

2025 年 9 月 1 日

第 36 期

总第 711 期

赢得人工智能竞赛：美国人工智能行动计划

【译者按】今年 7 月，美国白宫办公室发布《赢得人工智能竞赛：美国人工智能行动计划》。该计划聚焦创新、基础设施、国际外交与安全等三大支柱，涵盖 90 多项具体行政命令，凸显美国在人工智能领域“争夺全球主导权”的战略意图，包括破除监管壁垒、保障 AI 契合美国价值观与言论自由、向盟友输出 AI 技术、抵制中国在国际 AI 治理的影响、加强算力与半导体出口管控、协调全球技术保护等，以此确保美国领先地位，抢占经济与军事利益。赛迪智库信息化与软件产业研究所、电子信息研究所、知识产权研究所、安全产业研究所、节能工业与环保研究所对该计划进行了编译，期望对我国有关部门有所帮助。

【关键词】人工智能 竞赛 创新 治理

引言

美国正投身于人工智能（AI）全球主导权的争夺战。特朗普总统上任伊始便签署了第 14179 号行政令——《消除美国在人工智能领域领导地位的障碍》，呼吁美国在这场全球竞赛中保持领先，并下令制定 AI 行动计划。

美国人工智能行动计划的三大支柱是：创新、基础设施，以及国际外交与安全。美国需在各领域加快创新步伐、拓展创新广度，在人工智能新技术的研发与应用上赶超竞争对手，同时破除阻碍私营部门创新的不必要监管壁垒。美国需要建设并维护庞大的人工智能基础设施及配套能源体系。为此，特朗普政府将继续抵制激进气候教条与官僚主义繁文缛节，要“大干快上，全力建设”，将美国人工智能打造为全球人工智能的黄金标准，并确保其盟友都依托美国技术开展建设。

这三大支柱贯穿以下几项原则。第一，美国工人是特朗普政府人工智能政策的核心。本届政府将确保本国工人及其家庭从这场技术革命创造的机遇中获益。人工智能基础设施建设将为美国工人带来高薪岗位，而人工智能在医疗、制造业等众多领域实现的突破，将提升全体美国人的生活水平。人工智能将通过辅助而非取代人类工作，改善美国人的生活。第二，人工智能系统必须

摒弃意识形态偏见。当用户寻求事实信息或分析时，系统设计应以追求客观真理为目标，而非服务于社会工程议程。人工智能系统正成为不可或缺的工具，深刻影响着美国人获取信息的方式，同时也必须值得信赖。最后，我们必须防止先进技术遭恶意行为者滥用或窃取，同时监测人工智能带来的新兴及不可预见风险。这需要我们时刻保持警惕。

支柱一：加速人工智能创新

美国需拥有全球最强 AI 系统并引领其创新应用，联邦政府应助力私营部门主导的创新蓬勃发展。

消除繁文缛节与繁重监管

为保 AI 全球领先，美国私营部门需摆脱官僚束缚。特朗普已采取举措，如撤销拜登政府 AI 第 14110 号行政令，联邦不向设繁琐 AI 法规、浪费资金的州拨付相关资金，但不干涉各州通过审慎且不阻碍创新的法律。

建议的政策行动

- 科学技术政策办公室（OSTP）牵头，向企业与公众征集信息，梳理阻碍 AI 创新应用的联邦法规，联合相关机构施策。
- 管理和预算办公室（OMB）牵头，依 2025 年 1 月 31

日第 14192 号行政令，协同联邦机构排查、修订或废止不必要阻碍 AI 研发应用的各类文件。联合设 AI 自主资金项目的联邦机构，确保资金分配时考量各州 AI 监管环境，对监管可能影响资金效用的州限制拨款。

- 联邦通信委员会（FCC）牵头，评估各州 AI 法规是否妨碍其履行 1934 年《通信法》义务与职权。
- 审查上届政府启动的联邦贸易委员会（FTC）调查，确保其责任认定理论不过度负担 AI 创新；同时审查 FTC 各类令文，适时修改或撤销不当负担 AI 创新的文件。

确保前沿人工智能保护言论自由和美国价值观

前沿 AI 将深刻影响教育、工作及媒体消费，其设计需融入言论自由，美政府政策不得干扰。需保障 AI 时代言论自由，且联邦采购 AI 需客观反映真相，不服务社会工程议程。

建议的政策行动

- 商务部（DOC）借国家标准与技术研究院（NIST）牵头，修订 NIST AI 风险管理框架，删除错误信息、多样性、公平性与包容性及气候变化相关内容。
- 更新联邦采购指南，确保政府仅与能保障系统客观、无自上而下意识形态偏见的前沿大型语言模型（LLM）开发者合作。

- 商务部借 NIST 人工智能标准与创新中心（CAISI）牵头研究，酌情发布中国前沿模型评估报告，审查其与中国共产党论调及审查制度的一致性。

鼓励开源与开权重人工智能

开源和开放权重 AI 模型供全球免费下载修改，对创新价值独特：初创企业无需依赖封闭供应商，企业与政府可处理敏感数据，学术研究需其开展严谨实验。

美国需拥有符合自身价值观的领先开放模型，这具有地缘战略价值，联邦政府应为开放模型营造支持性环境。

建议的政策行动

- 完善算力金融市场，保障初创与学术界获大规模算力，联邦联合商务部 NIST、OSTP、NSF 的 NAIRR 与行业合作。NAIRR 试点与领先科技企业合作，助科研界获私营部门的计算、模型、数据及软件资源，并接入更多科研人员与教育工作者。
- 为 NAIRR 打造精简可持续运营基础，接入 OSTP 牵头发布新版《国家 AI 研发战略计划》，指导联邦 AI 研究投入，推动下一代 AI 突破。
- 商务部 NTIA 召集利益相关方，推动中小企业采用开源及开放权重模型。

推动人工智能的广泛应用

如今释放 AI 潜力的瓶颈在于应用范围窄、落地慢。美国医疗等关键行业技术落地滞后，因缺技术信任/了解、监管复杂、治理与风险标准不明，联邦统筹可助 AI 在全美产业“先行先试”。

建议的政策行动

- 全国建监管沙盒与 AI 卓越中心，供各方快速部署测试 AI 工具并共享数据成果，由 FDA、SEC 等主导，商务部借 NISTAI 评估项目支持。
- 商务部 NIST 牵头，在医疗、能源、农业等领域联合多方，加快 AI 系统国标制定推广，同时评估 AI 生产力提升效果。
- 国防部协同 ODNI，定期更新国防部与 IC 联合评估（对比美与对手 AI 工具采用水平），依评估结果调整双方 AI 采用计划。
- 情报界、DOE、商务部 AI 标准与创新中心、NSC、OSTP 合作，优先收集共享影响国安的外国前沿 AI 项目情报。

在人工智能时代赋能美国工人

特朗普政府支持工人核心的 AI 议程。AI 可提升生产力、催生新产业并为劳动者创机遇，但也会改变工作模式，需助其平稳过渡。政府已发 2025 年 4 月第 14277、14278 号行政令（《推动

美国青少年 AI 教育发展》《为美国人未来高薪技能岗位做好准备》），后续将优先扩 AI 知识技能培养、评估其对劳动力市场影响、试点再培训。

建议的政策行动

- 劳工部（DOL）、教育部（ED）、国家科学基金会及商务部牵头，将 AI 技能培养列为相关资金项目核心，融入职业技术教育（CTE）、劳动力培训、学徒制等联邦资助项目。
- 财政部牵头明确 AI 素养技能项目可纳入《国内税收法典》第 132 条合格教育援助范畴，允许雇主提供免税培训补偿，扩大私营部门 AI 技能投入。
- 劳工统计局（BLS）与商务部联合，借人口普查局、经济分析局（BEA）现有数据，研究 AI 对劳动力市场影响，分析其对就业、岗位替代及工资的作用。
- 劳工部设 AI 劳动力研究中心，联合相关机构持续评估 AI 对劳动力市场及劳动者的影响，定期发报告、做情景规划并提建议，为政策制定提供依据。
- 劳工部酌情用现有资金资助 AI 相关失业者快速再培训，指导各州确定合格失业工人，明确快速反应资金用于提升风险工人技能的方式。

- 劳工部与商务部试点应对 AI 劳动力挑战的举措（如再培训、入门岗位技能适配），依托现有法案授权，推出可扩展、重绩效的策略，助劳动力系统适应市场变化。

支持下一代制造业

AI 将为物理世界带来新创新（如自主无人机、自动驾驶汽车、机器人技术）。美国及盟友需成这些下一代技术的世界级制造商，AI 等技术为制造与物流带来创新契机（含国防安全技术），联邦政府应优先投资以引领工业复兴。

建议的政策行动

- 通过国防部、商务部、能源部、国家科学基金会等机构，依托小企业创新研究计划、小企业技术转让计划、科研补助金、CHIPS 研发计划、相关法案授权及其他交易授权等渠道，投资开发推广基础及转化型制造业技术。
- 商务部授权国家电信技术和信息管理局牵头，联合行业与政府，梳理美国机器人及无人机制造业供应链瓶颈。

投资于人工智能驱动的科学研究的

AI 将改变科学研究，已突破蛋白质结构、新型材料生成模型，通用模型在提假设、设计实验上潜力巨大。但科研方式需要重大变革，否则 AI 预测价值有限。AI 时代需投入更多促进理论转工业化，并需建新型基建、支持新型科研组织。

建议的政策行动

- 联合国家科学基金会（NSF）、能源部（DOE）、商务部国家标准与技术研究院（NIST）等，投资工程、材料、化学等多领域自动化云实验室，由私营、联邦、研究机构及 DOE 国家实验室协作打造。
- 以长期协议支持研究组织，助力其用 AI 等技术突破基础科学。
- 评审新项目提案时，纳入过往资助项目的科学与工程数据集影响评估，激励公开高质量数据。要求联邦资助研究者，披露研究中供 AI 使用的非专有、非敏感数据集。

建设世界一流的科学数据集

高质量数据已成为国家战略资产，其他国家在海量科学数据积累方面已领先我们。美国必须牵头打造全球规模最大、质量最高的人工智能适用科学数据集，同时尊重个人权利，保障公民自由、隐私及机密信息安全。

建议的政策行动

- 指示国家科学技术委员会（NSTC）机器学习与人工智能小组委员会，针对生物、材料科学、化学、物理等数据类型，制定 AI 模型训练最低数据质量标准建议。
- 颁布《2018 年保密信息保护和统计效率法案》要求的

关于可访问性推定及扩大安全访问范围的管理和预算办公室法规。

- 在国家科学基金会和能源部内部建立安全计算环境。
- 为美国国家科学基金会的国家安全数据服务（NSDS）示范项目创建在线门户。
- 由国家科技委员会牵头，联合美国农业部、能源部等单位，共同制定联邦土地生命全基因组测序计划。

推动人工智能科学本身的发展

人工智能未来的突破或许也会同样改变人工智能所能达成的成果。美国务必持续充当这类突破的领先开创者，而这要从对前沿最具前景的路径开展战略性、针对性投资起步。

建议的政策行动

- 优先对理论、计算及实验研究进行投入，以此维持美国在探寻可推动人工智能能力发展的全新且具变革性范式方面的领先地位。

投资于人工智能可解释性、控制性和稳健性方面的突破

模型的无法解释性导致特定人工智能系统的行为难以预测。进而导致在国防、国家安全等关乎生命安全的领域应用先进人工智能技术时面临重重挑战。

建议的政策行动

- 国防高级研究计划局牵头进行技术开发,以推进人工智能可解释性、人工智能控制系统和对抗鲁棒性研究。
- 在《国家人工智能研发战略计划》中,将人工智能可解释性、控制性和稳健性的基础研究进展列为优先事项。
- 国防部、能源部等应联合发起人工智能黑客松活动,重点关注透明度、有效性、使用控制及安全漏洞等方面。

建立人工智能评估生态系统

评估是人工智能行业衡量 AI 系统性能与可靠性的常用方式。在受监管行业,严格的评估可成为定义并衡量 AI 可靠性及性能的关键工具。随着时间推移,监管机构应探索如何在现有法律适用于 AI 系统时运用评估手段。

建议的政策行动

- 由商务部下属的国家标准与技术研究院发布相关指南和资源,开展 AI 系统评估。
- 支持人工智能模型测评科学的发展,此项工作由商务部下属国家标准与技术研究院牵头,联合能源部、国家自然科学基金会及其他联邦科研机构共同推进。
- 在商务部下属人工智能标准与创新中心的统筹下,每年至少召开两次会议,为联邦机构与研究界搭建交流平台,分享 AI 评估体系构建过程中的经验与最佳实践。

- 通过能源部和国家科学基金会投资建设 AI 测试平台，以便在安全的真实环境中对 AI 系统进行试点测试。
- 由商务部牵头组建国家标准与技术研究院人工智能联盟，推动各方协作建立新型测量科学。

加快政府内部人工智能的应用

借助人工智能工具，联邦政府可为公众提供效率更高、成效更佳的服务。人工智能的变革性应用有助于打造美国人民期望且应得的高效响应型政府。管理和预算办公室已通过减少拜登政府实施的繁琐规定，推动政府采用人工智能技术。

建议的政策行动

- 正式确立首席人工智能官委员会（CAIOC）为跨机构人工智能应用协调合作的主要平台。
- 在人事管理办公室的协助下，制定一项人才交流计划，允许联邦工作人员快速借调至其他需要专业人工智能人才（如数据科学家和软件工程师）的机构。
- 由总务管理局（GSA）协同管理和预算办公室，创建人工智能采购工具箱，以在切实可行的最大范围内促进联邦机构间的规范统一。
- 与 GSA 合作实施先进技术转让与能力共享计划，促进各机构间先进人工智能技术与应用案例的快速共享。

- 要求所有联邦机构在实际可行的范围内,确保前沿语言模型的员工都能使用此类工具并接受适当培训。
- 在管理和预算办公室的支持下,召集一批拥有高影响力服务提供商的机构,试点并推广人工智能应用。

推动国防部采用人工智能

人工智能有望改变国防部的作战行动与后勤办公,美国必须在武装部队中积极应用人工智能。鉴于国防部在联邦政府内的作战需求别具一格,理应采取专门政策措施推动人工智能的应用。

建议的政策行动

- 明确国防部人员大规模运用人工智能所需的人才与技能,并实施人才培养计划,以满足人工智能人才需求。
- 在国防部建立人工智能与自主系统虚拟试验场,首先确定这类设施所需的技术、地理、安全及资源需求范围。
- 在国防部内制定简化流程,对主要作战及支援职能涉及的工作流进行分类、评估与优化,列出优先通过人工智能实现自动化的工作流清单。某工作流成功实现自动化后,国防部应尽快将其永久转为人工智能实施模式。
- 国防部牵头与云服务提供商、计算基础设施运营商及其他相关私营部门实体达成协议,明确国家紧急情况下国防部对计算资源的优先使用权。

- 将高级军事学院打造为人工智能研发与人才培养中心。

保护商业和政府的人工智能创新

要维持美国在人工智能领域的领先地位，美国政府需与行业紧密协作，在前沿人工智能技术的传播与国家安全关切间恰当平衡。美国政府有效应对美国人工智能公司、人才、知识产权及系统所面临的安全风险也至关重要。

建议的政策行动

- 国防部、国土安全部、商务部的人工智能标准与创新中心及情报界其他合适成员牵头，与美国主要人工智能开发者开展合作，助力私营部门积极守护人工智能创新。

在法律体系中打击合成媒体

在音频、视频或照片等领域的恶意深度伪造技术是人工智能一大风险。为应对该风险采取进一步行动。

建议的政策行动

- 由商务部国家标准与技术研究院牵头，考虑将其“法医证据守护者”深度伪造评估项目升级为正式指南，并配套制定自愿性法医基准。
- 司法部（DOJ）牵头探索采用类似《联邦证据规则》第901（c）条拟议稿的深度伪造标准。

由司法部法律政策办公室牵头，就《联邦证据规则》中所有

与深度伪造相关的拟议增补内容提交正式意见。

支柱二：构建美国人工智能基础设施

人工智能促使美国要构建远超当下规模能源发电量。自 20 世纪 70 年代起，美国能源产能便陷入停滞，而中国却快速完善了自身电网。美国要达成人工智能主导地位，就得改变这一态势。

为数据中心、半导体制造设施和能源基础设施设立简化审批流程，并确保安全

人工智能发展需要芯片制造厂、数据中心，以及供能的新能源设施，然而美国的政策法规严重制约了这类基础设施的建设速度。目前，特朗普已推动《国家环境政策法》改革，启动许可技术现代化项目，成立国家能源主导委员会（NEDC），并推出美国投资加速器计划。

建议的政策行动

- 依据《国家环境政策法》设立新的分类排除条款，以覆盖通常不会对环境造成重大影响的数据中心建设活动。
- 扩大 FAST-41 流程的适用范围，将 2015 年《修复美国地面交通法案》中所有符合条件的数据中心及数据中心能源项目纳入其中。
- 研究为数据中心制定全国统一环保许可的必要性。若必

要，需确保该许可无需提交施工前通知，并涵盖与现代人工智能数据中心规模一致的开发场地。

- 通过精简或放宽《清洁空气法》《清洁水法》《综合环境响应、赔偿与责任法》及其他相关法律项下的法规要求，加快环境许可审批进程。
- 指示拥有大量土地资源的联邦机构筛选适合大规模开发的场地用于建设数据中心及其配套发电基础设施。
- 建立安全防护机制，防止对手向此类基础设施植入敏感数据。确保国内人工智能计算体系基于美国产品构建。
- 扩大人工智能在环境审查中的应用，加快审查进程并提升审查质量，

建设与人工智能发展速度相匹配的电网

电气化推进与人工智能技术进步带来的用电需求持续攀升，使电网承受的压力与日俱增。美国必须制定全面战略，推动电网升级扩容。

建议的政策行动

- 全力稳定现有电网，保护存量资产，保障电力持续稳定供应且价格可负担。美国需避免关键发电设施过早退役，探索现有产能的创新利用方式。确保电网全域符合全国统一的资源充裕度标准，保障电力供应持续充足。

- 优化现有电网资源，提高输电系统的效率和性能。美国探索应用先进的电网管理技术，升级输电线路，增加现有线路的输电容量。美国还应研究新方法，引导大型电力用户在电网关键时期管理用电，释放更多电力潜力。
- 优先推动可靠、可调度电源的快速互联，在技术前沿积极应用新能源发电。改革电力市场，使财政激励与电网目标相契合，确保发电投资能够切实反映系统需求。
- 制定战略蓝图，通过稳定当前电网、优化现有资源、建设未来电网，以应对 21 世纪复杂的能源形势。

恢复美国半导体制造能力

如今，美国必须让半导体制造业回归本土。重振后的美国芯片产业将创造数千个高薪岗位，巩固本国的技术领先地位，并保护供应链免受外国竞争对手的干扰。

建议的政策行动

- 由 CHIPS 计划办公室牵头，取消 CHIPS 资助的半导体制造业项目的所有额外政策要求。商务部及其他相关联邦机构应简化阻碍半导体制造业发展的法规。
- 由商务部牵头，审查半导体领域的补助金与研究计划，加快将先进人工智能工具融入半导体制造业的进程。

为军方和情报部门建设高安全级别的数据中心

人工智能系统可能会被用于处理美国政府的部分高度敏感数据。部署这些模型的数据中心必须能够抵御最坚决、最具实力的国家行为体发起的攻击。

建议的政策行动

- 国防部、情报界、国家安全委员会及商务部国家标准与技术研究院牵头,联合行业力量与相关联邦资助研发中心,为高安全性人工智能数据中心制定新的技术标准。
- 推动各机构采用分类计算环境,支持可扩展且安全的人工智能工作负载。

培养建设人工智能基础设施所需的技术劳动力

美国需投资培养负责人工智能基础设施建设、运营与维护的劳动力。针对人才短缺问题,政府应明确该领域的重点岗位,构建现代化技能体系,支持行业主导的培训项目,并通过普通教育、职业技术教育及注册学徒制拓宽早期人才培养渠道。

建议的政策行动

- 由劳工部与商务部牵头,启动全国性计划,明确人工智能相关基础设施建设所需的重点职业。联合雇主、行业协会及其他相关方,制定或完善国家技能框架与能力标准,为课程设置、资质认证及劳动力投资方向提供参考。
- 通过劳工部、能源部、教育部、国家科学基金会及商务

部，联合州和地方政府及劳动力系统相关方，支持开发行业主导的培训项目。由雇主与培训方共同设计，确保学员结业即可上岗，并能直接对接招聘流程。激励雇主提升员工技能，助其转向优先职业。商务部应将这些培训模式纳入基础设施投资项目，并优先资助能够弥补人才缺口、培养契合雇主需求人才的项目。

- 在劳工部、教育部与国家科学基金会的牵头下，联合教育及劳动力系统的利益相关方，拓展早期职业体验项目与学徒前培训，吸引初高中生接触人工智能基础设施领域的优先职业。
- 教育部职业技术与成人教育办公室应指导各州及地方职业技术教育系统，调整学习计划以适配人工智能基础设施优先职业的要求。
- 在劳工部主导下，推广注册学徒制。简化优先发展产业及相关职业中新项目的启动流程，消除雇主参与的障碍，如简化注册手续、扶持中介机构，以及确保项目设计贴合雇主需求。
- 由美国能源部牵头，依托其国家实验室的人工智能专业知识与技术能力，为本科生、研究生、博士后及教育工作者拓展实践研究培训与发展机会。同时，与社区学院

及技术/职业院校合作，培养新劳动力，并助力现有劳动者转型，以填补关键人工智能岗位的空缺。

加强关键基础设施的网络安全

网络及关键基础设施在运用人工智能时也面临对抗性威胁。因此，在安全关键领域或国土安全相关应用中使用人工智能时，必须采用安全设计的、稳健且具备弹性的系统，能够监测性能变化，并对数据投毒、对抗性样本攻击等潜在恶意行为发出警报。

建议的政策行动

- 国土安全部牵头，联合商务部的人工智能标准与创新中心及国家网络总监办公室，成立人工智能信息共享与分析中心（AI-ISAC），推动人工智能安全威胁信息与情报的共享。国土安全部制定并更新针对私营部门的指导文件，协助其修复和应对人工智能特有的漏洞与威胁。
- 确保联邦机构掌握的人工智能漏洞信息，通过协作整合机制与私营部门共享。

推动“安全即设计”的人工智能技术与应用

人工智能系统易受某些对抗性输入的干扰，美国政府应推动弹性强、安全性高的人工智能开发与部署，抵御虚假或恶意输入。

建议的政策行动

- 由国防部牵头，与商务部国家标准与技术研究院及国家

情报总监办公室合作,持续完善国防部的负责任人工智能和生成式人工智能框架、路线图及工具包。

- 由国家情报总监办公室牵头,与国防部及商务部人工智能标准与创新中心协商,依据《第 505 号情报界指令》,发布有关人工智能保障的情报界标准。

提升联邦政府应对人工智能事件的能力

人工智能的普及必须确保系统一旦发生故障,能够最大程度降低对关键服务或基础设施的影响,并迅速启动应对措施。为此,美国政府应推动人工智能事件响应行动的发展,并将其纳入现有的公共和私营部门事件响应原则及最佳实践中。

建议的政策行动

- 由商务部国家标准与技术研究院牵头,联合人工智能和网络安全行业,确保人工智能被纳入事件响应团队的标准制定、响应框架、最佳实践及技术能力中。
- 修订网络安全与基础设施安全局的《网络安全事件与漏洞响应手册》,将人工智能系统纳入考量范围,并要求首席信息安全官必要时与首席人工智能官、高级机构隐私官员、商务部人工智能标准与创新中心及其他相关机构官员进行协商;各机构应相应更新其下属手册。
- 国防部、国土安全部和国家情报总监办公室牵头,协同

科学技术政策办公室、国家安全委员会、管理和预算办公室及国家网络总监办公室，共享人工智能漏洞信息。

支柱三：引领国际人工智能外交与安全

要在全球人工智能竞争中胜出，美国必须利用其在数据中心建设、计算硬件性能和模型方面的领先优势建立持久的全球联盟，同时防止对手坐享这些创新与投资成果。

向盟友与伙伴输出美国人工智能

美国必须通过向其盟友国家出口包括硬件、模型、软件、应用及标准的人工智能技术栈，以实现美国 AI 技术的全球推广与普及，并阻止美国盟友依赖竞争对手的技术。

建议的政策行动

- 在商务部内设立专项计划，征集行业联盟关于全栈人工智能出口方案的提案，并协同经济外交行动小组、美国贸易发展署、进出口银行、美国国际开发金融公司及国务院需与商务部商讨选定的提案，推动达成符合美国批准的安全要求和标准的交易。

抵制中国在国际治理机构中的影响力

联合国、经济合作与发展组织、七国集团、二十国集团等国际机构已提出人工智能治理框架和发展战略。美国支持理念相近

的国家合作，鼓励以共同价值观发展人工智能。但多数 AI 监管措施与美国价值观相悖或受到中国企业的影响。

建议的政策行动

- 由国务院和商务部牵头，凭借美国在国际外交及标准制定组织中的地位，推动促进创新、反映美国价值观的国际 AI 治理方案。

加强人工智能算力出口管制

美国应该创新出口管制方式，阻止竞争对手获取先进 AI 算力是地缘战略竞争的关键，也是国家安全的保障。

建议的政策行动

- 由商务部、白宫科技政策办公室和国家安全委员会牵头，与业界合作，探索利用先进人工智能算力芯片位置验证功能，确保该类芯片不流入受关注国家。
- 由商务部牵头，与情报界开展合作，监控人工智能算力领域的新兴技术发展，确保全面覆盖可能存在芯片转移行为的国家或地区。强化对高风险国家的监控，降低这些国家转移美国原产先进人工智能计算设备的风险。

堵塞现有半导体制造出口管制的漏洞

美国及其盟友在半导体制造产业链的关键组件和工艺上近乎垄断。美国必须继续以开创性研究和新型发明引领全球半导体制

制造业，但也必须防止对手以危害国家安全的方式使用这些创新成果来达成其自身目的。这需要采取新的措施填补现有半导体制造业出口管制的漏洞，并辅以强化的执法手段。

建议的政策行动

- 由美国商务部牵头，针对半导体制造子系统制定新出口管制措施。目前，美国及其盟友已对半导体制造主要系统实施出口管制，但尚未对许多组件子系统加以管控。

全球协调保护措施

美国必须对敏感技术实施严格的出口管制，并应鼓励合作伙伴及盟友遵循其管制措施，不得补位。若盟友违规定，美国应运用外国直接产品规则和次级关税等工具来实现更大的国际协调。

建议的政策行动

- 商务部与国务院牵头，协同国家安全委员会、能源部及国家科学基金会，制定、实施和共享互补性技术保护措施的相关信息，降低来自战略对手及相关实体的风险。
- 国务院牵头，协同商务部、国防部和能源部，制定人工智能全球联盟技术外交战略计划，旨在确保盟友不会向对手提供拟实施出口管制的技术。
- 拓展新举措以促进人工智能技术栈的多边管制，平衡美国与盟友的管制措施之间的竞争环境。

- 商务部与国防部牵头，协同盟友确保其采纳美国的出口管制措施，与美国共同制定新管控措施，并禁止对手向其国防工业基地供货或获得国防供应商的控股权。

确保美国在前沿模型的国家安全风险评估方面处于领先地位

人工智能系统可能新的国家安全风险，涉及网络攻击、化生放核爆（CBRNE）武器开发以及新的安全漏洞。美国 AI 前沿模型中存在的风险，或可预示外国对手可能掌握的技术水平。

建议的政策行动

- 人工智能标准与创新中心牵头，联合其他具备 CBRNE 与网络风险相关专业知识的机构，与前沿人工智能开发者合作，共同评估前沿人工智能系统的国家安全风险。
- 人工智能标准与创新中心牵头，协同国家安全机构，评估在关键基础设施及其他领域使用对手人工智能系统可能引发的安全漏洞及其他恶意的可能性。
- 优先在国家标准与技术研究院和人工智能标准与创新中心、能源部、国防部及情报界等联邦机构招募顶尖人工智能研究人员，确保联邦政府能够持续对人工智能系统开展前沿性评估与分析。
- 人工智能标准与创新中心应与国家安全机构及相关研究机构合作，构建、维护并在必要时更新国家安全领域

的人工智能评估体系。

投资生物安全

人工智能可能成为恶意行为者合成有害病原体及其他生物分子的新工具。应对这一问题需采取多层级策略，既要筛查恶意行为者，也要辅以新工具与基础设施来实现更有效的筛查。同时必须协同盟友及合作伙伴，推动这些措施在国际层面落地。

建议的政策行动

- 所有接受联邦科研资助的机构，须使用具备完善核酸序列筛查与客户验证程序的核酸合成工具及服务商。应为此类要求建立执法机制，而非依赖自愿申报。
- 白宫科技政策办公室牵头，组织政府和行业代表制定数据共享机制，促进核酸合成服务商间的信息互通，以识别潜在欺诈或恶意客户。
- 人工智能标准与创新中心应与国家安全机构及相关研究机构合作，构建、维护并在必要时更新国家安全领域的人工智能评估体系。

译自：*Winning the Race: AMERICA'S AI ACTION PLAN*

译文作者：赛迪工业和信息化研究院 董永亮 李嘉鑫 牛家祺
牛堃瑛 谭力 曹智超 于晓丹

联系方式：15620533135
电子邮件：lijiaxin@ccidthinktank.com

咨询翘楚在这里汇聚

规划研究所

工业经济研究所

电子信息研究所

集成电路研究所

产业政策研究所

科技与标准研究所

知识产权研究所

世界工业研究所

无线电管理研究所

信息化与软件产业研究所

军民融合研究所

政策法规研究所

安全产业研究所

网络安全研究所

中小企业研究所

节能与环保研究所

材料工业研究所

消费品工业研究所

编辑部：工业和信息化部赛迪研究院

通讯地址：北京市海淀区万寿路27号院8号楼12层

邮政编码：100846

联系人：王 乐

联系电话：010-68200552 13701083941

传 真：010-68209616

网 址：www.ccidwise.com

电子邮件：wangle@ccidgroup.com

报：部领导

**送：部机关各司局，各地方工业和信息化主管部门，
相关部门及研究单位，相关行业协会**

编辑部：赛迪工业和信息化研究院

通讯地址：北京市海淀区紫竹院路 66 号赛迪大厦 8 层国际合作处

邮政编码：100048

联系人：袁素雅

联系电话：(010) 88559543 13263204219

传 真：(010) 88558833

网 址：www.ccidgroup.com

电子邮件：yuansuya@ccidthinktank.com

