

2026-HY-E029
USA/AII/IRR



区域国别研究报告

上海市哲学社会科学规划办公室

2026 年 7 月 28 日

美国人工智能管控政策与企业出海风险

上海对外经贸大学

上海市企业走出去综合服务平台

《**区域国别研究报告**》是上海市哲学社会科学规划办公室依托上海市各高校和科研院所专业研究力量，紧扣服务企业走出去现实需要，专为“上海市企业走出去综合服务平台”打造的区域国别研究品牌。

《报告》基于学者“在地研究”田野调研、企业出海实务经验以及其他信息，聚焦国别/区域、产业/行业、在地合规运营三类场景，推出三类系列成果。其中，“**国别报告**”系列以对象国政治、经济、社会、文化等内容为研究对象，重点围绕宏观经济形势、营商环境、中资企业经营状况、机遇挑战等维度，解析对象国各领域的发展态势，为企业海外布局提供决策参考；“**行业报告**”系列针对重点产业跨境布局或企业走出去的行业赛道，深入研判对象国的重点行业发展格局；“**合规报告**”系列回应企业海外合规运营实务关切，系统梳理对象国重点领域的监管要点，为企业在地运营提供应对策略参考。

摘 要

报告围绕美国人工智能政策的最新动向，重点研判2026年以来美国人工智能政策“限制—放松—再收紧”的管控模式及其对中国企业出海的影响。总体看，美国正在以国家主导权重塑人工智能政策体系，一方面以“最低负担监管”“统一联邦框架”“促进技术出口”为名为本国企业扩张松绑，另一方面通过出口管制、投资审查、实体清单、执法罚款、盟友规则和基础设施竞争，对外企技术空间施压。

企业出海的风险管控宜从传统贸易合规扩展到全链条经营安全。过去中国科技企业出海主要关注数据合规、隐私保护、地缘舆论和市场准入；当前则必须同时面对美国出口管制、投资审查、供应链穿透、技术来源证明、云服务限制、海外融资结构审查、人才流动限制、开源模型合规、行业客户安全审查等多重风险。大模型、AI Agent、智能驾驶、机器人、AI 芯片、云计算和工业智能化相关企业承压更甚。

目 录

一、美国人工智能政策的转向	1
（一）立法节奏加快	1
（二）竞争局势胶着	2
（三）豁免本土企业安全审查	2
二、企业需关注的主要问题	3
（一）半导体辅助耗材亦管控	3
（二）“出口管控”到“征税管控”	4
（三）AI 创业公司出境合规	5
三、企业或将面临的主要风险	7
（一）供应链断供与许可反复风险	7
（二）客户合规排斥与市场准入风险	7
（三）海外融资并购和股权架构风险	7
（四）人才流动和团队稳定风险	8
（五）开源模型和数据合规风险	8
信息来源	9

一、美国人工智能政策的转向

(一) 立法节奏加快

2025 年 12 月 11 日，美国签署《确保全国人工智能政策框架》行政令，强调美国人工智能服务于国家和经济安全，提出以“最低负担”为原则，防止州级监管碎片化对人工智能创新造成阻碍，并要求相关部门提出建议，避免州级过度监管，以统一全国政策框架。2026 年 3 月 20 日，白宫发布《全国人工智能立法框架》，向国会提出人工智能立法建议，预防各州监管“拼图化”、保护创新、维护联邦政府在人工智能政策中的主导地位。

这表明，美国人工智能政策已从“产业政策文件”走向“联邦法律框架”。其直接目的是削弱加州、科罗拉多、纽约等州可能形成的高强度监管约束，为本国模型公司、云平台和芯片企业创造统一、低摩擦的国内市场；其深层目的，是通过联邦层面的制度整合，在国际竞争中保持更快迭代速度。对外资企业而言，这意味着美国企业在本土将获得更低合规负担和更强政策确定性，而外资企业进入美国及其盟友市场时则可能面临更相关程度的审查。

（二）竞争局势胶着

Stanford HAI《2026 人工智能指数报告》显示，美国 2025 年私人 AI 投资达到 2859 亿美元，为中国 124 亿美元的 23 倍以上；美国新获融资的 AI 企业数量也明显领先。美国在数据中心、云平台、基础模型公司、AI 芯片和风险资本方面保持体系化优势，数据中心和电力资源正在成为新的竞争门槛。该报告同时提示，不可低估中国政府引导基金和产业政策投入的实际规模。

（三）豁免本土企业安全审查

2026 年 5 月，美国一度酝酿要求前沿模型在上市前向政府提交安全评估或开展自愿审查的行政令。但 5 月 21 日前后，美方推迟或调整了该行政令的签署进程，公开理由集中在“不愿削弱美国技术领先优势”。美国国内人工智能治理的底层排序正在发生变化：当安全审查可能延缓模型发布、削弱企业商业节奏时，政策优先级会向“保持领先”倾斜。这种取向意味着美国企业在模型迭代、产品上市和资本扩张上进一步获得速度优势；同时，美国政府会把更多安全压力外移，通过对中国企业、第三国合作方和海外市场的管控来体现“安全治理”。

二、企业需关注的主要问题

（一）半导体辅助耗材亦管控

2026 年开年，美国商务部工业和安全局（BIS）连续采取执法行动避免美国企业向中国相关企业输送受控物项。根据 BIS 文件，2026 年 2 月 BIS 与 Applied Materials 及其韩国子公司达成 2.525 亿美元民事和解，指控其未经授权向受限中国实体再出口半导体制造设备。该案为 BIS 历史上金额居前的出口管制处罚之一。更值得关注的是，BIS 2026 年 4 月对加州 Coastal PVA Technology 的处罚，涉及半导体制造用聚乙烯醇（PVA）刷等辅助耗材。BIS 文件称，该公司通过第三方分销商向 SMIC 北京、SMIC 北方等实体清单企业销售相关产品，且缺乏正式出口合规制度。该案说明，美国出口管制边界已经从“高端芯片和设备”延伸到“半导体制造辅助耗材”，从直接出口延伸到第三方分销和转口渠道，从大型跨国企业延伸到中小供应商。

一方面，海外供应商对中国半导体、AI 硬件和云计算企业的合规顾虑将明显上升，即使是低敏感度物项、EAR99 物项或普通耗材，也可能因最终用户、最终用途

或关联实体问题被拒绝供货。另一方面，中国企业在海外建设数据中心、芯片实验室和研发平台时，可能面临供应商穿透审查、运输文件审查、客户身份审查和售后服务限制，项目周期和成本均将上升。

（二）“出口管控”到“征税管控”

2026 年 1 月 15 日前后，美国对部分先进计算芯片出口政策作出调整，将 H200、AMD MI325X 等产品从此前更严格的拒签逻辑，调整为逐案审查、附带条件的许可机制。与此同时，美国对符合特定性能门槛、经美国过境但并非用于美国供应链的相关芯片征收 25% 从价关税。Baker McKenzie、Mayer Brown 等机构分析认为，这种制度组合实质上“将出口管制”与“财政征税”进行区分，即企业满足关税和许可条件后才可获得有限出口资格。

美国芯片政策出现重要变化：不再单纯追求完全切断中国算力获取，试图以许可证、关税、配额和最终用途审查建立“可控准入”。一方面，美国政府借此缓解英伟达、AMD 等企业因中国市场受限而产生的商业压力；另一方面，美国仍把 Blackwell、B200、Vera Rubin 等下一代平台排除在许可范围之外，确保先进算力有限获取。

从中国企业角度看，H200 等芯片即便获得许可，也不代表供应链风险消除。许可证批准、芯片生产排期、美国过境关税、企业合规承诺、中国进口审批、客户使用范围以及后续服务支持之间存在多个不确定节点。换言之，企业面对的是“许可获批未必到货，到货未必稳定使用，稳定使用未必可持续扩容”的复杂环境。若企业据此大规模调整技术路线，可能在美国政策再次收紧时陷入被动。

（三）AI 创业公司出境合规

2026 年 4 月至 5 月，围绕 Meta 收购 AI 创业公司 Manus 的交易，中国监管部门据报要求撤销或重组相关交易，并对部分创始人出境作出限制。Reuters 援引媒体报道称，Manus 创始人寻求融资以回购公司，以执行中国政府要求撤销 Meta 收购的安排。该案成为中美人工智能投资审查双向趋严的标志性事件。

不少中国人工智能创业企业采用开曼、新加坡或其他离岸架构，试图在中美监管之间保持融资和并购弹性。Meta-Manus 案显示，只要核心团队、技术来源、数据资产、早期运营或实质控制与中国存在较强联系，即使形式上完成境外重组，仍被认定处于中国安全审查范围内。与此同

时，美国 CFIUS 也会从美国投资者、美国用户数据、美国模型能力和国家安全角度审查相关交易。双方管辖权主张相互叠加，使企业可操作的合规回旋余地显著压缩。

这对中国企业出海尤其重要。AI 创业公司若希望在海外融资、并购或建立研发总部，必须提前评估技术敏感性、数据边界、人员身份、股权结构、知识产权归属和客户区域。单纯通过注册地迁移规避监管的路径正在失效，企业需要从设立之初就建立清晰的技术分层、数据分域、人员合规和投资者准入机制。

三、企业或将面临的主要风险

(一) 供应链断供与许可反复风险

先进芯片、服务器、网络设备、先进封装、EDA 软件、高端存储以及数据中心关键部件，均可能受到美国出口管制或第三国转运审查影响。企业在海外建设算力集群时，即使项目所在地不是美国，也可能因设备含有美国技术、供应商受美国管辖、资金经过美国金融体系而受到限制。尤其是采用美国 GPU 和云平台的外资企业，需警惕许可证变化导致合同履行受阻。

(二) 客户合规排斥与市场准入风险

美国正推动“全栈美国 AI 技术方案”向盟友和伙伴输出，可能在政府、金融、能源、电信、交通、医疗等敏感行业形成事实准入门槛。外资企业即使具备价格和工程优势，也可能因客户担心美国制裁、数据安全审查或政治舆论风险而被排除在关键项目之外。

(三) 海外融资并购和股权架构风险

Meta-Manus 案及美国 CFIUS 实践表明，AI 企业融资并购已进入高敏感区。母国背景团队、源自母国的数据资

产、在母国完成早期训练的模型、服务母国重点行业的产品，均可能被认定具有安全敏感性。企业若未提前设计知识产权、数据、团队和治理结构，后续融资、上市、并购可能遭遇监管阻断。

（四）人才流动和团队稳定风险

人工智能竞争正在从技术和资本扩展到人才。若核心创始人、算法负责人、芯片架构师和安全研究人员在跨境流动中受到出境限制、签证审查或雇佣限制，企业海外研发中心和客户交付能力将受到影响。

（五）开源模型和数据合规风险

AI 企业出海越来越依赖开源模型、开源框架和公开数据集。但美国可能通过开源许可证、安全评估、模型权重传播限制、云端调用审查等方式影响开源生态。欧盟、英国、加拿大、澳大利亚等市场也在加强 AI 透明度、版权、隐私和安全评估要求。企业若缺乏模型来源记录、数据授权证明和安全测试报告，可能在海外被诉或被监管问询。

牛东芳(上海对外经贸大学)

信息来源

1. 白 宫： 《Ensuring a National Policy Framework for Artificial Intelligence》，2025 年 12 月 11 日。

2. 白 宫： 《National Policy Framework for Artificial Intelligence: Legislative Recommendations》，2026 年 3 月 20 日。

3. 美国商务部 BIS: Applied Materials 及其韩国子公司出口管制和解公告，2026 年 2 月 11 日。

4. 美国商务部 BIS: Coastal PVA Technology Final Order, 2026 年 4 月 13 日。

5. Morgan Lewis： 《BIS Revises Export Review Policy for Advanced AI Chips Destined for China and Macau》，2026 年 1 月。

6. Baker McKenzie： 《BIS Revises License Review Policy for Advanced Computing Commodities / AI Semiconductors to China and Macau》，2026 年 1 月。

7. Mayer Brown： 《Administration Policies on Advanced AI Chips Codified》，2026 年 1 月。

8. Stanford HAI： 《The 2026 AI Index Report》。

9.CFR：《DeepSeek V4 Signals a New Phase in the U.S.-China AI Rivalry》，2026 年 4 月。

10.OpenAI：《OpenAI, Oracle, and SoftBank expand Stargate with five new U.S. AI data center sites》，2025 年 9 月。

11.RAND：《Evaluating Potential Artificial Intelligence Energy Capacity at Different Data Center Sites》，2026 年 3 月。

12.NVIDIA：Fiscal 2026 及 FY2027 Q1 财报公告。

13.Reuters、AP、The Guardian、CNBC 等关于 AI 模型审查行政令、Meta-Manus 交易、英伟达芯片政策及 Stargate 建设的分析。



联系地址：淮海中路 622 弄 7 号 308 室

联系电话：021-33165460

联系邮箱：zbzh@sh-popss.gov.cn

本报告为研究团队基于公开信息、行业调研、数据分析及专业研究方法独立编制完成的研究成果，仅供行业研究、学术研讨、决策参考交流使用，不构成任何商业、投资、法律、财税及其他专业实操建议。报告免费获取，未经书面正式授权，任何机构及个人不得擅自转载、复制、篡改、摘抄、传播本报告全部或部分内容。