汉坤法律评述
2025 年 9 月 5 日
HANKUN
汉坤律师事务所
Han Kun Law Offices
北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约 | 硅谷

AI 管制前沿 — 美国出口管制政策观察

作者：段志超 | 蒋睿馨 | 张雪晨 | 曾媛 | 时悦

芯片和算力是人工智能（“**AI**”）发展的重要基础。近年来，中国的芯片公司已经取得了长足的进步，为中国人工智能企业的模型训练和应用提供了越来越多的底气。但在一段时间内，中国企业对美国芯片技术和算力仍然有一定程度的依赖性。有鉴于此，在中美科技博弈与经济竞争的大背景下和美国日益趋严的出口管制政策下，如何确保中资公司在获得先进芯片和算力过程中的合规性是兼具战略性意义和挑战性的话题。本文旨在梳理美国 AI 领域出口管制政策及中国企业的应对之法，为中国企业提供指南。

一、美国出口管制概述

美国对 AI 领域的出口管制政策以《出口管理条例》（Export Administration Regulations，“**EAR**”）为核心，通过多重规则限制先进技术的跨境流动。近年来，更是通过扩大外国直接产品规则（foreign direct product rule，“**FDPR**”）、调整出口管制分类编号（“**ECCN**”）的技术参数或新增 ECCN 管制物项、增设实体清单等手段，逐步构建起覆盖硬件、技术和软件的综合性管制框架，目前已从单纯的技术限制演变为地缘战略工具，对全球科技产业链造成深远影响。

2018 年通过的《出口管制改革法案》（Export Control Reform Act，“**ECRA**”）是美国出口管制法律体系的重要基石，EAR 则是该法案授权下的核心执行条例，覆盖敏感物项出口的全流程管控。2022 年以来，美国商务部工业与安全局（BIS）以 EAR 为基础，密集推出一系列新规，全面限制中国获取与发展先进 AI 算力的能力。具体而言，美国对半导体与 AI 的出口管制，目前仍以“先进计算”两轮规则（2022 与 2023 年）[1]为主干：对满足阈值的高性能芯片及其整机、相关软件与技术实施许可管制，并通过最低成分比例（de minimis）与 FDPR，把境外制造、但使用受控美国技术/软件或含美国受控成分生产的物项“拉回”EAR 管制范围，并通过上述规则、清单管制与尽调义务等组合拳，持续收紧对先进算力与训练能力的管制。AI 芯片（如英伟达 A100、H100）、先进半导体制造设备及相关技术被列入特定 ECCN（如 3A090、4A090），成为重点管制对象。以 2023 年 10 月新规为例，当芯片“总处理性能”（TPP）≥4800，或 TPP≥1600 且“性能密度”≥5.92（属 3A090.a），TPP 2400–<4800 且密度 1.6–<5.92，或 TPP≥1600 且密度 3.2–<5.92（属 3A090.b）时，原则上需要许可[2]。根据新规相关标准，英伟达的 H100、H800、A100、A800 等型号的芯片、AMD 的

[1] 参见：https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3158-2022-10-07-bis-press-release-advanced-computing-and-semiconductor-manufacturing-controls-final/file；https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3353-2023-10-16-advanced-computing-supercomputing-ifr/file。

[2] 参见：https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3353-2023-10-16-advanced-computing-supercomputing-ifr/file。

MI300A、MI300X 等型号的芯片均将受限。

2025 年 1 月，BIS 发布《人工智能扩散框架》（“AI Diffusion Rule”）[3]，推出了新的出口管制要求，拟进一步扩大 ECCN 3A090.a 和 ECCN 4A090.a 下的管制芯片范畴，并首次以 ECCN 4E091 对闭源（closed-weight）且在训练中使用超过 10^{26}次计算操作的前沿 AI 模型权重的出口、再出口或境内转移实施许可要求，并对 D:5 组国家及澳门地区适用更严格政策。2025 年 5 月 13 日，在前述《人工智能扩散框架》生效前夕，BIS 宣布撤销该规则并同步发布两份行业指引与一份政策声明，转以执法指引方式提示风险点与注意义务[4]。但《人工智能扩散框架》的撤销并不意味着美国降低了对 AI 发展所需的高级芯片的管制力度，反而表明特朗普政府拟搭建 AI 高性能芯片的管制体系的意图，BIS 也在官网表示，将在未来发布新的《人工智能扩散框架》的替代规则[5]。

在上述日趋严苛的监管背景下，企业在涉及受控芯片交易方面面临更多的合规风险。一方面，频繁出台的芯片管制新规给企业开展商业活动带来较大不确定性和合规成本。例如，芯片管制的性能阈值规则存在不可预测性，2023 年底，英伟达为中国市场设计推出 H20 芯片，虽通过降低算力参数符合了当时出口标准，但仍在 2025 年 4 月被列入管制范围。另一方面，在穿透式执法调查的压力下，通过第三国中转获取高性能芯片的方式也遭到严厉打击。从今年 1 月开始，美国政府机构就开始对某中资人工智能公司涉嫌通过新加坡的中介公司购买受限的英伟达芯片开展调查，并且持续施压新加坡、马来西亚严查 AI 芯片流向问题。

二、中国企业对芯片管制的应对：出海场景下的合规风险分析

在复杂多变的芯片管制国际环境下，中国企业通过出海可以获取更广阔的市场空间和资源支持。但受美国长臂管辖影响，出海并不能完全规避芯片出口管制要求。在不同管制场景下，企业仍面临合规风险。

（一）硬件采购层面的风险分析

1. 直接采购芯片

对于总部在中国的出海企业，为满足 AI 模型训练所需的高算力需求，可能选择在境外自建数据中心或机房并采购高性能 GPU（包括受 EAR 管辖的相关物项）。

根据 EAR 规定，向总部或最终母公司位于澳门地区及 D:5 组国家（包括中国大陆和香港）的实体出口此类高性能物项（如按 ECCN 归类为 3A090、4A090 的芯片），原则上须申请许可证，且在多数情形下适用推定拒绝的许可审查政策[6]。经由第三国中转、拆单或变更用途申报，均不足以排除对华（再）

[3] 参见：https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion。

[4] 三项指导意见分别为包括《BIS 关于可能适用于训练人工智能模型所用的先进计算芯片及其他商品的管控的政策声明》（BIS Policy Statement on Controls that May Apply to Advanced Computing Integrated Circuits and Other Commodities Used to Train AI Models“《先进芯片政策声明》”）、《防止先进计算芯片被转移用途的行业指导》（Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits，“《先进芯片行业指导》”）以及《关于一般禁令 10（GP10）适用于中华人民共和国（PRC）先进计算芯片（ICs）的应用指南》（Guidance on Application of General Prohibition 10 (GP10) to People’s Republic of China (PRC) Advanced-Computing Integrated Circuits (ICs)，“《一般禁令 10 指南》”），参见：https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens。

[5] https://www.bis.gov/press-release/department-commerce-announces-rescission-biden-era-artificial-intelligence-diffusion-rule-strengthens。

[6] 15 CFR 742.6(b)(10)(ii). Policy for Country Group D:5 and Macau. For items specified in paragraph (a)(6)(iii)(A) of this section, applications for exports, reexports, or transfers (in-country) to or within Macau or destinations specified in Country Group D:5 or to an entity headquartered in, or whose ultimate parent company is headquartered in, either Macau or a destination specified in Country Group D:5 will be reviewed under a presumption of denial。

出口的实质认定，并可能被纳入规避评估。

具体到实践层面，若中国企业的海外子公司直接在境外采购受 EAR 管辖的高性能芯片，并用于自建机房训练 AI 模型，根据 EAR 最终用途限制规则，此类交易多数情况下不适用任何许可例外。因此，该模式在实际操作中既面临出口管制限制，又存在被推定拒绝许可的风险。

2. 通过海外第三方公司采购 GPU 自用

在直接采购芯片受限的情形下，若通过第三方公司（“**第三方**”）获得底层高算力 GPU（如 A800、H800），并基于此向中国客户提供算力服务，该安排亦难以切断最终控制/使用与中国总部（或 D:5 组国家/澳门地区母公司）之间的实质联系，易被按规避处理。根据 EAR 下一般禁令 10（“**GP10**”），任何人均不得在“明知”存在违反 EAR 行为的情况下，采购、使用、销售、运输、出口、资助、订购、藏匿、存储或以其他方式参与与该等违法行为相关的受 EAR 管辖物项的交易，若通过第三方采购受控 GPU，可能会被认定为“以其他方式”参与受 EAR 管辖物项的交易。且在执法过程中，BIS 对“明知”的认定标准极为宽泛，相关交易主体难以通过主张不知情来规避责任。

此外，BIS 近期加强了对第三方“转运”的执法。2025 年 8 月 5 日，美国司法部公布一则案例，两名中国公民因违反美国出口管制规定向中国公司提供受控 GPU 芯片被逮捕并面临刑事指控。涉案人员通过其控制的 ALX Solutions Inc.公司，在未获得 BIS 许可的情况下，于 2022 年 10 月至 2025 年 7 月期间向中国输出“专为 AI 应用设计”的 GPU 芯片（用于自动驾驶、医疗诊断等领域）。BIS 以及联邦调查局已介入调查该案[7]。

（二）采购云服务层面的风险分析

在高性能 GPU（如 A100/H100）硬件直采路径被严格收紧后，通过境外云服务获取算力资源已成为部分企业应对硬件获取难的重要解决方案。根据 BIS 既有咨询意见，在未向用户传输受控软件/技术的前提下，单纯提供计算能力的云服务通常不构成 EAR 管辖下的“出口”，服务提供方原则上不被视为“出口方”，但这一商业模式的转变并非处于“监管真空”。如前所述，在 GP10 的要求下，企业对交易链条中存在的 EAR 违规具备“明知/应知”（例如对受控 GPU 的来源、取得方式或再出口明显违规；或受控 GPU 持有人为 EAR 限制获取受控 GPU 的实体或其子公司），也即，无论其是否直接参与受控物项的采购过程，可能触发（i）**GP 10**（明知仍继续违规交易，对受 EAR 管辖物项的**使用/服务**亦在规制之列），以及（ii）**EAR 第 764.2(b)条下，**协助他人违规的责任。

为降低风险，建议企业对云服务商与算力来源开展基于风险的尽职调查（含来源合规声明、名单筛查、合同承诺与终止条款、地理与访问控制、日志留痕等），并关注美国关于云服务提供商对客户识别/训练活动报告类规则进展及其与 EAR 的衔接要求，详见第三部分“美国云服务监管概述与分析”。

（三）数据跨境传输风险分析

同时，受限于半导体制程与高性能算力芯片的可得性，中国企业在海外调用先进算力资源开展大模型训练时，除硬件层面的限制外，还需要重点关注数据跨境与算法技术出口限制等合规义务。

一方面，在数据层面，模型训练通常需要依赖海量数据，需要关注训练数据获取的合规性。即便是互联网公开信息或开放数据集，在利用爬虫等技术手段时必须严格遵守使用范围。对于通过第三方许可获得的数据，则需要进一步审查其来源是否合法合规：如涉及个人信息，需确保第三方已经履行告知与

[7] https://www.justice.gov/usao-cdca/pr/two-chinese-nationals-arrested-federal-complaint-alleging-they-illegally-shipped-china。

同意等个人信息保护义务。此外，在美国《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政命令》（Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern，"14117 行政令"）下，获取美国公民敏感数据或政府相关数据还将在此基础上进一步受限。

除此之外，数据跨境传输同样带来了合规挑战。例如，中国《数据安全法》要求重要数据出境通过安全评估，而部分国家或地区还设有数据本地化存储要求，对企业海外存储架构提出了额外限制。

另一方面，在算法与技术层面，如果企业将境内的模型算法传输至境外算力平台进行训练，或将训练后的模型算法回传境内或出口到其他国家，如相关模型算法落入到限制出口或禁止出口的技术范围内，也将触发技术出口管制监管。

三、美国云服务监管概述与分析

随着算力需求持续攀升，对高算力有需求的中国企业除直接采购 GPU 外，云服务平台已成为重要替代方案。相关企业需特别注意通过云服务提供商间接调用受 EAR 管制的先进计算芯片（如 3A090/4A090 芯片）所引发的合规风险。根据 BIS《先进芯片政策声明》及司法实践，若云服务提供商明知其提供的算力资源将用于或代表中国实体训练 AI 模型，且该模型涉及敏感最终用途（如军事、情报领域），则可能触发许可证审查要求。此类间接调用模式虽未被 EAR 明确列为管制对象，但 BIS 已通过"危险信号"将"无法确认用户总部不在中国"等情形纳入高风险特征，企业需警惕被认定为规避管制的实质性认定风险。

（一）美国对 AI 发展中云服务的监管

美国政府近来关注中国实体通过云服务获取高性能算力的问题。2024 年 1 月，美国商务部曾发布《拟议规则》[8]，公开征求意见，拟通过"了解你的客户（KYC）"等措施，加强对中国实体利用海外云服务获取算力的监管，弥补现有出口规则在云计算场景下的漏洞。

如前所述，2025 年 5 月 13 日，美国商务部发布三项政策，尽管这些指导文件本身不具法律约束力，具体技术细节及合规措施仍待立法说明，但它们反映了 BIS 的执法立场与监管导向，对云算力提供等 AI 服务模式中的合规风险进行了重点提示。其中：

- 《BIS 关于可能适用于训练人工智能模型所用的先进计算芯片及其他商品的管控的政策声明》（下称"《先进芯片政策声明》"）[9]明确，在"知悉/应知"所训练的 AI 模型将用于大规模杀伤性武器（WMD）或军事-情报等敏感最终用途/用户的前提下，下列活动可能在 EAR 第 744 部分"兜底（catch-all）"管制下触发许可要求：（1）出口、再出口或境内转移受 EAR 管制的先进计算 IC 或相关商品（例如 3A090.a、4A090.a 及第 3/4/5 类的.z 项）给任何第三方（如境外 IaaS 提供商/数据中心），且知悉该提供商将使用这些物项为总部位于 D:5 组国家（含中国大陆和香港）或澳门的主体进行（或代表其进行）AI 模型训练；（2）如果 IaaS 等服务提供商在明知其拥有并转移[10]的先进计算芯片或其他受管制物项将被用于或代表总部位于 D:5 组国家（含中国大陆和香港）的实体训练 AI 模型。此类场景下，对中国或其他国家的云服务提供商/客户，若作为"外国 IaaS 提供商"

[8] *Taking Additional Steps To Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*: https://www.federalregister.gov/documents/2024/01/29/2024-01580/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious。

[9] BIS Policy Statement on Controls that May Apply to Advanced Computing Integrated Circuits and Other Commodities Used to Train AI Models，https://www.bis.gov/media/documents/ai-counter-diversion-industry-guidance-may-13-2025.pdf。

[10] 此"转移"定义为改变最终用途或最终用户。

面向总部位于 D:5 国家的客户提供算力，需格外关注自身的合规义务；

- 为加强《先进芯片政策声明》所涉及场景的风险管理，《先进芯片行业指导》（Industry Guidance to Prevent Diversion of Advanced Computing Integrated Circuits）[11]中列示了“危险信号”及尽职调查参考。例如，在新开展交易或合作时，若作为客户的 IaaS 服务商无法确认其用户总部不在中国，则出口商、再出口商或转让方在提供受 EAR 管制的先进计算芯片时应将此情形视作危险信号。未来 BIS 可在执法过程中据此判断企业是否尽到了合理的注意义务。

因此，对于总部位于中国的公司，通过云服务使用基于受 EAR 管辖的先进计算芯片（如 3A090 芯片）的算力进行模型训练，也可能触发美国出口管制限制。目前，美国监管关注的重点主要集中在与大规模杀伤性武器、军事或情报相关的最终用途/用户，尚未扩展至所有 AI 模型训练活动。但需特别注意，BIS 已明确将云服务规避管制风险列为未来政策优先关注事项，云服务企业需警惕监管范围扩展带来的合规压力。

（二）监管趋势

如前所述，尽管 2025 年 1 月提出的《人工智能扩散框架》已被撤销，BIS 在官网明确表示，将发布替代性的新规。

由于新规尚未出台，现有框架仍可作为参考：拟设一项 ECCN 编号 4E091，将经 10^{26}次计算训练而成的 AI 模型权重列为管制物项，对其跨境转移施加许可证要求。其中，对出口至总部位于中国实体的许可证将适用“推定拒绝”政策。相对应地，BIS 拟通过《先进芯片行业指导》强化云计算服务提供商的 KYC 义务，要求对非 Tier 1 地区实体利用云服务训练符合 4E091 标准的闭源 AI 大模型时，必须实施严格的尽职调查与合规管控措施。

四、总结

随着中美科技博弈与经济竞争加剧，美国对 AI 领域的出口管制日益严苛，企业面临着复杂的合规挑战。美国以 EAR 为核心，通过扩大外国直接产品规则、调整出口管制分类编号等手段，构建起全方位管控网络。在此背景下，企业获取高性能算力芯片的合规成本显著攀升，一方面，企业无论是自行直接采购，抑或是通过其海外子公司、关联公司等进行采购高性能芯片，均严格受限；另一方面，即便其通过独立的第三方代购等模式获取芯片，也仍存在被认定为规避管制的实质性风险。

就云计算服务场景而言，通过云服务提供商间接获取基于受 EAR 管辖的先进计算芯片的算力开展模型训练，同样可能触发出口管制审查机制。出海企业需注意：（1）云服务提供商本身在获取或转移先进计算芯片时，可能受到 EAR 的出口许可限制；（2）若服务提供商在服务过程中向境外传输了受控的软件/技术，或涉及 U.S. person 受限活动，可能触发 EAR 下的合规义务；（3）在云服务提供商明知其提供的算力将被用于或代表 D:5 组国家（含中国大陆和香港）及澳门主体训练 AI 模型，且该模型用于敏感最终用途时，可能触发许可证要求。

此外，企业必须密切关注政策更新。鉴于美国出口管制相关政策更新频繁，虽然目前尚未有生效的专门的 AI 监管框架，但企业可关注 BIS 不定期发布的 FAQ、政策声明及执法案例。在开展相关领域业务时，企业应避免任何形式的规避行为，严格遵守相关规定，以降低合规风险。

[11] https://www.bis.gov/media/documents/ai-counter-diversion-industry-guidance-may-13-2025.pdf。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com

蒋睿馨

电话： +86 10 8524 5808
Email： ruixin.jiang@hankunlaw.com