CCID 赛迪智库 译丛

2023 年 5 月 15 日　　第 15 期　　总第 594 期

美国国家网络安全战略（2023 版）

【译者按】今年 3 月，美国白宫发布近五年来的首份《国家网络安全战略》（以下简称“《战略》”），《战略》详细阐述了美国政府改善数字安全的系统性方法，旨在帮助美国准备和应对新出现的网络威胁。报告围绕建立“可防御、有韧性的数字生态系统”，给出了保护关键基础设施、破坏和摧毁威胁行为者、塑造市场力量、投资于有韧性的未来、建立国际伙伴关系等五大支柱共 27 项举措。赛迪智库网络安全研究所对该报告进行了编译，期望对我国有关部门有所帮助。

【关键词】网络安全 美国 可防御 有韧性 支柱 举措

一、背景概述

互联网繁荣互联的未来愿景能否实现，将取决于各种基础技术和系统的网络安全与韧性。网络安全对于国家经济关键功能、关键基础设施的正常运行、民主制度的力量建设、数据和通信隐私保护，以及国防安全保障都至关重要。因此，自拜登政府成立之初，美国就果断采取多项行动加强网络安全，包括任命白宫高级网络安全官员、签署旨在改善国家网络安全的行政命令、与私营部门和盟友密切合作等，来提高美国抵御和应对专制国家网络威胁的能力，保护美国国家利益。整体来看，通过吸取过往经验教训，近些年美国在数字生态体系协同防御方面取得了重大进展。

然而，美国数字生态体系基础架构的不稳定性减弱了这些工作成效，数字生态体系的组成部分仍然容易被破坏和利用，且常常为恶意行为体所利用。因此，美国必须从根本上改变数字生态体系基础的不稳定性，将优势转化给生态体系的保卫者，并不断挫败威胁它的力量。为建立一个可防御、有韧性的数字生态体系，攻击者将付出比防御者更高的代价，敏感或私人信息将得到安全保护，不会因某些事件或错误引发灾难性、系统性的后果。本《战略》将使美国及其盟友和伙伴得以共同构建这一安全可信的数字

生态体系，使之先天就更容易防御、更具韧性，且契合美国的价值观。美国预计利用十年的时间实现这些成果。

《战略》从两方面着手建立制度机制，一方面，建立强有力的合作，特别是公共和私营部门之间的合作，对于保护网络空间至关重要。合作还有助于应对系统性挑战，可为个人用户和小型机构分担部分网络安全责任。通过与产业、民间团体以及州、地方、部落和属地政府合作，美国将重新平衡网络安全的责任，使之更加有效和公平。另一方面，重新调整激励机制，鼓励对安全、韧性和有前景的新技术的长期投资。美国将与盟友和伙伴合作，推行负责任的国家行为规范，追究各国在网络空间中不负责任的行为，并斩断全球危险网络攻击背后的罪犯链条。美国将提供必要的资源和工具，以确保在最关键的基础设施中实施有效的网络安全措施。

（一）《战略》发布的宏观环境

1、新兴趋势

在新兴技术和日益复杂且相互依存的系统的发展推动下，未来 10 年将成倍增加因不安全信息系统所衍生的系统性风险。

一是，世界正在进入到一个对数字化更加依赖的新阶段，各种软件和系统变得越来越复杂，在为企业和消费者提供价值的同时，也增加了美国国家层面的不安全感。美国常常以牺牲安全性

和韧性为代价，将新的功能和技术叠加到本已错综复杂而脆弱的系统上。尤其是人工智能系统（这些系统能够以自身开发者意想不到的方式行事）的广泛应用，正在加剧美国许多重要技术系统的复杂性和风险。

二是，数字技术越来越多地触及美国人生活中的敏感地带，技术在提供便利的同时，也带来了新的、往往不可预见的风险。随着人们的生活与视频/音频流、可穿戴设备和生物识别技术交织在一起，所收集个人数据的数量和私密性呈指数级增长，而对这些数据的窃取行动也在迅速增加，这为各种恶意行为体提供了对个人实施监视、操纵和勒索的新载体。

三是，互联网不断通过各种共享平台将个人、企业、社区和国家连接起来，使规模化的商业解决方案和国际交流成为可能。但这种全球互联互通的加快也带来了网络安全风险，如对某一机构、行业或国家的攻击可以迅速蔓延至其他行业和地区。就像2017年俄罗斯对乌克兰实施的“非佩提亚”（NotPetya）网络攻击，最终就波及到了欧洲、亚洲和美洲，造成了数十亿美元的损失。随着世界系统网络相互依存度的提高，这类攻击的潜在破坏性会继续加大。

四是，下一代互联互通正在打破数字和物理世界之间的界限，使美国一些最重要的系统正面临着被破坏的风险。美国的工厂、

电网和水处理设施，以及其他重要的基础设施，正越来越多地淘汰旧的模拟控制系统，并迅速引入数字运营技术（OT）。先进的无线技术、物联网和太空资产，包括民用和军用的定位、导航和授时，环境和气象监测，以及从银行到远程医疗的日常互联网活动，将加速这一趋势，迫使美国将许多基础系统联网，这会使网络攻击能够对人们的日常生活造成更大的破坏和影响。

2、恶意行为体

恶意的网络活动已经从蓄意破坏，发展到了间谍活动与窃取知识产权、针对关键基础设施的破坏性攻击、勒索软件攻击，以及旨在破坏公众对美国民主基础信任的网络影响活动。攻击性黑客工具和服务（包括外国商业间谍软件）曾经仅有少数资源丰富的国家能够获取，而现在却严重泛滥。在这些工具和服务的支持下，犯罪集团的网络行动已经对美国及其盟友和合作伙伴的国家安全、公共安全和经济繁荣构成了威胁。尤其是勒索软件攻击已经扰乱了从能源管道和食品企业到学校和医院等美国和世界各地的关键服务和运营。近些年，勒索软件攻击造成的经济损失持续攀升，每年高达数十亿美元。

（二）《战略》以“通向具有韧性的网络空间之路”为目标

整个数字生态体系的利益相关方之间开展深入而持久的合作，是实现生态体系可防御、更具韧性且契合美国价值观的基础。

本《战略》旨在围绕以下五个支柱建立和加强合作：

（1）保卫关键基础设施；

（2）瓦解和摧毁威胁行为体；

（3）造市场力量以推动安全性和韧性；

（4）加大投入，打造有韧性的未来；

（5）建立国际伙伴关系以追求共同目标。

上述每项工作都需要各个利益相关群体开展前所未有的合作，包括公共部门、私营企业、民间团体以及国际盟友和合作伙伴。本《战略》围绕五大支柱阐明了各方的共同目标和优先事项愿景，重点阐述了在实现该愿景的过程中将面临的挑战，并确定了各机构工作的具体战略目标。

为了实现上述支柱提出的愿景，本《战略》将就美国的网络空间作用、责任和资源的分配方式做出两项根本性转变。在实现这些转变的过程中，美国渴望的不仅仅是提高自身的防御能力，而且要应对那些目前与美国利益相悖的基础的不稳定性。

1、重新平衡保护网络空间安全的责任

网络空间中最具能力和条件的参与者必须更好地管理数字生态体系。目前，降低网络风险的重任更多是落在终端用户侧。某

个人一时的判断失误，使用了过期的密码，或错误点击了某个可疑链接，不应该影响到国家安全。美国的总体网络韧性不能依赖最小的机构和公民个人的持续警惕。相反，无论在公共或私营部门，美国必须对最具能力和条件的参与者提出更高要求，以确保美国数字生态体系的安全性和韧性。在一个自由和互联互通的社会中，美国的数据会被各种系统所掌握并依赖其运行，而保护数据并确保关键系统的可靠性，是各系统所有者、运营商及相关技术供应商的责任。政府的作用包括：保护自身的系统；确保私人实体（特别是关键基础设施实体）保护他们的系统；履行政府的核心职能，比如从事外交、收集情报、征收经济成本、执法，以及采取打击行动来应对网络威胁。产业和政府必须共同推动有效和公平的合作，纠正市场失灵，最大限度地减少网络事件对社会最弱势群体的伤害，并保护美国共享的数字生态体系。

2、重新调整激励机制以鼓励长期投资

美国有必要重新平衡必要的激励机制，为构建未来的数字生态体系奠定更强大、更具韧性的基础。本《战略》概述了联邦政府将如何利用一切可用的工具来重塑激励机制，并以合作、公平和互利的方式来实现共同目标。美国必须确保市场力量和公共计划均鼓励安全性和韧性，打造一支强大且多元化的网络人才队伍，通过设计追求安全性和韧性，战略性地协调网络安全的研发

投入，并促进美国数字生态体系的合作管理。为实现这些目标，联邦政府将着力于平衡和协调上，以最小的代价实现最大的防御能力和系统韧性。事实上，联邦政府正在不断加大投入，如更新维护美国的基础设施、对美国的能源系统进行数字化转型并实现脱碳、保护美国的半导体供应链、使美国的加密技术现代化，以及重振美国的外交和国内政策重点。

（三）《战略》内容依据现行政策制定

本《战略》是在过往塑造美国战略环境和数字生态体系的重大成就的基础之上，为美国网络安全管理制定的全新方法。《战略》是基于第 13800 号行政命令《加强联邦网络和关键基础设施的网络安全》、第 13691 号行政命令《促进私营部门网络安全信息共享》、第 13636 号行政命令《改善关键基础设施网络安全》、第 21 号总统政策指令《关键基础设施安全性和韧性》和第 41 号总统政策指令《美国网络事件协调》所建立的框架，目标是确保联邦系统的安全和与私营部门的合作。

本《战略》取代了 2018 年的《国家网络战略》，但保留了包括数字生态体系的协同防御等诸多优先事项，《战略》还延续了第 14028 号行政命令（EO）《改善国家网络安全》、《第 5 号国家安全备忘录》（NSM）“改善关键基础设施控制系统的网络安全”、《第 8 号国家安全备忘录》“改善国家安全机构、国防部

和情报系统的网络安全”、《2008 年国家网络安全综合计划》等行政措施的基本方向。本《战略》与《国家安全战略》和《国防战略》均是由一支跨部门团队制定的，其经过了与私营部门和民间团体长达数月的磋商。

二、支柱一：保护关键基础设施

美国致力于建立持久有效的协同防御模式，公平分配风险和责任，为数字生态系统提供基本的安全和韧性，具体包括五项举措。

（一）战略目标 1.1：制定支持国家安全和公共安全的网络安全要求

目前，美国政府已在多个关键行业建立了网络安全自律要求，包括运输安全管理局牵头的石油和天然气管道、航空和铁路，以及环境保护署牵头的供水系统等，旨在确保关键基础设施安全和有韧性地运营。但目前美国缺乏统筹性的、强制性的监管要求，导致关键基础设施安全管理出现了诸多不一致和不充分的效果。当下，美国的战略环境需要现代和灵活的网络安全监管框架，可针对不同行业的风险特征，通过统筹协调来避免监管重复，同时顾及到实施成本。事实上，最有效的监管框架是那些在危机发生前就已到位的框架，而不是在危机发生后出台紧急法规。

1、制定网络安全法规

在制定关键基础设施的网络安全法规时：一是应以绩效为基础，利用现有的网络安全框架、自愿一致的标准和指南，包括网络安全和基础设施安全局（CISA）的网络安全绩效目标和国家标准与技术研究院（NIST）的改善关键基础设施网络安全的框架。二是具有一定的灵活性，在对手提高能力和改变战术时有足够的敏捷性来调整应对。三是鼓励监管机构推动采用安全设计原则，优先考虑基本服务的可用性，确保系统设计能够应对安全故障并快速恢复。法规将界定最低预期网络安全做法或目标，但本届政府鼓励并将支持各实体进一步努力超越这些要求。四是本届政府将审视各机构的权力差距，并通过与行业、国会和监管机构的合作来弥补这些差距，以更好地在云计算和其他重要第三方服务行业中推进网络安全实践。

2、理顺和精简新的和现行的法规

有效的法规可以最大限度地降低合规成本和负担，使各机构能够投入资源来建立韧性并保卫其系统和资产。通过以符合现行政策和法律的方式利用现有的国际标准，监管机构可以最大限度地减少独特要求的负担，并减少对监管协调的需求。此外，在联邦法规存在冲突、重复或过于繁琐的情况下，各监管机构必须携手合作，尽量降低这些危害。必要时，美国将寻求跨境监管协调，

以防止网络安全要求阻碍数字贸易往来。在可行的情况下，监管机构不仅要努力协调法规和细则，还要协调对受监管实体的评估和审计。

3、使受监管实体能够承受安全成本

不同的关键基础设施行业承受网络安全成本的能力各不相同，包括不加干预就不会轻易增加投资的低利润行业，以及可以承受改善网络安全的边际成本的行业等。在某些行业，监管可能是必要的，可以创造一个公平的竞争环境，使企业不会在网络安全方面竞相比烂。而在其他行业，则鼓励监管机构通过调节税率、税收结构或其他措施来激励在网络安全方面的必要投资。在制定新的网络安全要求时，鼓励监管机构与受监管实体进行协商，以了解如何满足这些要求。

（二）战略目标 1.2：扩大公私合作规模

保护关键基础设施免受网络安全威胁，需要一种仿照互联网分布式结构的网络防御模式。美国将借助结构化的职能职责，以及数据、信息和知识的自动共享交换所带来的强大连通性，以加强各个主体之间的合作，从而实现这种分布式的网络模式这本质上是将机构的协作与技术驱动的连通性相结合，创造一个基于信任的“网络中的网络”，进而建立态势感知系统，促使网络安全保护主体采取集体和的同步行动保护美国的关键基础设施。

网络安全和基础设施安全局是关键基础设施安全性和韧性的国家协调机构，负责与行业风险管理机构（SRMAs）进行协调，使联邦政府能够扩大与全美关键基础设施所有者和运营商之间的协调。联邦政府将继续加强网络安全和基础设施安全局与其他行业风险管理机构之间的协调，投资于行业风险管理机构能力的发展，并督促他们积极呼应行业内关键基础设施所有者和运营商的需求。此外，联邦政府将与产业合作，确定各行业的需求，并评估当前行业风险管理机构能力方面的差距。联邦政府还将加强深化与软件、硬件以及管理服务提供商等私营部门的战略合作，旨在借助这些供应商的技术能力来重塑网络环境，以提高安全性和韧性。网络安全和基础设施安全局和行业风险管理机构将探索技术和组织机制，以加强和发展机器对机器的数据共享。

（三）战略目标 1.3：整合联邦各网络安全中心

联邦政府必须协调各部门的权力和能力，使之共同承担保障关键基础设施防御的责任。联邦网络安全中心将作为协作节点，负责整合政府在国土防御、执法、情报、外交、经济和军事任务上的职能。一旦整合成功，这些职能将推动政府内部的协调，并使联邦政府能够有效和果断地支持非联邦合作伙伴。接下来，联邦政府需要进一步努力加强和整合联邦政府的运营能力，完善联邦网络安全中心的整合。国家网络总监办公室将主导政府的各项

工作，加强各中心的整合、找出能力差距，并制定实施方案，以实现迅速和大规模的合作。

（四）战略目标 1.4：更新联邦事件响应计划和流程

私营部门有能力在没有联邦直接援助的情况下缓解大多数网络事件。而当他们需要联邦援助时，联邦政府必须做到统一、协调、全面响应。遭受网络威胁的机构必须了解在哪种情况下应该联系哪些政府机构。联邦政府必须提供明确的指导，说明私营部门的合作伙伴在网络事件中如何联系联邦机构寻求支持，以及联邦政府可以提供何种形式的支持。

（五）战略目标 1.5：实现联邦防御现代化

本届政府将推动基于零信任原则的联邦系统现代化策略。通过提高自身网络的防御能力和韧性，联邦政府将成为私营部门效仿的典范。

1、共同保护联邦文职机构

由于各机构的组织结构、任务、能力和资源各有不同，联邦文职行政部门的网络安全成果也大相径庭。美国必须为联邦网络安全制定一个模式，以平衡各机构单独的权力和能力以及通过共同防御方法实现的安全利益。美国将继续通过整个联邦政府的重点行动来建立联邦的凝聚力：行政管理和预算局将与网络安全和基础设施安全局进行协调，制定一项行动计划，通过行使共同防

御，提升集中共享服务的可用性，以及缓解软件供应链的风险，以确保联邦文职行政部门系统的安全性。

2、发展现代化的联邦系统

联邦政府必须更换或升级无法抵御复杂网络威胁的信息技术和运营技术系统。行政管理和预算局将领导制定一项多年生命周期计划，淘汰维护成本高昂且不堪一击的陈旧系统，以加快联邦文职行政部门的技术现代化。该计划预期在 10 年内淘汰所有无法落实美国《零信任架构战略》的陈旧系统，或以其他方式降低该时间段内无法取代的系统的风险，如通过加速迁移至基于云的服务，提升整个联邦政府的网络安全态势，进而提升其向美国人民提供数字服务的安全性和韧性。

3、保护国家安全系统

国家安全系统（NSS）负责存储和处理联邦政府的一些最敏感的数据，必须确保其免受各种网络和物理威胁，包括来自内部、网络犯罪分子和其他国家对手的威胁。国家安全局局长作为国家安全系统的国家管理者，将与行政管理和预算局进行协调，为联邦文职行政部门各机构的国家安全系统制定一项计划，以确保实施《第 8 号国家安全备忘录》对增强网络安全的要求。

三、支柱二：瓦解和摧毁威胁行为者

美国将动用外交、信息、军事（动能和网络）、金融、情报和执法能力等一切国家力量和手段来瓦解和摧毁试图威胁美国利益的行为者。美国的目标是让恶意行为者无法通过持续的网络活动来威胁美国的国家安全或公共安全。

（一）战略目标 2.1：整合联邦政府的打击活动

打击活动必须具有持续性和针对性，使网络犯罪活动无利可图，让从事恶意网络活动的外国政府行为者不再将其视为实现其目标的有效手段。联邦政府必须整合美国司法部、国防部、情报部门现有的打击活动，进一步开发技术和组织平台，以实现持续、协调的行动。美国国家网络调查联合任务部队（NCIJTF）作为协调整个政府破坏行动的多机构协调中心，将以更快的速度、规模和频率协调这些行动。

（二）战略目标 2.2：加强公私业务合作以扰乱对手

鼓励私营部门合作伙伴与国家网络取证和培训联盟（NCFTA）等一个或多个非营利组织进行联合协作，针对特定威胁的合作，由少数值得信赖的运营商组成，并由相关枢纽负责托管并提供支持。此外，应加强利用虚拟协作平台促进信息共享，并迅速开展工作以瓦解对手。

（三）战略目标 2.3：提升情报共享和通知受害者的速度和规模

一是联邦政府将提高网络威胁情报共享的速度和规模，以便政府在掌握某机构即将被攻击或可能已经受到威胁的信息时，主动给网络保护者发出警报并通知受害者。二是行业风险管理机构将与网络安全和基础设施安全局、执法机构以及网络威胁情报整合中心进行协调，确定其部门内的情报需求和优先事项，并制定与政府和非政府合作伙伴共享警报、技术指标、威胁背景及其他相关信息的流程。这些流程必须为私营部门提供机制，以便他们及时向联邦政府提供反馈和与自身相关的威胁情报，从而优化对网络威胁的瓦解和进一步的情报收集。三是联邦政府还将审查解密政策和流程，以确定在哪些情况下有必要扩大额外的机密访问和许可，以便向关键基础设施的所有者和运营商提供可操作的情报。

（四）战略目标 2.4：防止滥用美国网络基础设施

恶意网络行为者利用美国的云基础设施、域名注册商、主机和电子邮件提供商以及其他数字服务，对美国及国外的个人、企业、政府和其他机构实施犯罪活动、恶意操作和间谍活动。通常，这些服务都是通过外国转售商租赁的，转售商与美国供应商之间存在多级隔离，制约了这些供应商处理投诉或回应美国当局法律

程序的能力。联邦政府将与云计算和其他互联网基础设施提供商合作，快速发现对美国基础设施的恶意使用，与政府共享恶意使用的报告，使受害者更容易报告这些系统的滥用情况，并使恶意行为体从一开始就更难获得这些资源。

（五）战略目标 2.5：打击网络犯罪和勒索软件

鉴于勒索软件对关键基础设施服务的影响，美国将利用国家力量采取四方面举措：利用国际合作，破坏勒索软件生态系统，孤立那些为犯罪分子提供安全避风港的国家；调查勒索软件犯罪，并利用执法部门和其他部门破坏勒索软件基础设施和行为者；增强关键基础设施抵御勒索软件攻击的能力；解决滥用虚拟货币洗钱的问题。

四、支柱三：塑造市场力量以推动安全性和韧性

美国将通过塑造市场力量让数字生态系统中最有能力降低风险的人承担责任，具体包括六项举措。

（一）战略目标 3.1：让数据管理者负起责任

政府支持各项数据保护立法工作，对收集、使用、传输和维护个人数据的数据处理主体的能力制定强有力的明确要求，加强地理位置、健康信息等敏感数据保护。相关立法应确保个人数据安全保护制度与国家标准与技术研究院制定的标准和指导原则

相一致。

（二）战略目标 3.2：推动安全物联网设备的发展

政府将按照《2020 年物联网网络安全改进法案》的指示，通过联邦研发（R&D）、采购和风险管理工作，持续改善物联网网络安全。此外，政府也将按照第 14028 号行政命令“改善国家网络安全”的指示，继续推进物联网安全标签计划的开发。通过推广物联网安全标签，消费者将能够比较不同的物联网产品所提供的网络安全保护，从而创造一种市场激励机制，让整个物联网生态体系更加安全。

（三）战略目标 3.3：让提供不安全软件产品和服务的实体承担责任

一是，政府将与国会和私营部门合作，立法规定软件产品和服务的责任。任何此类立法都应防止具有市场支配力的制造商和软件发行商通过合同完全免除责任，并为软件的特定高风险场景制定更高的注意义务标准。**二是**，为制定安全软件开发的注意义务标准，政府将推动制定一个可调节的免责框架，以保护那些安全开发和维护其软件产品和服务的企业免于承担责任。**三是**，为进一步鼓励采用安全软件开发实践，政府将鼓励跨技术门类、跨行业协调的漏洞披露；促进软件物料清单的进一步发展；开发一个流程来发现和减轻被广泛使用或支持关键基础设施的软件所

带来的风险。**四是**，通过与私营部门和开源软件社区合作，联邦政府还将继续投资于安全软件的开发，包括内存安全语言和软件开发技术、框架和测试工具。

（四）战略目标 3.4：利用联邦拨款和其他激励措施加强安全投入

政府将与 SLTT 实体、私营部门和其他合作伙伴合作，通过技术援助和其他形式的支持平衡申请人的网络安全需求。推动对设计上具有安全性和韧性的关键产品和服务的投资，并在关键基础设施的整个生命周期维持和激励安全性和韧性。联邦政府还将优先为旨在加强关键基础设施网络安全和韧性的网络安全研究、开发和演示（RD&D）项目提供资金。

（五）战略目标 3.5：利用联邦采购机制来改进问责制

对联邦政府供应商的合同要求一直是提升网络安全的有效手段。第 14028 号行政命令“改善国家的网络安全”要求加强和标准化联邦机构的网络安全合同要求。政府将继续尝试通过采购来制定、执行和测试网络安全要求的新概念，进而带来新颖且可扩展的方法。

（六）战略目标 3.6：探索联邦网络保险的保障机制

在灾难性事件发生之前构建应对机制，而不是在事件发生后匆忙制定一揽子援助计划，可以为市场提供确定性，并使国家更

具韧性。政府将评估联邦保险应对灾难性网络事件的需求和可能的结构，支持现有的网络保险市场

五、支柱四：投资于有韧性的未来

美国将通过战略投资和协调合作的行动，建立一个更安全、更有韧性、更保护隐私、更公平的数字生态系统，具体包括六项举措。

（一）战略目标 4.1：保护互联网的技术基础

要维护和拓展开放、自由、全球化、可互操作、可靠和安全的互联网，需要持续参与标准的制定过程，以融入美国的价值观，确保技术标准能够带来更安全和有韧性的技术。美国将与行业领袖、国际盟友、学术机构、专业协会、消费者团体和非营利组织合作，以确保新兴技术的安全、实现互操作性、促进全球市场竞争，并保护美国的国家安全和经济优势。

（二）战略目标 4.2：重振联邦网络安全研发

借助联邦的力量，优先研发可防御且有韧性的架构，并减少基础技术的漏洞，是联邦网络安全研究和发展战略计划中重要的内容。联邦政府将加强研发和示范（RD&D）社区建设，积极预防和降低现有和下一代技术中的网络安全风险。各部门和机构将指导研发和示范项目，以推进关键基础设施所使用的人工智能、

运营技术和工业控制系统、云基础设施、电信、加密技术、系统透明度和数据分析等领域的网络安全性和韧性。

（三）战略目标 4.3：为美国未来的后量子做准备

联邦政府将优先推动脆弱公共网络和系统向量子加密环境过渡，并制定相应的缓解策略，以便在面对未来的未知风险时具备提供加密敏捷性的能力。私营部门应遵循政府的模式，为美国未来的后量子准备自己的网络和系统。

（四）战略目标 4.4：确保未来的清洁能源安全

政府将协调联邦政府、产业以及州、地方、部落和属地各利益相关方的工作，部署安全、可互操作的电动汽车充电器网络、零排放充电基础设施以及零排放公共交通和校车。能源部还将与行业、州、联邦监管机构、国会和其他机构合作，持续促进配电和分布式能源资源的网络安全。

（五）战略目标 4.5：支持数字身份生态体系的发展

联邦政府将鼓励并支持对强大、可验证的数字身份解决方案的投资，以加强和保护个人隐私、公民权利和公民自由；防止意外后果、偏见和潜在的滥用；允许个人选择供应商和自愿使用；提高安全性和互操作性；促进包容性和可及性；以及完善技术和个人数据使用的透明度和问责制。

（六）战略目标 4.6：制定国家战略加强网络安全人才储备

增加网络教育和培训的获取途径，不断扩充网络人才队伍，解决经济部门对网络安全专业知识的需求，解决公共部门在招聘、留住和发展人才与能力方面面临的独特挑战，进而满足保护联邦数据和信息技术基础设施的要求。

六、支柱五：建立国际伙伴关系以追求共同目标

美国将致力于建立一个由各国组成的广泛联盟，维护一个开放、自由、全球、可互操作、可靠和安全的互联网，具体包括五项举措。

（一）战略目标 5.1：建立联盟来对抗对数字生态系统的威胁

美国将召集志同道合的国家、国际商界和其他利益攸关方，推进建设互联网未来愿景，促进安全和可信的数据流动，联合应对更广泛的潜在安全挑战。美国将与其盟友和伙伴合作，为数字时代制定新的协作执法机制。例如，欧洲网络犯罪中心在推动法律框架现代化、培训执法人员、改进溯源、与私营部门伙伴合作，以及应对欧洲的恶意网络活动方面发挥了重要作用。为了扩大这种模式，美国将支持与其他地区的合作伙伴建立类似的有效枢纽。

（二）战略目标 5.2：加强国际合作伙伴的能力

美国将调集各公共和私营部门以及先进地区合作伙伴的专业知识，开展协调有效的国际网络能力建设和业务合作。在执法领域，司法部将继续通过双边和多边接触以及协议、正式和非正式合作，提供国际和区域领导，建立更强大的网络犯罪合作模式。国防部将继续加强与各国军方之间关系，以获取盟友和伙伴的独特技能和视角，同时帮助其建设自身能力，为美国的集体网络安全态势做出贡献。

（三）战略目标 5.3：扩大美国援助盟友和伙伴的能力

推动美国与遭受重大网络攻击的盟国和合作伙伴合作，帮助其调查、应对和从此类事件中快速恢复。例如，美国正在领导北约（NATO）努力建立虚拟的网络事件支持能力，以便盟友在应对重大恶意网络活动时能够更有效地相互支持。

（四）战略目标 5.4：建立联盟以加强负责任的国家行为的全球规范

与盟友和伙伴合作，发表协调一致的声明，对违反规定的政府进行外交谴责，并同时施加外交孤立、经济惩罚、反网络和执法行动、法律制裁等相应的后果进行威慑。

（五）战略目标 5.5：为信息、通信和运营技术产品和服务提供安全的全球供应链

美国将与盟友和伙伴合作，通过 IPEF、四方关键和新兴技术工作组以及 TTC 等区域伙伴关系，实施跨境供应链风险管理的最佳做法，努力将供应链转移到伙伴国家和值得信赖的供应商。

七、《国家网络安全战略》实施策略

（一）评估成效

在实施本《战略》时，美国将评估所开展的投资行为、美国的实施进展，以及这些措施的最终结果。国家网络总监办公室将与国家安全委员会、行政管理和预算局等各机构进行协调合作，并每年向总统、总统国家安全事务助理和国会报告本战略、相关政策和后续行动在实现目标方面的效果。

（二）吸取经验教训

联邦政府将优先吸取从网络事件中获得的经验教训，并将这些经验教训应用在本《战略》的实施过程中。例如，2022 年夏，网络安全审查委员会完成了对 Log4j 漏洞的首次审查，并根据审查过程中的发现，向产业界、联邦机构和软件开发社区提供了明确、可操作的建议。在网络安全审查委员会结束审查工作后，联邦政府可通过适当的行政措施来优化自身的运行，进而落实委员会的建议，必要时可与国会合作以加强相关权力。

除了网络安全审查委员会以外，还需要更广泛的国家行动来

从网络事件中学习。比如，美国鼓励监管机构在监管框架中纳入事件审查流程，也鼓励网络安全和基础设施安全局以及执法机构建立流程，定期从调查和事件应对活动中吸取经验教训。此外，美国也鼓励私营企业进行上述审查，并分享他们的成果，以体现本《战略》的有效实施。

（三）推动投资

维护开放、自由、全球化、可互操作、可靠和安全的互联网，并建立更具防御能力和韧性的数字生态体系，将需要联邦政府、盟友和合作伙伴以及私营部门划时代的投资。本《战略》中包含的许多联邦行动，旨在增加私营部门在安全、韧性、改进合作以及研发方面的投资。就联邦机构而言，若要支持私营部门合作伙伴并提高其执行重大联邦任务的能力，将需要有针对性的投资。为指导这类投资，国家网络总监办公室以及行政管理和预算局将联合向各部门和机构发布关于网络安全预算优先事项的年度指导意见，以推进政府的战略方针。国家网络总监办公室将与行政管理和预算局合作，确保各部门和机构预算提案的一致性，以实现本《战略》中规定的目标。本届政府将与国会合作，为网络安全活动拨款，以紧跟网络生态体系的内在变化速度。