] Cybersecurity & Infrastructure Security Agency. The national strategy to secure cyberspace national strategy to secure cyberspace[EB/OL]. (2003-02)[2022-10-10]. https://www.energy.gov/ceser/articles/national-strategy-secure-cyberspace-february-2003https://www.cisa.gov/national-strategy-secure-cyberspace.

[13] OBAMA B. Executive order: promoting private sector cybersecurity information sharing[EB/OL]. (2015-02-13)[2022-11-13]. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[14] Cybersecurity & Infrastructure Security Agency. Executive order on strengthening the cybersecurity of federal networks and critical infrastructure[EB/OL]. (2017-05-11)[2022-11-15]. https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

[15] TRELLIX. Path to cyber readiness: preparation, perception and partnership[EB/OL]. (2022-04-14)[2022-10-15]. https://www.trellix.com/en-us/assets/docs/tcrr-path-to-cyber-readiness-preparation-perception-and-partnership.pdf.

Analysis and Enlightenment of the Implementation of the "Executive Order on Improving the Nation's Cybersecurity" in the United States

ZHANG Ye-yang[1], LIU Wei[1], FANG Shi[2]

(1. Institute of Scientific and Technical Information of China, Beijing　100038;
2. Peking University, Beijing　100091)

Abstract: After the SolarWinds incident came to light in 2021, the U.S. Biden administration issued "Executive Order on Improving the Nation's Cybersecurity", outlining 55 actions that the U.S. federal agencies need to take to improve their agency's cybersecurity capabilities. After the executive order was issued, the Biden administration released a series of important documents, which have important implications for the U.S. cybersecurity-related fields, causing major changes in the U.S. federal government's cybersecurity landscape. Starting from the background of the executive order, this paper analyzes its implementation, interprets the important policies and measures adopted in accordance with it, summarizes the problems existing in its implementation, and finally puts forward the reference significance to China's cybersecurity field.

Keywords: cybersecurity; SolarWinds; executive order; zero trust architecture; supply chain security