

赢得竞赛：美国人工智能行动计划

2025 年 7 月

“今天，我们站在一场新的科学发现前沿，这场前沿由人工智能等变革性技术定义.....在这些领域取得的突破有可能重塑全球力量平衡，催生全新产业，并彻底改变我们的生活方式和工作方式。随着全球竞争对手竞相开发利用这些技术，确保美国在全球技术主导地位上无可争议且不可挑战，已成为国家安全当务之急。为了保障我们的未来，我们必须充分发挥美国创新的全部潜力。”

唐纳德·J·特朗普

美国第 45 任及第 47 任总统

目录

引言

支柱一：加速人工智能创新

消除繁文缛节和过度监管

确保前沿人工智能保护言论自由与美国价值观

鼓励开源与开放权重人工智能

推动人工智能应用，为人工智能时代美国工人赋能

支持下一代制造业

投资人工智能驱动的科学

建立世界级科学数据集

推进人工智能科学

投资人工智能可解释性、控制与鲁棒性突破

构建人工智能评估生态系统

加速政府采用人工智能

推动国防部采用人工智能

保护商业与政府人工智能创新

打击司法系统中的合成媒体

支柱二：建设美国人工智能基础设施

为数据中心、半导体制造设施和能源基础设施创建简化
许可程序并确保安全

开发匹配人工智能创新速度的电网

恢复美国半导体制造业

为军事与情报界建设高安全性数据中心

培养人工智能基础设施技能型劳动力

强化关键基础设施网络安全

推广安全设计人工智能技术与应用

促进成熟的联邦人工智能事件响应能力

支柱三：引领国际人工智能外交与安全

向盟友与伙伴出口美国人工智能

反制中国在国际治理机构中的影响力

加强人工智能计算出口管制执法

填补现有半导体制造出口管制漏洞

确保美国政府处于评估前沿模型国家安全风险的前沿

投资生物安全

引言

美国正处于赢得人工智能全球主导权的竞赛之中。谁拥有最庞大的人工智能生态系统，谁就将制定全球人工智能标准，并获得广泛的经济与军事利益。正如我们在太空竞赛中获胜一样，美国及其盟友必须在这场竞赛中胜出。特朗普总统在就职首日即签署第 14179 号行政命令《消除美国人工智能领导地位的障碍》，呼吁美国保持在此全球竞赛中的优势，并指示制定人工智能行动计划。

赢得人工智能竞赛将为美国人民开启人类繁荣、经济竞争力与国家安全的新时代。人工智能将使美国人能够发现新材料、合成新化学物质、制造新药，并开发新能源利用方法——这将引发工业革命。它将催生全新的教育、媒体和通信形式——信息革命。它还将实现全新的智力成就：解读曾经无法破译的古籍卷轴、在科学与数学理论领域取得突破、创造新型数字与实体艺术——这将是文艺复兴。

工业革命、信息革命与文艺复兴同时发生——这就是人工智能带来的潜力。摆在我们面前的机遇既鼓舞人心又令人谦卑。抓住机遇或错失机遇，选择权在我们手中。

美国人工智能行动计划包含三大支柱：创新、基础设施与国际外交与安全。美国需要在人工智能技术的开发与应用方面比竞争对手更快、更全面地创新，并拆除阻碍私营部门发展的不必要的监管壁垒。正如副总统万斯在 2025 年 2 月巴黎人工智能行动峰会上所言，“用繁重的监管限制人工智能发展不仅会不公平地影响现有企业.....还会使我们有史以来最具前景的技术之一陷入

瘫痪。”这就是特朗普总统在上任首日即撤销拜登政府危险的监管政策的原因。

我们需要建设和维护庞大的人工智能基础设施及其所需能源。为此，我们将继续摒弃激进的气候教条和官僚作风，正如本届政府自就职以来所做的那样。简而言之，我们需要“大力建设！”

我们需要确立美国人工智能——从先进半导体到模型再到应用——作为全球黄金标准，并确保盟友基于美国技术开发。

贯穿三大支柱的若干原则包括：

美国工人是特朗普政府人工智能政策的核心，政府将确保国民及其家庭从这场技术革命中获益。人工智能基础设施建设将为美国工人创造高薪岗位，医学、制造业等领域的突破将提升全体美国人的生活水平。政府相信人工智能将通过补充而非替代人类工作来改善生活。

人工智能系统必须免受意识形态偏见影响，在提供事实信息或分析时应追求客观真理而非社会工程议程。这些工具正在深刻塑造美国人获取信息的方式，但也必须是值得信赖的。

同时，必须持续的警惕、防范恶意行为者滥用或窃取先进技术，并监测人工智能可能产生的新兴和不可预见风险。

本行动计划明确了联邦政府近期需执行的政策目标。其目的是阐述本届政府可为美国人民实现全球人工智能主导愿景的具体政策建议。人工智能竞赛是美国必赢之战，本行动计划即是胜利路线图。

迈克尔·J·克拉特西奥斯（总统科学技术助理）

大卫·O·萨克斯（人工智能与加密货币特别顾问）

马可·A·鲁比奥（总统国家安全事务助理）

支柱一：加速人工智能创新

美国必须在人工智能系统的开发和应用领域成为全球领导者，同时消除阻碍私营部门创新的监管和繁文缛节。

1、消除繁文缛节和过度监管

为实现美国在人工智能领域的全球领导地位，美国私营部门必须摆脱官僚束缚。特朗普总统已采取多项措施，包括撤销拜登政府发布的第 14110 号行政命令（该命令设置了严格的监管框架）。人工智能在早期发展阶段不应被联邦或州政府层面的官僚主义扼杀。联邦资金不应流向那些因监管负担过重而影响资金有效性的州，但也不应干涉各州在不严重限制创新的前提下通过合理法律的权力。

政策行动建议

— 由科学技术政策办公室（OSTP）牵头，向企业及公众发起信息请求（RFI），调查当前哪些联邦法规阻碍人工智能创新与应用，并与相关联邦机构合作采取行动。

— 由管理和预算办公室（OMB）牵头，根据 2025 年 1 月 31 日发布的第 14192 号行政命令（《通过去监管化促进繁荣》），

协调各联邦机构识别、修订或废除阻碍人工智能开发或部署不必要的法规、备忘录、指导文件等。

— 由 OMB 牵头，与拥有人工智能相关自主资助项目的联邦机构合作，确保在符合法律的前提下，在资金分配时考虑各州的监管环境，对监管可能阻碍资金有效性的州，联邦则限制拨款。

— 由联邦通信委员会（FCC）评估州人工智能法规是否干扰其依据《1934 年通信法案》履行职责的能力。

审查联邦贸易委员会（FTC）对前一届政府期间启动的所有规则进行调查，确保其不提出对人工智能创新构成不当负担的责任理论；修改或撤销任何对创新造成过度负担的最终命令、法令或禁令。

2、确保前沿人工智能保护言论自由与美国价值观

人工智能系统将在教育、就业和媒体消费中发挥深远影响，必须从底层设计上保障言论自由，并确保联邦政府资助的系统客观反映真相而非社会工程议程。

政策行动建议

— 由商务部（DOC）通过国家标准与技术研究院（NIST）修订《NIST 人工智能风险管理框架》，删除其中涉及虚假信息、多样性、公平性与包容性（DEI）、气候变化的表述。

— 更新联邦采购指南，确保联邦政府仅与承诺其系统客观中立、无意识形态偏见的前沿大型语言模型（LLM）开发者签约。

— 由 DOC 通过 NIST 人工智能标准与创新中心（CAISI）开展研究，并发布评估报告，分析中国人工智能模型是否与中国共

产党的宣传口径及审查机制保持一致。

3、鼓励开源与开放权重人工智能模型

开源和开放权重 AI 模型应该给开发人员免费提供，供世界上任何人下载和修改。以这种方式分布的模型对创新具有独特的价值，因为初创公司可以灵活地使用它们，而不依赖于封闭的模型提供商。这样，开源和开放权重 AI 模型既免费提供给开发人员，也可供世界上任何人下载和修改。以这种方式分布的模型对创新具有独特的价值，因为初创公司可以灵活地使用它们，而不依赖于封闭的模型提供商。它们也有利于商业和政府采用人工智能，因为许多企业和政府都有敏感数据，无法发送给封闭的模型供应商。它们对于学术研究至关重要，学术研究通常依赖于获取模型的权重和训练数据来进行科学严谨的实验。

我们需要确保美国拥有基于美国价值观的领先开放模式。Open 源代码和开放权重模型可能成为全球某些商业领域和学术研究的全球标准。因此，它们也具有地缘战略价值。虽然是否以及如何发布开放式或封闭式模型的决定从根本上取决于开发人员，但联邦政府应该为开放式模型创造一个支持性的环境。它们也有利于商业和政府采用人工智能，因为许多企业和政府都有敏感数据，无法发送给封闭的模型供应商。它们对于学术研究至关重要，学术研究通常依赖于获取模型的权重和训练数据来进行科学严谨的实验。

政策行动建议

— 改善高性能计算市场，为初创企业和学术机构提供规模化算力。通过 NIST、OSTP 及国家科学基金会（NSF）的国家人工

智能研究资源（NAIRR）试点项目，推动算力金融市场的成熟。

- 与领先科技公司合作，通过 NAIRR 试点扩大中小企业对私有部门计算资源、模型、数据和软件的访问。

- 建立可持续的 NAIRR 运营能力，连接全国科研人员与教育工作者。

- 由 OSTP 牵头发布新版《国家人工智能研发战略计划》，指导联邦人工智能研发投入。

- 由 DOC 通过国家电信和信息管理局（NTIA）召集利益相关方，推动中小企业采用开源与开放权重模型。

4、推动人工智能应用

当前，利用人工智能全部潜力的瓶颈不一定是模型、工具或应用程序的可用性，而是人工智能应用范围有限和速度缓慢，特别是在大型、成熟的组织更是不足。由于各种因素，包括对技术的不信任或缺乏了解、复杂的监管环境以及缺乏明确的治理和风险缓解标准，美国许多最关键的行业，如医疗保健，在采用方面尤其缓慢。联邦政府的协调努力将有利于在整个美国工业界建立一种动态的、“先尝试”的人工智能文化。

政策行动建议

- 在 FDA、SEC 等监管机构的支持下，由 DOC 牵头建立全国性监管沙盒或人工智能卓越中心，允许快速部署和测试 AI 工具，并公开共享数据和结果。

- 由 NIST 牵头，在医疗、能源、农业等领域开展多利益相关方协作，制定人工智能系统国家标准，并评估其对任务生产力

发挥提升效果。

— 由国防部（DOD）与国家情报总监办公室（ODNI）定期更新美中及对手国家人工智能采纳水平的联合评估，并据此调整国防部和情报界的 AI 应用策略。

— 通过 IC、DOE、CAISI、NSC 和 OSTP 合作，优先收集可能影响国家安全的外国前沿 AI 项目的情报。

5、在人工智能时代赋能美国工人

特朗普政府支持工人优先的人工智能议程。通过提高生产力和创造全新的产业，人工智能可以帮助美国建立一个为美国工人提供更多经济机会的经济体。但它也将改变所有行业和职业的工作方式，要求组织机构做出认真的回应，帮助工人应对这一转变。特朗普政府已经在这方面采取了重大措施并发挥领导作用，包括 2025 年 4 月的第 14277 号（“推进美国青年的人工智能教育”）和第 14278 号（“让美国人为未来的高薪技术贸易工作做好准备”）行政命令。为了继续实现这一愿景，特朗普政府将推进一系列优先行动，扩大人工智能素养和技能发展，不断评估人工智能对劳动力市场的影响，并试点新的创新，以快速再培训并帮助工人在人工智能驱动的经济中茁壮成长。

政策行动建议

— 由劳工部（DOL）、教育部（ED）、NSF 和 DOC 牵头，将人工智能技能发展纳入职业与技术教育（CTE）、学徒制等联邦资助项目。

— 财政部将明确人工智能技能培训可享受《国内税收法典》第 132 条的教育费用税收抵免，鼓励企业投资员工培训。

- 由劳工统计局（BLS）和 DOC 通过人口普查局、经济分析局（BEA）研究人工智能对劳动力市场的影响，分析就业创造、替代和薪资效应。

- 在 DOL 下设立人工智能劳动力研究中心，持续评估人工智能对劳动力的影响，并生成政策洞察。

- 由 DOL 利用现有资金为受 AI 影响的失业工人提供再培训，并明确州政府如何使用“快速响应基金”支持高风险群体的技能升级。

- 在 DOL 和 DOC 试点新方法，解决 AI 引发的劳动力市场问题（如快速再培训和技能需求变化）。

6、支持下一代制造业

人工智能将在现实世界中实现广泛的新创新：自动驾驶无人机、自动驾驶汽车、机器人和其它尚不确定的发明。美国和我们值得信赖的盟友成为这些下一代技术的世界级制造商至关重要。人工智能、机器人技术和相关技术为制造和物流领域的新能力创造了机会，包括应用于国防和国家安全的能力。联邦政府应优先投资于这些新兴技术，并迎来新的工业复兴。

政策行动建议

- 通过 DOD、DOC、DOE、NSF 等机构的小企业创新研究（SBIR）计划、小企业技术转移（STTR）计划等，投资基础与应用制造技术。

- 由 DOC 通过 NTIA 召集行业与政府利益相关方，识别美国机器人和无人机制造的供应链挑战。

7、投资人工智能驱动的科学研究的

与许多其他领域一样，科学本身也将被人工智能所改变。人工智能系统已经可以生成蛋白质结构、新材料和其他许多东西的模型。越来越强大的通用模型在制定假设和设计实验方面显示出希望。这些新兴能力有望加速科学进步。然而，只有在科学实施方式发生重大变化，包括有利的科学基础设施的情况下，他们才会这样做。如果科学家不能扩大实验规模，那么人工智能支持的预测就没什么用了。今天的基础科学往往是一个劳动密集型的过
程；人工智能时代将需要更多的科学和工程研究，将理论转化为工业规模的企业。这反过来又需要新的基础设施和新型科学组织的支持。

政策行动建议

- 通过 NSF、DOE、NIST 等机构投资自动化云实验室，覆盖工程、材料科学、生物学等领域。
- 使用长期协议支持聚焦研究组织，推动基础科学突破。
- 通过科研数据披露激励机制，鼓励研究人员公开高质量数据集。
- 要求联邦资助的研究人员披露研究中使用的非敏感数据集。

8、建立世界级科学数据集

随着政府追求人工智能创新目标并利用该技术的经济效益，高质量数据已成为国家战略资产。其他国家，包括我们的对手，在积累大量科学数据方面已经领先于我们。美国必须领导创建世界上最大、质量最高的人工智能科学数据集，同时尊重个人权利，

确保公民自由、隐私和保密保护。

政策行动建议

— 由 NSTC 机器学习与人工智能小组委员会制定生物、材料科学等领域数据的最低质量标准。

— 推动《2018 年机密信息保护与统计效率法案》的实施，降低联邦数据访问壁垒。

— 在 NSF 和 DOE 建立安全计算环境，支持受控访问联邦数据的 AI 应用。

— 创建在线门户，提供联邦数据 AI 用例的公共访问入口。

— 探索建立联邦土地生命全基因组测序计划，为生物基础模型提供数据支持。

9、占据人工智能科学前沿

正如 LLM 和生成式人工智能系统代表了人工智能科学的范式转变一样，未来的突破也可能改变人工智能的可能性。美国必须继续成为此类突破的领先者，而这始于对前沿最有前景的道路进行战略性、有针对性的投资。

政策行动建议

在即将发布的《国家人工智能研发战略规划》中，优先投资理论、计算与实验研究，探索 AI 新范式。

10、加大投资实现人工智能可解释性、控制与稳健性的突破

如今，人们对前沿人工智能系统的内部运作知之甚少。技术人员知道 LLM 在高水平上是如何工作的，但往往无法解释为什么模型会产生特定的输出。这可能会使预测任何特定 AI 系统的行为

变得困难。反过来，这种缺乏可预测性的情况可能会使在国防、国家安全或其他危及生命的应用中使用先进的人工智能变得具有挑战性。如果我们在这些研究问题上取得根本性突破，美国将能够更好地在高风险的国家安全领域充分利用人工智能系统。

政策行动建议

- 由 DARPA 牵头，与 DOC 的 CAISI 和 NSF 合作，开发 AI 可解释性、控制系统和对抗鲁棒性技术。

- 将上述领域列为《国家人工智能研发战略计划》的重点方向。

- 由 DOD、DOE、CAISI、DHS、NSF 等机构联合举办 AI 黑客马拉松，测试系统的透明度、安全漏洞和可控性。

11、构建人工智能评估生态系统

评估是指人工智能行业对人工智能系统性能和可靠性的判断。严格的评估可以成为定义和衡量受监管行业人工智能可靠性和性能的关键工具。随着时间的推移，监管机构应探索在将现有法律应用于人工智能系统时使用评估。

政策行动建议

- 由 DOC 的 NIST 发布联邦机构评估 AI 系统的指南和资源，并支持评估科学的研发。

- 至少每年两次召开 CAISI 会议，分享联邦机构与研究社区在 AI 评估中的经验与最佳实践。

- 通过 DOE 和 NSF 投资 AI 测试平台，支持安全、真实场景下的 AI 系统原型开发。

— 由 DOC 牵头成立 NIST AI 联盟，推动跨机构合作建立可扩展的 AI 评估指标。

12、加速政府采用人工智能进度

人工智能工具的使用可使联邦政府更高效、更有效地为公众服务，如加速缓慢且通常是手动的内部流程，简化公共交互等。总的来说，人工智能的变革性使用可以帮助实现美国人民所期望和应得的高度响应的政府。

OMB 已经通过减少拜登政府强加的繁重规则，推动了政府对人工智能的采用。现在是巩固这一成功的时候了。

政策行动建议

— 将首席人工智能官理事会（CAIOC）正式化，协调跨机构 AI 应用，并与总统管理委员会、首席数据官理事会等机构合作。

— 创建联邦雇员人才交换计划，快速调配数据科学家等专业人才。

— 由 GSA 开发统一的 AI 采购工具箱，确保联邦机构合规选择和使用 AI 模型。

— 实施高级技术转移与能力共享计划，加速跨机构 AI 能力转移。

— 要求所有联邦机构为能受益于前沿语言模型的员工提供访问权限和培训。

— 由 OMB 召集高影响力服务机构试点 AI 应用，提升公共服务交付效率。

13、推动人工智能在国防部的应用

人工智能有可能改变国防部的作战和后台运作。正如本行动计划所述，美国必须在其武装部队中积极采用人工智能，才能保持其全球军事优势，同时确保其使用人工智能是安全可靠的。由于国防部在联邦政府内部有独特的作战需求，因此值得采取具体的政策行动来推动人工智能的采用。

政策行动建议

- 识别国防部员工大规模应用 AI 所需的技能，并实施针对性的人才培养计划。

- 建立国防部 AI 与自主系统虚拟验证平台，初步规划技术、安全与资源需求。

- 开发标准化流程，优化国防部主要作战与支持功能的业务流程，并优先自动化。

- 与云服务商签订协议，确保战时优先访问计算资源。

- 将人工智能课程纳入军事学院核心教学体系，培养未来军事 AI 人才。

13、保护商业与政府人工智能创新

要保持美国在人工智能领域的领导地位，美国政府必须与行业密切合作，在尖端人工智能技术的传播与国家安全问题之间取得适当的平衡。美国政府还必须有效应对美国人工智能公司、人才、知识产权和系统的安全风险。

政策行动建议

- 由 DOD、DHS、CAISI 等机构与领先 AI 开发者合作，保护 AI 创新免受网络攻击、内部威胁等风险。

14、打击司法系统中的合成媒体

对许多美国人来说，录音、视频还是照片等恶意的深度伪造是人工智能带来一个明显风险。尽管特朗普总统已经签署了由第一夫人梅拉尼娅·特朗普倡导的《将侵犯隐私的图像从网络上移除的法案》，来防止露骨的、未经双方同意的深度造假，但我们还需要采取额外行动，特别是人工智能生成的媒体可能会对法律体系提出新的挑战。例如，假证据可能被用来试图剥夺原告和被告的正义。所以，政府必须为法院和执法部门提供克服这些新挑战所需的工具。

政策行动建议

- 由 NIST 将“司法证据守护者”深度伪造评估计划发展为正式指南和自愿性基准测试。
- 由司法部发布指导意见，建议司法机构采用类似《联邦证据规则》第 901(c)条的深度伪造证据标准。
- 司法部法律政策办公室对《联邦证据规则》的深度伪造相关修订提交正式意见。

支柱二：建设美国人工智能基础设施

人工智能的发展需要前所未有的能源与物理基础设施支持。美国必须突破传统监管桎梏，加速建设适配 AI 时代的算力集群、半导体产能和能源网络，同时确保基础设施的安全性。

1、为数据中心、半导体制造设施和能源基础设施创建简化

许可程序并确保安全

与过去的大多数通用技术一样，人工智能将需要新的基础设施：生产芯片的工厂、运行这些芯片的数据中心，以及为所有这些提供动力的新能源。美国的环境许可制度和其他法规使得在美国以所需的速度建设这一基础设施几乎是不可能的。

此外，这一基础设施也不得使用任何可能破坏美国人工智能主导地位的对抗性技术。

幸运的是，特朗普政府在改革这一制度方面取得了前所未有的进展。自上任以来，特朗普总统已经改革了几乎所有相关联邦机构的《国家环境政策法案》（NEPA）法规，启动了许可技术现代化计划，创建了国家能源主导委员会（NEDC），并启动了美国投资加速器。现在是时候在这一势头的基础上再接再厉了。

政策行动建议

- 在《国家环境政策法案》（NEPA）框架下，参考其他机构已有标准，为数据中心相关项目设立新的“无重大影响类别”（Categorical Exclusions），以提高效率。

- 扩大《修复美国地面运输法案》（FAST-41 流程）适用范围，覆盖所有符合条件的数据中心及能源配套项目。

- 探索制定全国性数据中心建设用水许可标准（基于《清洁水法》第 404 条款），简化审批流程。

- 通过精简《清洁空气法》《综合环境反应补偿与责任法》等法规，加速环境评估流程。

- 划拨联邦土地用于数据中心和能源设施建设，优先筛选适

合大规模开发的场地。

- 禁止敌对国家技术（如 ICTS 软硬件）接入美国 AI 基础设施供应链，确保算力堆栈基于美国技术。

- 扩大 AI 在环境评估中的应用（如能源部 PermitAI 项目），提升审批效率。

2、开发匹配人工智能创新速度的电网

美国电网是地球上最大、最复杂的系统之一，但它也需要升级来支持数据中心和未来的其他能源密集型行业。美国电网是现代经济的命脉和国家安全的基石，面临着一系列挑战，需要战略远见和果断行动。电气化和人工智能技术进步推动的需求不断升级，给电网带来了越来越大的压力。美国必须制定一项全面的战略，加强和扩大电网，不仅要应对这些挑战，还要确保电网的持续实力和未来增长的能力。

政策行动建议

- 短期：稳定现有电网运行，防止过早淘汰关键发电设施，探索备用电源在高峰期的弹性应用。

- 中期：优化输电网络效率，部署智能电网技术，鼓励大用户参与需求侧管理。

- 长期：优先接入可靠的可调度能源（如增强型地热、核裂变/聚变），改革电力市场激励机制。

- 制定 21 世纪能源战略蓝图，平衡短期稳定与长期技术创新需求。

3、重建美国半导体制造业

美国通过半导体的发明启动了现代技术。现在，美国必须将半导体制造业带回美国本土。重振美国芯片产业将创造成千上万高薪工作岗位、加强我们的技术领先地位、保护我们的供应链免受外国竞争对手的干扰。特朗普政府将领导这一振兴，且不会为美国纳税人做出糟糕的交易，也不会给企业带来全面的意识形态议程。

政策行动建议

— 由商务部芯片计划办公室（CHIPS Program Office）主导，确保纳税人资金高效使用，剥离无关政策要求。

— 推动半导体研发项目与 AI 工具深度融合，加速制造工艺创新。

4、为军事与情报界建设高安全性数据中心

人工智能系统特别适合处理当今原始情报数据，而且由于人工智能系统在未来可能具有的巨大扩展能力，所以人工智能很可能会与美国政府的一些最敏感的数据一起使用。部署这些模型的数据中心必须能够抵御最坚定、最有能力的国家机构的攻击。

政策行动建议

— 由国防部、情报界、国家标准与技术研究院（NIST）联合制定高安全 AI 数据中心技术标准。

— 推广机密计算环境，支持规模化安全 AI 负载运行。

5、培养人工智能基础设施技能型劳动力

为了建设美国人工智能未来提供动力所需的基础设施，我们还必须投资于建设、运营和维护人工智能的劳动力，包括电工、

高级暖通空调技术人员和许多其他高薪职业。为了解决许多关键岗位技工的短缺问题，特朗普政府应该确定支撑人工智能基础设施、发展现代技能框架、支持行业的优先角色推动培训，并通过通识教育、CTE 和注册学徒扩大早期渠道，以推动美国人工智能的领导地位。

政策行动建议

— 国家层面：由劳工部（DOL）和商务部（DOC）牵头，联合雇主与行业组织制定 AI 基础设施岗位技能框架。

— 培训体系：通过校企合作开发行业驱动的培训项目，整合学徒制与注册学徒计划。

— 教育早期介入：拓展中学和高中生的 AI 职业启蒙项目，对接本地产业需求。

— 联邦资金倾斜：优先支持填补 AI 技能缺口的培训计划，强化雇主与培训机构的直接衔接。

6、强化关键基础设施网络安全

随着人工智能系统在编码和软件工程能力方面的进步，它们作为网络攻击和防御工具的效用将扩大。对于关键基础设施的所有者来说，保持强有力的防御态势尤为重要，因为他们中的许多人的财务资源有限。幸运的是，人工智能系统本身可以成为优秀的防御工具。随着人工智能网络防御工具的持续采用，关键基础设施的提供商可以领先于新兴威胁。

然而，在网络和关键基础设施中使用人工智能会使这些人工智能系统面临对抗性威胁。在安全关键或国土安全应用中使用人工智能，都应该使用设计安全、稳健和有弹性的人工智能系统，

这些系统可以检测性能变化，并对数据中毒或对抗性示例攻击等潜在恶意活动发出警报。

政策行动建议

- 由国土安全部（DHS）牵头成立「AI 信息共享与分析中心」（AI-ISAC），促进关键基础设施领域威胁情报共享。

- 发布 AI 特定漏洞响应指南，推动联邦漏洞数据与私营部门共享。

7、推广安全设计人工智能技术与应用

人工智能系统容易受到某些类型的对抗性输入（例如数据中毒和隐私攻击）的影响，这会使其性能面临风险。美国政府有责任确保其依赖的人工智能系统，特别是用于国家安全应用的系统，免受虚假或恶意输入的影响。尽管在推进人工智能保障领域已经做了很多工作，但促进有弹性和安全的人工智能开发和部署应该是美国政府的核​​心活动。

政策行动建议

- 国防部（DOD）主导完善「负责任 AI 框架」，并与国家标准与技术研究院（NIST）合作制定军用 AI 安全标准。

- 国家情报总监办公室（ODNI）发布情报界 AI 安全指令，规范技术部署。

8、促进成熟的联邦人工智能事件响应能力

人工智能技术的激增意味着需要谨慎的规划，以确保在系统发生故障时，对关键服务或基础设施的影响降至最低，并立即做出响应。为了应对这种可能性，美国政府应促进人工智能事件响

应行动的发展，并将其纳入公共和私营部门的现有事件响应原则和最佳实践中。

政策行动建议

— 由国家标准与技术研究院（NIST）牵头，将 AI 纳入现有网络安全事件响应框架（如 CISA 指南）。

— 更新联邦机构首席信息安全官（CISO）与首席隐私官（CPO）的协作机制，强化跨部门响应。

支柱三：引领国际人工智能外交与安全

为了在全球人工智能竞争中取得成功，美国必须做的不仅仅是在本国境内推广人工智能，还必须推动全球采用美国的人工智能系统、计算硬件和标准。美国目前在数据中心建设、计算硬件性能和型号方面处于全球领先地位，美国必须利用这一优势建立一个持久的全球联盟，同时防止我们的对手搭我们的创新和投资的便车。

1、向盟友和伙伴国家出口美国人工智能技术

美国必须通过向所有愿意加入美国人工智能联盟的国家出口其完整的人工智能技术栈：硬件、模型、软件、应用程序和标准等，来满足全球对人工智能的需求。未能满足这一需求将是一个严重的战略错误，将导致这些国家转向我们的竞争对手，而美国技术的输出和传播将使我们的盟友避免对我们的战略竞争对手的技术依赖。

政策行动建议

— 在商务部（DOC）牵头下，建立行业联盟提案机制，推动全栈 AI 技术出口包（涵盖硬件、模型、软件及标准）。通过经济外交行动小组、美国国际开发金融公司（DFC）等机构，协调落实符合美国安全标准的交易。

2、反制中国在国际治理机构中的影响力

包括联合国、经济合作与发展组织、七国集团、二十国集团、国际电信联盟、互联网名称与数字地址分配机构等在内的大量国际机构提出了人工智能治理框架和人工智能发展战略。美国要支持志同道合的国家共同努力，鼓励人工智能的发展符合我们的共同价值观。但这些努力中有太多国家都主张制定繁琐的法规、模糊的“行为准则”，以推行与美国价值观不一致的议程，或者受到试图制定面部识别和监控标准的中国公司的影响。

政策行动建议

— 由国务院（DOS）和商务部（DOC）主导，在国际标准制定机构中倡导基于创新与价值观的 AI 治理路径，揭露中国技术标准对隐私与人权的潜在威胁。

3、加强人工智能计算出口管制执法

先进的人工智能计算对人工智能时代至关重要，既能带来经济活力，又能带来新的军事能力。因此，拒绝我们的外国对手获得这种资源既是地缘战略竞争的问题，也是国家安全的问题，所以我们应该采取创新的方法来执行出口管制。

政策行动建议

- 由商务部（DOC）、国务院（DOS）牵头，利用 AI 芯片的位置验证功能追踪技术流向，防止流入敌对国家。

- 建立情报与执法协同机制，监控高风险地区（如俄罗斯、伊朗）的芯片滥用风险。

4、填补半导体制造出口管制漏洞

半导体是人类有史以来最复杂的发明之一，美国及其亲密盟友几乎垄断了半导体制造管道中的许多关键组件和工艺，我们也必须继续以半导体制造领域的开创性研究和新发明引领世界。但美国也必须防止我们的对手以破坏我们国家安全的方式将我们的创新用于自己的目的。这需要采取新的措施来解决半导体制造出口管制方面的差距，同时加强执法。

政策行动建议

- 由商务部（DOC）主导，新增对半导体制造子系统的出口管控类别，确保全产业链技术封锁。

5、建立全球范围协调保护措施

美国必须对敏感技术实施强有力的出口管制。我们应该鼓励合作伙伴和盟友遵循美国的控制，而不是事后补漏。如果他们这样做，美国应该使用外国直接产品规则和二级关税等工具来实现更大的国际一致性。

政策行动建议

- DOC 和 DOS 负责牵头并与 NSC、DOE 和 NSF 协调，制定、实施和共享有关补充技术保护措施的信息，包括基础研究和高等教育，以减轻战略对手和相关实体的风险。这项工作应以

DOS 和 DOC 正在进行的现有努力为基础，或在必要时涉及新的外交活动。

— 此事由 DOS 牵头，与 DOC、DOD 和 DOE 协调，为人工智能全球联盟制定技术外交战略计划，以协调政府各部门的激励措施和政策杠杆，促使主要盟友在整个供应链中采用互补的人工智能保护系统和出口管制。该计划应旨在确保美国盟友不会向对手提供美国寻求实施出口管制的技术。

— 扩大新的举措，促进对人工智能技术栈的多边控制，避免完全依赖多边条约机构来实现这一目标，同时还包括现有的美国控制和所有未来的控制，以在美国和盟国控制之间创造公平的竞争环境。

— 在美国商务部和国防部的领导下，与盟友协调，确保他们采取美国的出口管制措施，与美国合作制定新的管制措施，并禁止美国对手为其国防工业基地提供物资或获得国防供应商的控股权。

6、确保美国评估前沿模型国家安全风险

在不久的将来，最强大的人工智能系统可能会在网络攻击和化学、生物、放射性、核或爆炸物（CBRNE）武器的发展等领域带来新的国家安全风险，以及新的安全漏洞。由于美国目前在人工智能能力方面处于领先地位，美国前沿模型中存在的风险可能预示着外国对手在不久的将来会拥有什么。了解这些风险的性质对于国防和国土安全至关重要。

政策行动建议

— 由国家情报总监办公室（ODNI）与国家标准与技术研究

院（NIST）合作，评估外国 AI 系统（尤其是中国模型）的漏洞与恶意行为。

- 招聘顶尖 AI 研究人员，强化联邦政府对前沿模型的分析能力。

7、投资生物安全

人工智能将释放生物学中几乎无限的潜力：治疗新疾病、新的工业用例等等。同时，它可以为恶意行为者合成有害病原体和其他生物分子创造新的途径。这个问题的解决方案是多旨在筛查恶意行为者的分层方法，以及用于更有效筛查的新工具和基础设施。随着这些工具、政策和执行机制的成熟，与盟友和合作伙伴合作以确保国际采用至关重要。

政策行动建议

- 要求联邦资助的生物研究机构使用具备客户验证能力的核酸合成工具，并建立数据共享机制以筛查可疑订单。

- 由科技政策办公室（OSTP）牵头，推动国际合作，强制推行生物合成技术安全标准。