美国《改善国家网络安全的行政命令》政策理念初探

张烨阳，刘 蔚
（中国科学技术信息研究所，北京 100038）

摘 要：2021 年美国政府因受 SolarWinds 等网络安全事件的影响，发布了《改善国家网络安全的行政命令》，拟通过强化美国联邦信息系统软件供应链安全、推广基于零信任架构的云技术使用、统一联邦信息系统运维阶段安全标准等手段全面提升美国联邦信息系统的网络安全防护能力，并借助市场的力量引领美国软件业在安全方面达到新的高度。本文从该行政命令出台的背景出发，分析了 SolarWinds 安全事件对于美国信息安全领域造成的挑战，对行政命令框架和应对网络安全挑战所采取的措施进行了解读，在此基础上提出该行政命令对我国信息安全领域的借鉴意义。

关键词：美国；网络安全；SolarWinds；行政命令；供应链安全；信息安全标准
中图分类号：TN915.08 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2022.08.002

1 背景

2021 年 5 月 12 日美国总统拜登签署了《改善国家网络安全的行政命令》（Executive Order on Improving the Nation's Cybersecurity），又称 14 028 号行政命令，这是美国当前在网络安全方面最详细的行政命令之一。2021 年发生的 SolarWinds 事件、Microsoft Exchange 事件和 Colonial Pipeline 事件等安全事件是促使该行政命令出台的重要原因。其中，SolarWinds 事件直接威胁到美国联邦机构和美国各大公司的信息安全，成为导致该命令出台的直接原因 [1]。

SolarWinds 是一家位于美国得克萨斯州奥斯汀市的大型软件公司，该公司的产品之一是名为 Orion 的 IT 性能监控系统。作为 IT 监控系统，SolarWinds Orion 拥有访问 IT 系统以获取日志和系统性能数据的特权。全球超过 30 000 个公共和私人组织（包括美国联邦机构）使用 Orion 网络管理系统来管理 IT 资源。正是这种软件的特殊性质及其广泛的部署使 SolarWinds 成为对网络攻击者非常有吸引力的目标。在本次 SolarWinds 安全事件中，攻击者攻入了 SolarWinds 公司的生产环境，将恶意代码插入到 Orion 系统的更新程序中，其后恶意代码通过系统更新潜入到受害者系统中，并在受害者的 SolarWinds Orion Platform 中创建了一个后门，其后攻击者便可以冒充用户通过该后门访问受害组织的账户 [2]。2020 年 3 月 26 日 SolarWinds 将带有后门恶意代码的 Orion 软件更新发布，攻击者借此入侵了数以千计的网络和系统，最终导致近 18 000 名客户下载了受感染的软件更新程序 [3]，美国有 9 个联邦政府机构和近 100 家公司在此次攻击中受到威胁 [4]。

美国作为世界信息产业的发源地和在 IT 信息领域实力最为强大的国家，其信息安全政策方面的一举一动都颇受关注。在遭受了历史上规模最大也

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。
通讯作者简介：刘蔚（1985—），女，博士，副研究员，主要研究方向为科学计量学。
收稿日期：2022-06-22

是最为复杂的网络攻击后，美国意识到自己的网络安全防护能力严重不足，并紧急发布了行政命令，计划迅速弥补相应政策及技术方面的安全漏洞。这份极具安全举措操作细节的行政命令将为美国未来的网络安全产业发展带来深刻的影响。

目前世界各主要国家都高度重视网络威慑能力建设，除成立网络部队外还不断增加网络武器的研制预算。2016 年至 2017 年黑客组织 The Shadow Brokers 公布了大量宣称来自高级持续性威胁（APT）组织“方程式”的黑客工具。这些顶级黑客工具隐蔽性高，被远程激活后可对被攻击设备进行控制，进而窃取国家情报和商业信息，且多个工具的唯一标识物与 2013 年斯诺登“棱镜门”曝光的美国国家安全局网络攻击平台操作手册中使用的唯一标识物吻合。除此以外同样以美国国家安全局为后台的高级持续性威胁组织“索伦之眼”的攻击目标更是直指中国、俄罗斯。

在此背景下，我国面临的信息安全形势日趋严峻，科技、金融、军事、电力等多个关乎社会稳定、国家安全的行业受到的扫描、渗透、高级持续性威胁攻击日益增多。为此，我国高度重视网络安全相关工作。在立法方面，我国 2016 年出台了《中华人民共和国网络安全法》，并以此为核心加速推进网络安全法律体系的建设，2017 年中央网信办印发《国家网络安全事件应急预案》，2021 年出台《中华人民共和国数据安全法》和《关键信息基础设施安全保护条例》。在加速推进政务办公国产化方面，推出了一批符合我国安全标准的国产化办公软硬件产品，并陆续在各政府部门、事业单位、央企中投入使用。

本文拟从《改善国家网络安全的行政命令》的细节出发，对该行政命令进行梳理，充分解读其应对近期网络攻击事件的措施，并对其理念、技术路线进行深入分析，从而为我国网络安全技术发展路线及相关政策制定提供借鉴。

2　《改善国家网络安全的行政命令》主要内容框架

《改善国家网络安全的行政命令》共包含 11 节 74 条，旨在通过消除政府与私营部门之间的网络安全威胁信息共享障碍、提高软件供应链安全性、建立网络安全审查委员会、创建响应网络事件标准手册、提高调查及补救能力、推进零信任安全架构技术的使用等手段，加强美国关键基础设施和联邦政府的网络安全。在应对危机、解决问题方式上可以归纳为以下几个方面。

2.1　联邦政府以身作则，引领美国信息系统安全达到新标准

在经历了 SolarWinds 事件、Microsoft Exchange 事件和 Colonial Pipeline 事件后，美国政府意识到目前网络安全政策及技术已无力阻挡网络攻击者对其国家安全和经济安全构成的挑战，为此在该行政命令第一节中强调，渐进式改进不会带来所需的安全性，需要做出大胆的改变和重大投资，以保护支撑美国生活方式的重要机构。在具体实现方式方面强调预防、检测、评估和补救是本届政府在加强网络安全方面的政策，并要求联邦政府必须要以身作则。所有联邦信息系统都应满足或超过本命令规定和发布的网络安全标准和要求，期待用这种方式首先让美国联邦文职行政部门和联邦政府软件供应商做出改变，从而进一步引领整个美国计算机产业向着更高的安全标准迈进，最终使其免受恶意网络攻击者的侵害。

2.2　更新联邦采购条例，破除信息共享障碍

联邦采购条例是美国联邦机构在使用财政拨款采购商品和服务时使用的主要法规，同时还包含采购所需的标准招标条款和合同条款。在 SolarWinds 事件中，部分服务提供商出于自身利益考虑或受合同条款限制，在发现网络攻击迹象后未第一时间通知相关政府部门或机构，导致该网络攻击范围进一步扩大。为阻止此类事件再次发生，行政命令一方面要求更新联邦采购条例，在其标准合同条款中，授权美国联邦政府 IT、OT 服务提供商按照各联邦机构要求对网络威胁和事件信息进行收集，另一方面要求服务提供商在发现其提供的软件或服务发生网络事件时，必须根据网络安全事件级别，按照业界公认的格式，在规定的时间内与相关机构共享网络安全事件相关的信息。

2.3　加快推进基于零信任架构的云技术在联邦政府系统中的应用

截至 2020 年 12 月，美国联邦政府 9 个机构的系统遭受了 SolarWinds 黑客攻击，并且由于攻击方

式隐蔽，攻击者很可能对系统进行了长达 14 个月的不受限制的访问。这迫使拜登政府在该项总统令中要求美国联邦文职行政部门在 60 天内制定零信任架构实施计划，并要求各机构尽可能采用零信任架构向云技术迁移。零信任架构的应用意味着抛弃传统的网络安全信任区，不断验证、检查和记录所有访问应用程序的流量以识别异常活动，而云技术的应用则可以使美国联邦机构一方面从云服务提供商处获取包括网络安全专业人才、设备在内的大量网络安全资源，加强业务系统的安全防护，另一方面更加便捷地按照同一安全标准对原本分散的联邦信息系统进行统一安全管理，避免个别信息系统因缺少维护而成为攻击者发起网络攻击的跳板。

2.4 提升美国联邦信息系统全生命周期安全

为了弥补美国在多次大规模网络攻击事件中暴露的安全短板，行政命令在加强软件供应链安全、系统安全漏洞的检测、响应、系统运行过程中日志信息的收集、维护等多个方面提出了要求，涉及信息系统全生命周期的各个环节，力争全面提升美国联邦信息系统的安全性。在加强供应链安全方面，由于商业软件在成本的约束下会优先考虑软件的可用性，在功能和性能方面首先满足客户的需求，而把完整性和保密性放在相对次要的位置，故行政命令提出了关键软件的概念，认为联邦政府所使用的关键软件安全性和完整性对联邦政府履行职能的能力至关重要，迫切需要通过严格且可预测的机制确保产品安全运行。在联邦系统运维方面，为使美国联邦网络安全牵头机构能够在出现系统安全漏洞时对各机构信息系统进行更全面的分析，行政命令要求各机构采取标准化信息安全响应流程，统一应对安全事件及安全漏洞的方案，确保牵头机构在发现网络漏洞时能以一致且集中的方式跟踪各机构对特定安全事件的响应程度。在技术层面，行政命令计划通过端点检测和响应系统（EDR）的部署以及网络和系统日志收集方式的标准化，使联邦政府从系统层、网络层获取更多网络安全信息，以更好地抵御、防范网络攻击。

2.5 建立网络安全审查委员会

行政命令要求美国国土安全部与美国司法部根据《国土安全法案》设立网络安全审查委员会，意在当美国联邦文职行政部门系统和非联邦系统发生重大网络安全事件时，第一时间对引发事件的威胁活动、相关漏洞、应采取的措施进行评估、审核。委员会由美国国防部、美国司法部、美国网络安全和基础设施安全局、美国国家安全局和美国联邦调查局的代表以及私营部门的网络安全代表或软件供应商组成。当审查的事件涉及美国联邦文职行政部门信息系统时，美国行政管理和预算局的代表须参加会议。委员会的主席和副主席，由一名美国联邦官员和一名来自私营部门的人员担任。该委员会在发生重大网络事件后召开会议，分析发生的情况并提出具体建议，以改善网络安全，避免反复出现同样的错误。

3 《改善国家网络安全的行政命令》主要技术路线

SolarWinds 网络安全事件造成如此广泛且严重的影响，在客观因素方面主要有以下两点：首先，攻击者以美国市场主流的系统监控软件为目标，对其采用了供应链攻击的方式，渗透至软件供应商的生产环境，并将恶意代码插入尚未发布的 SolarWinds 更新程序中。后期随着软件更新，恶意代码被传播至 18 000 多名客户的系统中。在成功攻入首批客户的系统后，攻击者以此为出发点，又进一步攻击了与此系统存在信任关系的低安全等级系统，扩大了受害系统范围。其次，从技术的角度看，在恶意代码传播到客户服务器后，攻击者采用哈希算法和压缩算法对代码本身进行加密，且在恶意程序连接其命令控制服务器前检查是否有安全软件运行，这相比以往的攻击手段更具隐匿性，使系统运维人员较难发现被攻击的迹象。主观因素方面，在本次网络安全事件中，部分服务提供商出于自身利益的考虑或受合同条款限制，在发现网络攻击迹象后不能第一时间通知相关政府部门或机构，从而导致网络攻击范围进一步扩大。针对在本次网络安全事件中暴露出的以上问题，《改善国家网络安全的行政命令》在以下四个方面采取了针对性的措施。

3.1 在软件制造方面，提升供应链安全

（1）将涉及美国联邦政府履行关键职能的软件定义为关键软件，迅速提高关键软件的安全性和完整性。

（2）在限定的时间内，发布软件开发安全性指南及指导文件，并在指导文件中要求软件开发

商：①构建安全的开发环境、在企业中建立多因素认证的资源访问控制、对开发环境的数据进行加密、记录开发环境使用的产品并尽量减少外部依赖。②采用自动化工具定期对软件的完整性和潜在漏洞进行检查。③维护准确的软件代码或组件来源信息并在软件开发过程中反复检查和执行针对第三方软件组件、工具、服务的控制措施。④向软件购买者公布软件物料清单。⑤确定软件开发商源代码的最低测试标准，明确测试的工具和方式。

（3）在联邦机构软件采购方面，要求各机构在颁布软件开发安全指南后的 30 天内，严格遵循指南相关规定。对于已有的软件，在续签软件升级或维护合同时，各机构可要求豁免遵循指南内的规定。此类请求在提交时，要附有在有限期限内遵循指南要求的计划及对潜在风险的缓解计划。对于尚未进行的软件采购，一方面对现有软件采购合同进行修改，要求软件供应商按照软件开发安全指南的要求进行软件开发并提供证明，另一方面各机构应从采购计划中删除不符合软件开发安全指南的产品。

（4）启动消费品标识计划，标识软件通过的安全评估等级，以此反映出产品的安全性，使采购软件的客户可以快捷地了解该软件的安全水平。

3.2　在系统部署方面，推广使用基于零信任架构的云技术

（1）通过向技术和人员投资，推动现有系统向云服务迁移，以便集中和简化对网络安全数据的访问，推动网络安全风险识别和管理分析。

（2）要求联邦各机构负责人在规定时间内为云技术的部署和使用划拨资源，并给出完成系统向云端迁移的时间表。

（3）为使联邦政府更好地预防、检测、评估和应对网络安全事件，行政命令要求各机构尽可能采用零信任架构向云环境迁移原有系统。在此迁移过程中，行政命令要求美国行政管理和预算局以及美国网络安全和基础设施安全局通过发布联邦云安全战略、云安全技术参考架构文档、云服务治理框架对各机构系统迁移过程和迁移后需要采取的数据保护措施进行指导。

3.3　在数据安全方面，梳理敏感数据资产，强化加密措施

（1）要求美国联邦文职行政部门负责人与美国网络安全和基础设施安全局局长协商，评估其机构非机密数据的类型和敏感性，重点确定机构认为最敏感和受到最大威胁的非机密数据，并确定这些数据的合理处理和存储方案。

（2）要求各机构在美国网络安全和基础设施安全局的指导下，最大限度地对各机构管理的静态和传输数据采用多重认证和加密。无法在规定时间内完成多重认证和数据加密的机构应向美国网络安全和基础设施安全局以及国家安全事务主席助理提交书面说明。

3.4　在系统运维方面，加强信息收集并对安全事件应对策略进行统一

（1）在终端主机层面，通过端点检测和响应计划，在美国联邦文职行政部门的终端上安装安全管理软件，对终端的安全漏洞情况和网络安全信息进行收集，对终端的应用程序及网络的运行情况进行检测。当发现安全威胁时，对相应的威胁进行遏制、记录，并将威胁信息上传至安全管理控制端。

（2）在服务系统层面，要求美国联邦各机构及其 IT 服务提供商加强对联邦信息系统的网络和系统日志信息的收集。在具体操作层面，除了对要维护的日志类型、保存日志的时间、保护日志的方法做出要求外，为确保日志数据的保密性和完整性，还对日志收集后需采用的加密手段、完整性检验手段做出了要求。

（3）在对安全漏洞和安全事件的标准化响应方面，为了避免各个联邦机构在应对安全漏洞和安全事件过程中因流程不同而导致的混乱，行政命令要求美国国土安全部、美国网络安全和基础设施安全局牵头制定一套统一的，可以描述事件响应各阶段进度和完成情况的网络安全事件应对流程，并要求各个联邦机构在系统运维过程中按照此流程开展网络安全事件应对工作。这样可以确保发生大规模安全事件时，牵头机构可以用较为一致的方式对事件进行分类并跟踪各联邦机构处理事件的进度。同时，行政命令还要求美国网络安全和基础设施安全局局长在机构完成事件响应后，审查和验证相关部门的事件响应和补救结果。

4　对我国的经验借鉴

我国正处在信息化浪潮之中，大量与国家安

全、民生相关的关键基础设施的运转都有赖于信息系统和网络的安全运行。目前国际形势错综复杂，我国面临的网络安全形势也日趋严峻，高级持续性威胁攻击事件层出不穷。为了更好地维护国家主权，保护重要基础设施的安全，为经济建设保驾护航，我国可从美国《改善国家网络安全的行政命令》中获得以下几个方面的经验。

4.1 在网络安全防范意识方面，针对部署重要业务系统的相关政府机构定期开展网络安全知识及网络安全形势教育活动

2016 年我国颁布的《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。2017 年中共中央办公厅印发的《党委 (党组) 网络安全工作责任制实施办法》明确了各单位党政一把手是各单位网络安全工作的主要负责人，也是网络安全工作的第一责任人。2021 年我国颁布《中华人民共和国数据安全法》以及《关键信息基础设施安全保护条例》。以上法规、办法的发布、出台让各政府机构、部门对网络安全给予了充分的重视，但网络安全的形势是在不断变化的，各种新的网络攻击手段层出不穷。为了应对网络攻击带来的挑战，需要各个机构协调人、财、物等多方面的资源去完成相应的网络安全防范工作。应定期对各个机构、部门的网络安全相关责任人以及负责网络安全工作的人员进行培训，一方面让他们通过培训了解目前最新的网络安全发展动态，另一方面在网络安全工作需要协调相应资源时，可以在一定程度上得到各机构、部门管理层的支持。

4.2 在软件设计、开发方面，出台政府软件产品准入标准，强化软件供应链安全，加强市场引导

在 SolarWinds 供应链事件中，由于攻击者能够访问 SolarWinds 软件的开发和交付通道，因此他们能够将恶意代码添加到名为 SolarWinds.Orion.BusinessLayer.dll 的 SolarWinds Orion 平台驱动程序中。对于这种供应链攻击来说，受感染的 dll 具有相应的数字签名，使得恶意软件长时间未被发现，从而对用户造成了巨大的影响。为了快速应对新型威胁，以保护关键基础设施安全，美国《改善国家网络安全的行政命令》提出迫切需要实施更加严格且可预测的机制，确保产品如期安全运行，其中“关键软件”的安全性和完整性尤其需要关注。其对关键软件开发环境的构建、信任关系的审核、软件开发环境中多因素认证的应用、开发环境数据的加密、日志的记录、自动化软件完整性验证工具的应用、自动化漏洞检测工具的应用、软件物料清单的标准、客户软件标识计划的推广都做出了详尽要求。其中最为重要的是对关键软件物料清单的重视。目前软件的开发已呈现出模块化的趋势，商业软件为了在最短时间内开发出满足功能需求的产品，多采用已有的或外来的功能模块进行堆砌，但若不对模块进行规范化管理，模块中存在的漏洞有可能在软件上线运行后成为重要的网络安全隐患。在这方面，我国《关键信息基础设施安全保护条例》已在 2021 年 4 月 27 日的国务院常务会议上通过，并自 2021 年 9 月 1 日起施行。但其中并没有表达类似关键软件的概念和相关要求，只是在第十九条中强调运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。这与抵御新型网络威胁的需求尚有较大差距，让运营者无法验证所采购的产品和服务是否安全。且采购产品和服务在被认为可能影响国家安全的情况下才应进行安全审查，这意味着对于产品是否会影响国家安全的判断带有主观性，安全审查工作应从软件开发时就予以开展。

为了提升我国关键信息系统的安全性，建议首先我国将部署在关键信息基础设施上的软件定义为关键软件，并制定关键软件开发标准，让相关部门对关键软件符合标准的情况予以审核。对符合标准的关键软件产品予以标识，并将其列入重要系统关键软件采购目录，使部署重要系统的机构在选购关键软件时可以对其安全性进行确认。这样一方面可以更好抵御供应链攻击威胁，另一方面可以借助政采市场带动我国整个软件行业向着更加安全、标准的方向发展。此外，要着重提升关键软件的全生命周期安全性。在关键软件开发过程中，要对关键软件的开发环境、开发企业内部的多因素认证资源访问控制措施、数据加密措施、开发环境使用的产品等方面提出相应要求。开发完成后，也要采用自动化工具定期对软件的完整性和潜在漏洞进行检查，维护准确的软件代码或组件来源信息，并在软件开

发过程中反复检查和执行针对第三方软件组件、工具、服务的控制措施。在关键软件交付时要向采购软件的机构公布软件物料清单，并向客户提供软件供应商源代码的最低测试标准，明确测试的工具和方式等信息。

4.3　在国家重要服务系统部署方面，引导现有系统向基于零信任架构的云服务迁移

我国目前已在大规模推广政务云建设。在提升效率、降低成本的同时应注重网络安全的提升。

一是充分利用云服务的优势，将政府服务系统进行集中部署，简化相关系统网络数据资源的访问。在云端部署各类专业网络安全设备，并配备专业的安全运维团队对纳管在云端的系统进行统一、集中的网络安全风险识别、管理、分析。同时注重对安全团队人员的定期培训，使其及时了解网络安全技术前沿领域发展动向。

二是我国应制定、发布云安全战略、云安全技术参考架构、云服务治理框架等方面的标准、指南，对现有政务服务系统向云服务的迁徙进行指导，同时应吸取 SolarWinds 事件中攻击者获得授权后进行东西向攻击的教训，推广零信任架构在云服务中的使用，赋予用户最低权限，并对数据资源访问进行多重验证，减少被攻击后遭受的损失。

4.4　在国家重要服务系统运维方面，出台关键系统网络安全相关细则，强化针对重要政务系统的信息收集能力

目前《中华人民共和国网络安全法》要求网络运营者采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。《信息安全技术网络安全等级保护基本要求》规定对于国家安全较为重要的三级系统，应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，对应用系统重要安全事件进行审计；详细记录操作日志；定期对运行日志和审计数据进行分析，以便及时发现异常行为。上述措施可在发生网络安全事件时，提供部分攻击溯源线索，但无法有效应对 SolarWinds 事件中的供应链攻击。在 SolarWinds 事件中，攻击者通过供应链攻击让恶意代码成为了系统监控软件的一部分，并通过对恶意代码进行编码、目标系统杀毒软件运行检测、动态解析域名等方式进一步降低了被发现的可能。

为了应对供应链攻击，建议首先在关键基础信息系统上强制安装终端保护系统，对终端安全漏洞情况、应用程序运行情况、网络流量数据信息进行收集、检测。当发现安全威胁时，对相应的威胁进行遏制、记录，并将威胁信息上传至安全管理控制端。其次，要求运营关键基础信息系统的部门加强对系统网络和日志信息的收集，并对所要维护的日志类型、格式，保存日志的时间，存储日志数据的方式，发生安全事件时提交日志数据的途径提出相应要求。为确保日志数据的保密性和完整性，还需对保存的日志数据进行加密和定期的完整性检验。同时，在数据安全方面，我国应在《中华人民共和国数据安全法》的基础上出台数据分级保护实施指南，对不同级别的数据采取不同的保护措施，对敏感重要数据的存储和传输应采用多重认证和加密措施。

4.5　在提升应对网络安全事件能力方面，对政府相关单位网络安全进行标准化管理

为在安全事件发生后更全面准确地对事件进行分析，美国《改善国家网络安全的行政命令》要求各个联邦机构采取标准化的网络安全事件响应流程。而《中华人民共和国网络安全法》在关键信息基础设施保护方面只是要求部门制定本行业、本领域的网络安全事件应急预案，并定期组织演练；当安全事件发生后，按照危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施，但未在标准化方面提出相关要求。我国应充分重视标准化在网络安全事件应急中的作用，制定统一的网络安全漏洞和安全事件响应标准，确保网络安全事件发生时以较为一致和集中的方式对事件进行分类及跟踪处理，提升网络安全事件反应速度及能力。

5　总结

网络安全目前被认为是国家安全中的重要一环，没有网络安全就没有国家安全。对我国而言，面对严峻的外部网络安全形势，如何确保我国的网络安全是一个长期性课题。本文从美国拜登政府的总统令《改善国家网络安全的行政命令》出发，分析了其政策出台的背景，分五个方面对行政命令的

主要内容进行总结，并对行政命令为了应对新型供应链网络攻击所采取的措施进行了研究，最后结合我国实际情况，提出了我国应对新型网络攻击、改善网络安全的建议。网络安全不是单纯的技术问题，而是人、技术、管理的结合，实现成功的网络安全防护需要部署有远见的高层决策者和具体业务操作人员，需要可实现安全目标的技术措施，还需要切合实际的管理措施，三者相互协同、共同作用，任何一环的缺失，都将使网络安全形同虚设。网络安全不是一时之功，需要根据全球网络安全前沿动态不断改进，最终实现我国网络安全长治久安，为我国社会、经济、民生等各领域的发展保驾护航。■

参考文献：

[1] Biden J R. Executive order on improving the nation's cybersecurity[EB/OL]. [2021-05-12]. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[2] Saheed O, Sean MK. SolarWinds hack explained: Everything you need to know[EB/OL]. [2022-01-29]. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know.

[3] Cimpanu C. SEC filings: SolarWinds says 18,000 customers were impacted by recent hack[EB/OL]. [2021-12-14]. https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/.

[4] Porter J. White House now says 100 companies hit by SolarWinds hack, but more may be impacted[EB/OL]. [2021-02-18]. https://www.theverge.com/2021/2/18/22288961/solarwinds-hack-100-companies-9-federal-agencies.

A Preliminary Study on the Policy Concept of the US Executive Order on Improving the Nation's Cybersecurity

ZHANG Ye-yang, LIU Wei

(Institue of Scientific and Technical Information of China, Beijing 100038)

Abstract: In 2021, the US government issued the "Executive Order on Improving the Nation's Cybersecurity" due to the impact of cybersecurity incidents such as SolarWinds. The executive order is planned to comprehensively improve the cybersecurity protection capabilities of the US federal information system by enhancing the security of the US federal information system software supply chain, promoting the use of cloud technology based on a zero-trust architecture, and unifying the security standards for the operation and maintenance phase of the federal information system, as well as leveraging the power of the market, leading the US software industry to new heights in security. Starting from the background of the executive order, this paper analyzes the challenges caused by the SolarWinds security incident to the US information security field, and interprets the framework of the executive order and the measures taken to deal with the cybersecurity challenges. On this basis, it puts forward the reference significance of the executive order to the field of information security in China.

Keywords: the U.S.; cybersecurity; SolarWinds; executive orders; supply chain security; information security standards