AI技术出口监管加速落地：受控技术、出海场景与企业应对

作者：杨建媛 赵雅泽、杜金阳、张梅然

2026-10-21

前言

2026年10月16日，商务部、科技部发布2026年第48号公告（以下简称“公告”），就《中国禁止出口限制出口技术目录》（以下简称“《目录》”）修订公开征求意见。公告附件1（以下简称“征求意见稿”）涉及人工智能、生物医药和光伏三个领域，其中拟增列人工智能相关技术23项。此次调整回应人工智能等技术发展及其在敏感领域应用带来的安全风险，并拟通过自动许可等便利措施支持正常国际技术交流合作。

对于相关科技企业而言，此次《目录》调整，可以围绕三个问题展开：哪些技术受到管制、哪些出口行为纳入管理，以及企业需要关注哪些监管安排。

一、受控技术：以敏感关联与技术能力划定管制边界

（一）管制原因：维护国家安全与经济技术竞争力

国家安全与经济技术竞争力，是理解本次《目录》调整的两个重要出发点。一方面，AI在敏感领域的应用不断拓展，需要防范技术滥用、失控和不当扩散对国家安全造成的风险；另一方面，相关技术凝结了我国长期研发积累，承载着产业发展和科技竞争的重要价值，其跨境转移也涉及国家经济技术权益的维护。

（二）管制对象：更新既有领域，并补充AI及其支撑体系的专门列管

纵览本次征求意见稿，我们从两个方面理解此次调整，并将拟列管的AI相关技术归纳为以下四类：

1. 既有领域的更新：AI增强原有技术能力，也带来新的安全风险与防护需求。

信息识别与处理：内容鉴伪、声纹识别、隐写与提取，涉及信息真实性、身份安全及隐蔽信息传递等问题；针对汉语及少数民族语言的翻译，还需结合本土语言资源保护及相关安全利益理解。随着AI生成、合成及识别能力的发展，这些领域原有的安全需求与技术边界也在发生变化。网络安全与对抗：AI提高了漏洞发现、利用链构建、恶意代码生成和规避防护的效率与自主性，使网络攻击和对抗更易实现自动化、规模化。相关管控因而可从保护关键系统、维护国家安全防御能力，以及防范攻击能力滥用和扩散的角度理解。

2. 围绕AI及其支撑体系的专门列管：针对此前缺少专门条目的技术，补充与其发展相适应的出口管理规则。

大模型与智能体：在中美围绕AI展开激烈科技竞争的背景下，这类技术既关系研发和产业应用优势，也涉及训练数据、敏感用途及自主行为等安全问题。此次设置的模型规模、全球领先水平和智能体自主能力等条件，体现出监管对最前沿、高水平技术能力的重点关注。芯片与算力集群：芯片提供AI训练和运行所需的计算、存储能力，算力集群则将大量设备组织起来协同工作，二者共同构成AI发展的重要基础。此次拟列管的相关芯片设计，以及面向超大规模集群的高速互联、高效调度和训练容错技术，重点在于维护AI关键支撑领域的技术积累与竞争优势。

（三）边界识别：结合敏感关联与技术能力区分禁止与限制出口技术

结合前述国家安全与经济技术竞争力的考量，本次拟列管技术的识别，可以重点把握两个维度：

敏感关联：看技术是否涉及与国家安全密切相关的高敏感应用场景、攻击对象或训练数据。这是禁止出口部分最突出的识别线索；限制出口部分也会根据数据来源等因素的敏感程度划定范围。技术能力：看技术能否准确、可靠、高效地完成任务，以及能在多大规模、何种复杂程度下达到目标。相关性能与规模门槛，将技术先进性和竞争价值落实为具体条件，在限制出口部分尤为突出，也用于进一步限定部分禁止出口技术的范围。

1. 禁止出口：以国家安全高敏感关联为首要识别线索

禁止出口是最严格的技术出口管理方式，其适用范围需要审慎划定。从本次征求意见稿的条目设置看，与国家安全的高敏感关联，是识别禁止出口技术的首要线索；在此基础上，再结合各条目规定的技术类型和能力条件，确定具体的禁止出口边界。

为便于对照识别，我们将征求意见稿列管的禁止出口技术项总结如下：

技术名称及类型		高敏感关联	核心能力关注
信息识别与处理	**高性能检测技术**：鉴伪系统及设备制造技术	**专门或者主要用于**我国网络数据跨境传输安全风险防范和处置。	**检得准、漏得少**：对深度合成图像、音视频或多模态信息，检测准确率和召回率达到95%以上。
网络安全与对抗	**信息对抗技术**： • 恶意代码生成与变异技术 • 对抗环境自适应演进与运行时动态行为修改技术 • 自动化免杀变种批量生成与分布式规模化部署技术	**可被用于攻击**国家关键信息基础设施、国防军工、核心政务等高敏感系统，或绕过国家安全防御体系。	**突破检测、适应防护环境、自动变异及批量生成等能力强**：各技术方向分别设置成功率、代码改写比例、变种数量或自动化程度等条件。
大模型与智能体	**人工智能大模型技术**	利用**我国核心数据**进行训练后提供服务。	**未另设技术能力门槛。**
	人工智能体技术	**专门或者主要用于**国家关键信息基础设施、国防军工、核心政务等高敏感场景。	**自主规划、协作、工具使用或动态决策**达到**高性能水平**，具体参照限制类智能体。

2. 限制出口：重点关注高精尖技术与关键能力

限制出口部分以技术能力为重要识别线索，通过性能、规模及特定技术条件划定范围，重点关注高精尖技术与关键能力。商务部官方答记者问亦明确，此次拟列管范围精准有限，有关措施正式实施后，绝大部分人工智能技术仍可以自由出口。

以受到普遍关注的大模型为例，征求意见稿对其核心技术指标设置了计算量达到10^{26}

次浮点运算、参数量达到2万亿，或能力达到全球领先水平的“三选一”标准。该项规定并非将一般大模型普遍纳入，而是通过规模和能力门槛，将关注重点集中于前沿模型。这一导向也可以结合国际规则与市场数据理解：

技术名称及类型			核心能力关注
信息识别与处理	高性能检测技术	深度合成图像、音视频或多模态信息的**检测系统及设备制造技术**	**检得准、漏得少**：准确辨别合成信息，同时减少漏检，准确率和召回率达到98%。
		视频、图像**信息隐写与提取技术**	**藏得隐、取得稳、少误报**：隐藏信息不易被察觉，提取结果可靠，并减少错误识别。
	信息处理技术	**语音声纹识别技术**，包括： • 声纹核心算法技术 • 防攻击与反伪造技术 • 声纹识别系统技术 • 声纹数据处理与保护技术等	**认得准、处理快、防冒充**：准确识别说话者身份，快速处理请求，识别录音回放、语音合成等欺诈；另关注**对少数民族语言或特定地域方言的识别能力**。
		专门或者主要用于汉语及少数民族语言的**翻译技术**	**译得准、质量高**：重点关注翻译质量及对原文含义的忠实程度，覆盖通用及专业场景。

		技术	求。
网络安全与对抗	信息对抗技术	人工智能**辅助漏洞挖掘技术**	**找得到、判得准、利用能力强：**能够发现漏洞、判断其能否被利用，进一步构建利用链，并在效率、自主性或发现数量上达到较高水平。
大模型与智能体	人工智能**大模型技术**	利用我国**重要数据**进行训练后提供服务的**大模型**	**以数据来源划定范围：**未另设技术能力门槛，并对符合条件的微量重要数据使用、合法公开获取等情形作出排除。
		权重参数、关键检查点、底层源代码、架构设计，以及训练优化、推理加速等**核心技术**	**规模大或能力领先：**从计算量、参数量或全球领先水平三个角度识别，满足其中一项即可。
	人工智能体技术	• 自主规划与任务分解技术 • 多智能体协同架构技术 • 工具调用与系统操作技术 • 人工智能博弈决策技术	**会规划、能协作、会用工具、能动态决策：**各技术方向分别关注复杂任务的拆解与执行、多智能体协同、多工具调用，以及动态环境中的策略调整能力，并设定具体量化指标。

芯片与算力集群	人工智能**芯片设计技术**	**处理芯片设计**技术	**能计算、善互联、支持新架构或特定应用：**关注计算功能、高速互联、先进封装及新型架构等条件，也覆盖自动驾驶、视觉、语音等应用场景。
		存储芯片设计技术，包括： • 3D 闪存芯片设计技术 • 内存芯片设计技术	**存得密、传得快、集成度高：**分别从存储密度、数据传输速率、制造工艺，以及键合、堆叠等结构条件划定范围。
	人工智能**算力集群技术**	• 片间或节点间**高速互连**技术 • 分布式**训练容错**技术 • 高效**通信调度**技术 • **异构集群**高效推理与调度技术	**连得上、速度快、跑得稳、用得好：**面向加速卡总数超过 1 万张的集群，关注高速连接、通信效率、故障恢复，以及不同厂商芯片和跨地域算力的协同利用。

国际规则：我国本次拟设计算量门槛在数值上比欧盟高一个数量级，与美国加州识别前沿模型的标准相当，体现出中美作为科技大国通过较高技术门槛聚焦前沿模型监管的相近思路。欧盟：《人工智能法案》（AI Act）第51条以训练累计计算量超过10^{25}次浮点运算作为“通用目的AI模型”系统性风险分类的推定门槛；美国：加州《前沿人工智能透明度法》（SB 53）以训练计算量超过10^{26}次整数或浮点运算界

定“前沿模型”，对其开发者施以发布透明度报告、报告重大安全事件等义务。市场数据：结合近期国内主流厂商已公开的模型参数来看，2万亿参数属于相对较高的规模指标。达到这一规模的主要集中于部分旗舰型号，多款通用模型尚未达到，体现出该项参数门槛较为明确的筛选和限缩作用。

下表从通俗角度概括各项技术的核心能力关注。考虑到AI技术快速迭代，且目前《目录》仍处于征求意见阶段，具体技术指标及适用条件后续可能会持续调整。

二、出口行为：围绕技术转移辨析典型出海场景

结合《中华人民共和国技术进出口管理条例》第2条，技术出口包括通过转让、许可、技术服务等方式将技术从中国境内向境外转移的行为。本次商务部官方答记者问进一步明确，判断人工智能出海是否属于技术出口管理范围，核心在于是否涉及限制类技术从中国境内向境外转移。进一步推理可得：转移是外观，核心是控制，故出口行为应基于针对受控技术“控制力”的转移情况来判断。

下文将结合人工智能企业常见的出海场景，进一步分析不同业务模式下的技术出口认定及其监管边界。

（一）模型海外部署：部署环境与模型形态影响具体管理安排

人工智能模型的海外部署涉及不同的技术交付方式和运行环境，相应的监管要求亦有所区别。商务部明确，相关措施正式实施后，限制类人工智能技术的海外本地化部署属于技术出口管理范围，但海外自有云等风险相对可控的情形拟适用自动许可等便利措施，本地端侧轻量化部署则不属于所述大模型技术出口管理范围。

场景一：海外客户私有化部署

中国企业将大模型权重、推理程序及部署文件交付至境外客户服务器，由客户独立部署和运行。此类安排涉及模型技术的跨境转移，只要相关技术符合《目录》的管制条件，即使中国企业保留知识产权，仍属于技术出口管理范围。

场景二：海外自有云部署

中国企业将受控模型部署至境外自有云环境，自行运营并通过API等方式向境外用户提供服务。虽然用户无需取得底层技术，但模型本身已发生跨境转移，仍属于技术出口管理范围。对此，商务部拟适用自动许可等便利措施，基本实现“即报即出”。

实践中，企业也可能租赁AWS、Azure等第三方云平台的计算资源，自行管理模型权重及访问权限。此类部署能否纳入“海外自有云”的范围并适用便利措施，仍是后续政策实施中值得关注的问题。

场景三：本地端侧轻量化部署

部分企业通过蒸馏、量化、剪枝等方式，将大模型转化为可在手机、电脑等终端设备上运行的轻量化模型。商务部明确，此类本地端侧轻量化部署不属于所述大模型技术出口管理范围。

不过，“轻量化”的具体认定标准尚未明确，对于基于受控基础模型开发、仍保留较强技术能力的端侧模型，能否适用上述排除安排，仍需审慎判断。

（二）API及SaaS服务：区分模型服务与技术交付，仅提供功能原则上不受控

商务部明确，利用限制类大模型向境外提供API调用、APP/网页交互及SaaS等服务，不属于所述大模型技术出口管理范围。此类模式下，境外用户获取的是模型功能及输出结果，而非模型权重、核心代码等底层技术。但涉及模型微调、蒸馏等定制化应用时，仍需关注是否向境外交付受控技术。

另需要区分的是，模型服务与模型部署属于不同环节；如提供服务前已将受控技术转移至境外部署，仍需就该部署环节另作判断。

场景一：模型微调（Fine-tuning）

境外客户提供数据，由中国企业在境内完成模型微调，并仅通过API提供定制化服务的，通常仍属于模型服务，不属于前述大模型技术出口管理范围；如进一步向境外交付微调后的模型权重等技术成果，则需判断交付内容是否符合《目录》的管制条件。

场景二：模型蒸馏（Distillation）

境外开发者自行利用API输出开展模型蒸馏，通常不能仅据此认定中国企业实施了受控技术出口。但如中国企业有意为境外客户开展模型蒸馏提供便利，并交付衍生模型或相关核心技术，则需结合交付内容及《目录》的管制条件进一步判断。

（三）跨境研发与技术合作：技术出口可能发生在技术指导和研发过程中

跨境研发与技术合作涉及技术指导、境外算力及研发平台使用、研发成果共享等多种场景，需关注受控技术是否在相关过程中向境外转移。

场景一：跨境技术指导

中国企业派遣技术人员赴境外提供技术指导，或由境内团队通过远程会议、协作平台向境外合作方传授符合《目录》管制条件的模型架构、训练优化方法等技术，即使未交付完整模型，也可能通过技术服务等方式实现受控技术的跨境转移。

场景二：利用境外资源开展研发

中国团队仅利用境外数据或算力开展研发，且未向境外传输受控技术的，通常不涉及受控技术出口；但如将受控模型权重、核心代码等上传至境外服务器，则可能构成受控技术出口。对于利用境外资源开展联合研发而发生的限制类技术出口，商务部拟适用自动许可等便利措施，基本实现“即报即出”。

场景三：“研发即交付”

实践中，境内团队也可能从零开展研发，使用境外数据、算力及开发环境，并事先约定成果归境外主体所有。此类模式下，技术成果可能在研发过程中逐步形成并直接存储于境外。如果最终成果属于限制出口技术，可能出现境外合作方已取得相关技术、企业却尚未完成技术筛查的情况，从而增加技术出口合规风险。

对该等情况，建议企业在项目启动初期，结合研发目标、技术方案及预期性能指标，初步判断拟形成的成果是否可能落入管制范围。对于可能涉及受控技术的项目，宜提前安排研发成果的存储及交付方式，尽可能保留对成果的管理和交付权限，并结合研发进展及时复核，以便履行必要的出口管理手续。

（四）模型开源：限制类技术开源拟享便利，已进入公共领域的技术不纳入管理范围

模型开源也可能涉及受控技术向境外转移。对于拟开源的限制类技术与已进入公共领域的技术，适用不同的管理安排。

对于拟开源且符合《目录》限制出口条件的技术，商务部拟适用自动许可等便利措施，基本实现“即报即出”；对于已通过开源、发表学术论文等方式进入公共领域的相关技术，商务部明确不纳入此次管理范围。

实践中，已开源模型所涉技术是否均已进入公共领域仍需具体判断。例如，即使模型权重已开源，尚未公开的训练方法、核心代码，以及后续版本新增的技术，也不能当然适用上述排除安排，仍需结合《目录》的管制条件进行评估。

（五）技术权属与控制关系变更：技术资料未实际出境也可能触发登记

此次公告除将技术所有权转让、境外使用授权纳入临时登记范围外，还明确包括“境内技术的所有权人或者实际控制人变更为境外主体”的情形。这意味着，除直接的技术转让或许可外，其他涉及技术权属或控制关系变化的交易，也可能触发登记要求。

例如，境外投资者收购境内AI企业，或集团内部通过股权重组、架构调整等方式调整相关技术的持有及控制关系，即使未伴随模型权重、源代码等技术资料的跨境交付，也需关注是否涉及临时登记要求。

上述规定虽未改变现行技术进出口的法定定义，但体现了监管对技术权属及实际控

制关系变化的进一步关注。

三、监管安排：登记先行，把握规则完善窗口与便利措施

（一）监管过渡期：管制方向已明确，具体规则仍有意见反馈空间

结合前期评估、临时登记及公开征求意见等安排，我们理解，监管将相关AI技术纳入出口管理的方向已较为明确，具体范围和实施安排仍可能会有进一步完善的空间。企业宜在评估业务影响、做好合规准备的同时，及时反馈实际需求与适用疑问。

一方面，相关监管已在推进，企业宜提前准备。据官方答记者问，此次修订前，主管部门已组织研究机构、行业组织开展评估，并听取主要企业的意见建议；公告也已依据《对外贸易法》第18条、第20条启动临时登记。这些安排表明，此次调整已有前期研究和具体管理措施支撑，企业宜尽早梳理相关技术与业务，评估拟议规则可能带来的影响。另一方面，监管强调精准审慎，具体规则仍可能有调整空间。此次《目录》修订强调列管范围精准有限，并拟为正常技术合作提供便利，体现出对AI技术管制的审慎态度。在前期听取企业意见的基础上，本次公开征求意见进一步扩大了意见征集范围。企业如对技术范围、指标或实施安排仍有意见，可结合实际业务及时反馈，为监管规则完善提供参考。

（二）过渡期实操：落实登记义务，为适用自动许可等便利措施做准备

1. 临时登记：及时排查技术与交易，落实出口前登记要求

临时登记自2026年10月16日公告发布之日起实施，持续至《目录》正式修订并实施之日。属于公告登记范围的技术出口，应在出口前通过商务部业务系统统一平台的“技术贸易管理信息应用”办理登记。

从制度性质上来看，临时登记可视为国家在实施技术出口管制前开展信息摸排与风险监测的工具。据此，我们建议企业积极落实登记义务：一方面是为了满足当前合规要求；另一方面，企业可借登记契机梳理自身技术资产，评估相关技术出口是否存在管制风险，实现风险前置识别。

企业开展排查时，可重点关注以下两点：

存量交易也需纳入排查。已经开始但尚未完成的出口同样属于登记范围。例如，公告发布前已签约，但相关技术尚未交付或仍在分批交付的交易，也需纳入排查。适用范围需先由企业自行判断。企业宜结合技术清单、合同及实际交付安排，核对是否涉及公告所列技术与登记情形；存在认定疑问的，可及时向商务部、科技部咨

询。

2. 自动许可：为开放合作提供便利，但企业仍需规范申报

结合官方答记者问，自动许可等便利措施可基本实现“即报即出”，体现了鼓励开放合作的政策导向。我们理解，这类安排是在监管保留必要申报、掌握技术跨境流动情况的同时，为符合条件的限制类技术出口提供便捷通道。但这并不意味着免除申报责任，企业仍应确保申报信息真实、准确、完整，并核实相关技术及业务场景符合适用条件。

根据征求意见稿及官方答记者问，自动许可等便利措施拟仅适用于限制类技术出口，主要涵盖以下情形：

（1）技术开源；

（2）中国企业在境外自建自营算力中心；

（3）赴境外开展芯片流片制造；

（4）利用境外资源开展联合研发；

（5）参与国际标准制定；

（6）限制类人工智能技术部署在海外自有云等风险相对可控的环境。

不过，现行技术出口许可涉及提出申请、取得许可意向书、开展实质性谈判与签约、取得技术出口许可证及合同生效等环节。自动许可如何衔接上述流程，申报与办理应安排在哪个节点，仍需结合后续规则及办理实践进一步明确，企业可持续关注相关实施安排。

（三）未来展望：审慎管控敏感与前沿技术，持续跟进《目录》调整

技术出口管制有助于维护国家安全与技术竞争优势，但也可能增加跨境合作成本，影响技术交流与产业发展。如何在保护关键技术与支持开放合作之间取得平衡，是监管需要持续面对的重要课题。

本次修订通过精细化条件限定列管范围、拟为特定场景提供便利，并明确根据技术发展动态调整《目录》，体现出对上述关系的审慎考量。我们理解，这对企业释放了积极信号：监管重点有所聚焦，正常技术合作仍有空间，企业也更有条件结合自身技术和业务安排规划出海路径。

企业可据此分阶段做好准备：短期内，落实临时登记，梳理技术资产及相关出海业务；长期则持续跟进《目录》和实施规则的变化，将技术研发、跨境合作与交付安排等纳入合规管理，并及时评估便利措施的适用可能性。

本文作者

杨建媛 (YANG Jianyuan)

合伙人

yangjianyuan@haiwen-law.com

扫描二维码
查阅律师简历

赵雅泽 (ZHAO Yaze)

zhaoyaze@haiwen-law.com

杜金阳 （DU Jinyang）

dujinyang@haiwen-law.com

张梅然（ZHANG Meiran）

zhangmeiran@haiwen-law.com

声明：本文不代表海问律师事务所对于任何相关问题的法律意见，如您需要法律意见或专业分析，请咨询本文相关作者。如需转载或引用该等文章的任何内容，请注明出处。未经本所书面同意，不得转载或使用该等文章中包含的任何图片或影像。如您有意就相关议题进一步交流或探讨，欢迎与本所联系。