

2025 年 5 月 19 日

第 15 期

总第 690 期

人工智能扩散框架

【译者按】2025 年 1 月，美国商务部工业和安全局（BIS）修订《出口管理条例》（EAR），并发布《人工智能扩散框架》（简称“框架”）。框架旨在加强美国对先进芯片和 AI 模型的控制，创建值得美国及其盟友信赖的生态系统。框架修订了先进计算芯片的管制措施，针对先进芯片创建了三项新许可例外，并更新了需通知先进计算（NAC）许可例外、先进计算许可例外（ACA）和数据中心最终用户授权规则；框架概述了 AI 模型的管制措施、许可例外资格和警示指南。赛迪智库电子信息研究所对框架中的主要内容进行了编译，期望对我国有关部门有所帮助。

【关键词】人工智能 先进芯片 AI 模型 管制 中美

1.摘要

美国商务部工业和安全局（BIS）通过一项临时最终规则，即本《人工智能扩散框架》，修订了《出口管理条例》（EAR）中有关先进计算集成电路（IC）的管制措施，并增加了一项针对某些先进的封闭式权重两用人工智能（AI）模型的人工智能模型权重管制措施。工业和安全局认为，为了保护美国国家安全和外交政策利益，扩大这些管制措施是必要的。与此同时，工业和安全局还引入了新的许可例外条款，并更新数据中心验证最终用户授权，以促进向不引起国家安全或外交政策问题的目的地的最终用户出口、再出口和转让（在国内）先进计算（集成电路）。这些变化将共同为人工智能和先进计算集成电路的负责任扩散和使用培育安全的生态系统。

2.背景

工业和安全局正在修订《出口管理条例》，扩大对ECCN（出口管控分类编号）3A090.a和4A090.a下受控的先进计算集成电路以及相应的.z物项的现有管制，并对新设立的ECCN 4E091下受控的某些先进封闭式权重两用人工智能模型的模型权重实施新的管制措施。美国政府广泛考虑了先进的军民两用人工智能模型对美国国家安全和外交政策利益的影响，下文将详细介绍这些

变化的背景。

《2018 年出口管制改革法案》（ECRA）（《美国法典》第 15 编第 4801 条等）强调，国家安全“要求美国保持其在科学、技术、工程和制造领域的领先地位，包括对创新至关重要的基础技术”。该法案还要求工业和安全局的规则“透明、可预测、及时”，并根据不断变化的情况“灵活调整”。

a. 先进人工智能模型的风险和优势

美国政府的专家们已经确定，随着这些模型能力的不断提高，它们将使恶意行为者能够从事对美国国家安全和外交政策目标构成深远风险的活动。正如美国国家情报总监办公室所评估的那样，人工智能模型有可能实现先进的军事和情报应用；降低非专家开发大规模杀伤性武器（WMD）的准入门槛；支持强大的进攻性网络行动；以及协助侵犯人权行为，如通过大规模监控。详见 2024 年 2 月 5 日国家情报总监办公室的《美国情报界年度威胁评估》。例如，根据描述化学合成物或生物序列的功能和机理的数据训练的两用人工智能模型，可以通过提供协议和故障排除信息，使非专业人员能够以低成本设计和生产此类武器，从而降低开发化学或生物武器的障碍。同样，国土安全部已确定，人工智能的进步可能会降低国家和非国家行为者开发大规模杀伤性武器的准入门槛，从而增强恶意行为者实施威胁美国国家安全的

攻击的能力。详见 2024 年 4 月 26 日国土安全部关于降低人工智能与化学、生物、放射及核威胁交叉点的风险的报告。

与此同时，美国政府的专家们已经确定，经验证实体在安全条件运行军民两用人工智能模型将有可能在美国和全球创造巨大的经济和社会效益。正如工业和安全局在之前的规则中解释的那样，军民两用人工智能模型有可能增加人们获得医疗保健、教育和食品的机会，并有助于应对气候变化等复杂问题。

b.人工智能扩散政策审查

认识到先进人工智能模型的益处和风险，美国商务部与美国政府各部门的合作伙伴开展了广泛而持续的政策进程，以考虑对先进人工智能技术向全球实体和目的地的扩散进行战略性、专门和有效管制。2022 年 10 月，美国工业和安全局对某些目的地实施了第一套管制措施，目的是通过限制其获得先进计算集成电路和某些用于制造先进计算集成电路和其他先进节点集成电路的半导体制造设备（SME），防止某些外国军事和情报部门获得自主开发先进武器建模和先进人工智能能力的的能力。工业和安全局认定，这些外国军事和情报部门将利用先进的人工智能来提高其军事决策、规划和后勤的速度和准确性，以及其自主军事系统，如用于认知电子战、雷达、信号情报和干扰的系统。工业和安全局还认定，这些军事和情报部门将无视人权，通过使用先进的人

工智能监控工具高效处理海量数据来监控、跟踪和监视公民，以及开展其他行动。因此，工业和安全局既管制了先进的计算集成电路，也管制了制造受控集成电路的半导体制造设备。

从那时起，工业和安全局不断评估和更新工业和安全局的管制措施，以确保它们尽可能有针对性和有效地保护美国的国家安全和外交政策。2023 年，工业和安全局更新了其先进计算管制的技术参数，并扩大了这些管制所适用的目的地范围，以涵盖 2022 年管制未涵盖的有关国家。工业和安全局还对代表总部设在国家组 D:5 或澳门的实体进行的先进计算集成电路活动和某些半导体最终用途实施全球许可要求。2024 年，工业和安全局对人工智能和半导体制造设备管制的范围进行了界定，并认识到促进负责任地推广先进人工智能技术的重要性，扩大了验证最终用户（VEU）授权的范围，使数据中心能够获得验证最终用户授权。该授权允许受许可要求限制的地点的实体在安全条件下通过简化流程接收受管制物项。工业和安全局在这一领域的工作符合美国支持全球发展的外交政策。

在过去的一年中，工业和安全局与来自美国政府各部门的国家安全和外交政策专家——包括国防部、能源部、国务院以及情报界的机构间出口管制合作伙伴——共同研究对先进人工智能技术的额外管制是否以及如何促进美国的国家安全和外交政策。

如下文所述，他们首先研究了如果允许最先进的人工智能模型或开发这些模型所需的物项通过目的地扩散到世界各地将产生的风险和益处。同时，他们还与技术专家合作，了解管制这些物项扩散的最有效手段，以应对风险。该规则详细说明了多部分管制结构，旨在降低相关国家（国家组 D:5 和澳门）获得最先进人工智能模型的风险，并使经过验证的实体能够获得这些模型的好处，同时保护国家安全。

i. 人工智能扩散对国家安全和外交政策的影响

先进人工智能模型在全世界的扩散将从三个根本方面影响美国的国家安全和外交政策利益。

首先，向美国以外的任何目的地出口先进的人工智能模型或生产这些模型的手段，都会增加盗窃或转移到相关国家和最终用户的风险。虽然不同目的地和最终用户的风险程度不同，但即使最终用户是经过验证的实体，目的地是拥有健全出口管制制度的美国盟国，也存在风险。

其次，除非美国以外的经验证实体本身能够获得大量先进计算集成电路或先进人工智能模型，否则先进人工智能模型的经济和社会效益将无法充分实现。这些实体可能会发现仅靠美国公司无法发现的有益应用，它们可能会增加先进人工智能模型惠及全世界人民的可能性。

第三，美国的国家安全要求美国保持在全球人工智能行业的技术领先地位。工业和安全局认为，为了保持美国在人工智能领域的领先地位，美国的先进人工智能模型开发商可能需要在美国境外建立大型先进计算集成电路集群。他们可能还需要在国外的设施中存储其模型，以确保能够向经过验证的外国客户提供高质量的服务。

ii. 负责任地控制人工智能扩散的手段

人工智能模型是由一系列数学运算组成的软件程序。当用户向程序输入数据时，程序会对输入数据执行这些运算，从而产生输出——信息、分析或媒体。这些运算的设计及其排列（称为模型结构）决定了模型输出的性质和质量。

训练当今最先进的人工智能模型，包括大型语言模型（LLM），需要能够处理大量数据和包含大量参数的模型的大型先进计算集成电路集群。人工智能模型的进步部分源于用于开发最大型人工智能模型的计算能力和训练数据的大幅增加。人工智能模型的结构和这些行业趋势表明，出口管制可以通过以下方式有效规范先进人工智能模型的全球扩散：（1）扩大对先进计算集成电路出口、再出口和转让（国内）的现有管制，这些集成电路是构建用于训练先进人工智能模型的大型集群所必需的；（2）对最先进人工智能模型的模型权重的出口、再出口和转让（国内）实施

新的管制。

iii. 先进人工智能技术扩散框架

该规则详细说明了控制先进人工智能模型扩散的专门战略方法。在高层次上，该战略旨在确保美国最先进的人工智能模型的模型权重仅在严格的安全条件下存储在美国境外，并且确保训练这些模型所需的大型先进集成电路集群建在转移或滥用风险相对较低的目的地。

本规则规定，向任何目的地的任何最终用户出口、再出口或转让（国内）先进计算集成电路或最先进人工智能模型的模型权重，必须获得许可。美国政府将根据目的地的敏感性、人工智能模型的计算能力或性能数量以及接收方同意的安全要求，对此类出口、再出口和（国内）转让申请进行审查。这一全球许可要求对于确保这些物项不被转移到令人担忧的目的地或最终用户至关重要。为了减轻转移或滥用风险相对较低的目的地和最终用户的负担，并促进经济上有益的活动，工业和安全局增加了其全球许可要求的灵活性。

工业和安全局正在通过以下方式实施这项战略：

（1）在新的出口管制分类编号（ECCN）4E091 下增加一项新的人工智能模型权重管制措施；

（2）修订 ECCN 3A090.a、4A090.a 和相应.z 项的许可要求

和审查政策；

（3）扩大经授权的先进计算（ACA）许可例外的国家范围；

（4）增加适用于先进计算集成电路、人工智能模型权重和相关物项的新人工智能授权（AIA）、先进计算制造（ACM）和低运算性能（LPP）许可例外；

（5）增加与人工智能模型权重相关的新红旗警示；

（6）将数据中心验证最终用户授权分为通用和国家验证最终用户授权；以及

（7）更新需通知先进计算（NAC）许可例外通知程序。

3.修订先进计算集成电路管制措施

如上所述，大型先进计算集成电路集群对开发先进人工智能模型至关重要。因此，工业和安全局可以通过实施管制，只允许向特定目的地和最终用户出口、再出口和转让（在国内）大量先进计算集成电路，从而降低恶意国家和非国家行为者获取先进人工智能模型的风险。与此同时，工业和安全局可以确保符合严格安全标准的目的地和最终用户能够获得大量先进计算集成电路。

对建造大型先进计算集成电路集群的管制是工业和安全局以往管制措施的合理延伸——以往管制措施的重点是允许少量的先进集成电路和相关半导体制造设备出口或再出口到某些目的

地——这样会对美国国家安全和外交政策造成风险。之前的这些管制措施是基于工业和安全局的判断，即这些目的地的军事和情报部门可能会利用哪怕只是少量的先进计算集成电路来提高其军事能力——这有悖于美国的国家安全和外交政策利益。

2022 年 10 月，工业和安全局发布了一项临时最终规则(87 FR 62186)，在两个方面对《出口管理条例》进行了重要修改。首先，该规则对某些先进计算集成电路、包含此类集成电路的计算机商品、某些半导体制造设备以及生产此类和其他先进集成电路所需的零部件实施了额外的出口管制。工业和安全局解释说，这些管制旨在限制中华人民共和国从事对美国国家安全和外交政策构成重大威胁的活动的的能力。

此后，在 2023 年 10 月，工业和安全局扩大了先进计算管制的范围，以涵盖其他相关目的地（国家组 D:1、D:4 和 D:5）。同样，工业和安全局对总部设在澳门或最终母公司设在澳门的实体或国家组 D:5 中的目的地的某些先进计算集成电路以及特定半导体制造和超级计算最终用途实施全球许可要求。由于人工智能技术变化迅速，工业和安全局一直在密切研究这些发展，并相应地更新其规则，以确保这些规则尽可能保持针对性和有效性。

工业和安全局还修改了其管制措施，以促进向某些同意在安全生态系统中使用这些物项的最终用户出口先进计算集成电路

和相关物项。2024 年 10 月，工业和安全局扩大了第 748.15 节中的验证最终用户（VEU）授权，将验证最终用户授权扩大到数据中心（89 FR 80080，2024 年 10 月 2 日）。工业和安全局解释说，数据中心对全球人工智能发展至关重要，美国致力于以尽量减少对美国国家安全的风险的方式促进国际人工智能发展。因此，工业和安全局扩大了验证最终用户授权，以促进向目的地（D:5 国家除外）预先批准的验证最终用户出口或再出口数据中心所需的物项，但前提是这些目的地需要获得 ECCN 分类为 3A090.a、4A090.a 和 .z 的第 3、4 和 5 类物项的许可。

自 2024 年 12 月 2 日起，工业和安全局扩大了对先进计算集成电路以及生产此类集成电路所需的半导体制造设备、软件和技术的管理制，这些集成电路可实现涉及国家安全的人工智能应用。具体来说，工业和安全局对某些高带宽内存（HBM）商品实施了新的管制措施。工业和安全局还对能够生产先进计算集成电路的其他半导体制造设备（如某些蚀刻、沉积、光刻工具等）以及能够增强此类半导体制造设备能力或可用于设计先进计算集成电路的软件实施管制。

本规则对 ECCN 分类为 3A090.a、4A090.a 的先进集成电路和第 742.6（a）（6）（iii）（A）节中的相关 .z 物项的出口作出了全球许可要求，然后规定了几种例外情况和授权途径，以促进转

移风险较低或可促进美国国家安全或外交政策利益（包括技术领先地位）的交易。如本规则其他部分所述，这些规定也符合美国有关全球发展的外交政策。

首先，该规则在新的第 740.27 节中为涉及某些低风险目的地的某些类型最终用户的所有交易规定了例外情况。具体来说，这些目的地包括符合以下条件的地方：（1）政府已采取措施防止先进技术的转移，（2）存在一个生态系统，使企业能够并鼓励企业使用先进的人工智能模型来推进美国及其盟友和合作伙伴的共同国家安全和外交政策利益。这些目的地列在第 740 部分第 5 号补充条款（a）款中，包括澳大利亚、比利时、加拿大、丹麦、芬兰、法国、德国、爱尔兰、意大利、日本、荷兰、新西兰、挪威、大韩民国、西班牙、瑞典、台湾、英国和美国。对于这些目的地，本临时最终规则的改动极小：这些目的地的公司只要证明符合第 740.27 节规定的具体要求，一般无需许可即可获得最先进的集成电路。

其次，工业和安全局对向国家组 D:5 目的地和澳门提供这些物项的严格规则不作任何改动。

第三，对于所有其他目的地，即非澳门、国家组 D:5 或第 740 部分第 5 号补充条款（a）款所列目的地，本规则建立了一个多部分框架，其中考虑到了交易的计算能力，以及（在某些情况下）

接收方同意的安全措施。首先，工业和安全局正在为数量有限的先进集成电路（即数量远远低于训练最先进的人工智能模型所需的数量）设立许可例外。只要出口商向工业和安全局发出通知，这一许可例外规定就能确保无意促进先进人工智能模型开发的交易不受阻碍地继续进行。涉及大量受控集成电路的交易将受新许可政策的制约，因为该政策规定，出口的集成电路数量不得超过特定国家的分配数量。为了提供可预测性，工业和安全局正在为 2025 年至 2027 年这一时期的分配做出具体规定。这一许可政策将使这些目的地的最终用户能够开发任何前沿领域之外的人工智能模型，从而使他们能够获得这些模型的经济效益，同时保护美国免受最重大的威胁。

与此同时，该规则还使这些目的地的实体能够获得经验证的身份，以便根据验证最终用户授权获得数量大得多的集成电路。验证最终用户授权允许同意采取具体、可核查和强有力的安全措施的实体获得大量先进集成电路，从而推进了美国的国家安全和外交政策。对于这些目的地的最终用户，即不属于澳门、国家组 D:5，也不属于第 740 部分第 5 号补充条款（a）款所列的最终用户，如果不符合国家验证最终用户授权的资格标准，工业和安全局正在实施先进集成电路的统一默认国家分配。自本规则生效之日起，先进集成电路的出口和再出口将计入这些分配额。这些分

配将限制先进集成电路被转移的风险，并鼓励这些实体满足获得验证最终用户授权的条件。这样，验证最终用户授权也将支持美国支持全球发展的外交政策。

A.新的全球许可要求

通过本临时最终规则，工业和安全局在新的第 742.6(a)(6)(iii)(A) 节中为 ECCN 3A090.a、4A090.a 和相应的.z 物项制定了全球许可要求。对这些物项的全球许可要求，包括那些通过先进计算外国直接产品规则 (FDPR) 受《出口管理条例》管辖的物项，将保护美国的国家安全和外交政策利益，使工业和安全局能够仔细检查任何转移或滥用风险较高的交易，并使美国政府能够了解先进集成电路的位置、最终用户和最终用途。此外，如下文所述，通过数据中心验证最终用户授权推广人工智能计算，将使世界各地的公司受益于在经过验证和保护的环境中分配人工智能计算。

ECCN 3A090.a 管制具有一个或多个数字处理单元的集成电路，其：(1) “总运算性能”达到或超过 4800；或(2) “总运算性能”达到或超过 1600 且“性能密度”达到或超过 5.92。ECCN 3A090.b 管制具有一个或多个数字处理单元的集成电路，其：(1) “总运算性能”达到或超过 2400 且小于 4800，“性能密度”达到或超过 1.6 且小于 5.92；或(2) “总运算性能”达到或超过

1600, “性能密度”达到或超过 3.2 且小于 5.92。

除了扩大对 ECCN 3A090.a 和 4A090.a 物项的国家管制范围, 工业和安全局还扩大了第 734.9 (h) (2) (i) 节中先进计算外国直接产品规则的目的地范围。工业和安全局用“全球”一词取代了国家组 D:1、D:4 和 D:5, 以及被排除在外的 A:5 和 A:6。因此, 现在的措辞规定, 如果“知道”外国生产的物项将运往全球, 或将安装到未指定为 EAR99 的任何“部件”、“组件”、“计算机”或“设备”中且将运往全球任何目的地, 则该外国生产的物项符合本 (h) (2) 款的目的地范围。

B. 3A090、4A090 及相应的.z 项和 4E091 的许可例外

根据本规则, 工业和安全局将在《出口管理条例》中增加三个适用于先进计算集成电路的新许可例外: 第 740.27 节人工智能授权许可例外、第 740.28 节先进计算制造许可例外和第 740.29 节低运算性能许可例外。此外, 它还在更新经授权的先进计算 (ACA) 许可例外的目的地范围。工业和安全局还在更新需通知先进计算流程, 以提高处理效率。作为更新流程的一部分, 工业和安全局和其他机构正在向需通知先进计算用户征集更多信息。

1. 人工智能授权 (AIA) 许可例外

这一新的许可例外规定授权向位于第 740 部分第 5 号补充条款 (a) 款所列目的地的实体出口、再出口或 (在国内) 转让符合

条件的先进计算集成电路及相关软件和技术，除非该实体的总部位于补充条款（a）款所列目的地之外，或其最终母公司的总部位于补充条款（a）款所列目的地之外。见第 740.27（a）节。

2. 先进计算制造（ACM）许可例外

新先进计算制造许可例外授权出口、再出口和（在国内）转让符合条件的物项（ECCN 3A090、4A090 和相关的.z 项商品、软件和技术）给位于非国家组 D:5 或澳门所列目的地的“私营部门最终用户”，条件是，如果这些最终用户的最终目的是“开发”、“生产”或（在仓库或其他类似设施中）储存这些符合条件的物项，这些用户的总部不在澳门或国家组 D:5 指明的目的地，且其最终母公司不在澳门或国家组 D:5 指明的目的地。如果物项的最终用途是训练人工智能模型或与“开发”、“生产”或（在仓库或其他类似设施中）储存此类符合条件的物项无关的任何其他活动，则实体不得使用此例外。

3. 低运算性能（LPP）许可例外

新增的第 740.29 节所规定的新的低运算性能许可例外授权向任何单个最终收货人出口和再出口不构成重大国家安全风险的低数量计算，即总运算性能每个日历年最高可达 26,900,000 的先进计算集成电路。

4. 更新 ECCN 3A090、4A090 和相应.z 项的需通知先进计

算许可例外和经授权的先进计算

目前，根据第 740.8 (a) 节，需通知先进计算 (NCA) 许可例外和经授权的先进计算 (ACA) 许可例外适用于 ECCN 编号为 3A090、4A090、3A001.z、4A003.z、4A004.z、4A005.z、5A002.z、5A004.z、5A992.z、5D002.z 或 5D992.z 的物项，但为在数据中心使用而设计或销售并符合 3A090.a 参数的物项除外。需通知先进计算 (NAC) 许可例外授权向澳门和国家组 D:5 中指定的目的地以及总部设在澳门或国家组 D:5 中指定的目的地的实体或其最终母公司设在澳门或国家组 D:5 中指定的目的地的实体出口和再出口指定物项，无论其位于何处，均需向工业和安全局发出通知。经授权的先进计算许可例外授权向国家组 D:1 及 D:4 (澳门、D:5 国家组目的地、总部或最终母公司设在澳门或 D:5 国家组目的地的实体除外，无论其位于何处) 指定的任何目的地或在其境内出口和再出口任何 ECCN 编号为 3A090、4A090、3A001.z、4A003.z、4A004.z、4A005.z、5A002.z、5A004.z、5A992.z、5D002.z 或 5D992.z 的物项 (设计或销售用于数据中心并符合 3A090.a 参数的物项除外)，以及在澳门和国家组 D:5 指定的目的地进行 (境内) 转让。第 740.8 (a) 节中的经授权的先进计算许可例外的目的地范围进行了修改，删除了 D:1 或 D:4，代之以“全球任何目的地”。因此，监管规则现在规定：“向全球任何目的地或在全球任何目的

地(澳门、国家组 D:5 指定的目的地或总部设在澳门或国家组 D:5 指定的目的地的实体或最终母公司设在澳门或国家组 D:5 指定的目的地的实体除外, 无论其位于何处), 以及在澳门和国家组 D:5 指定的目的地内的 (国内) 转让” 。

C. 数据中心验证最终用户 (DC VEU) : 通用和国家验证最终用户

2024 年 10 月, 工业和安全局修订了《出口管理条例》, 将验证最终用户授权扩展到数据中心验证最终用户。通过本规则, 工业和安全局进一步扩大了数据中心验证最终用户授权, 将其分为通用验证最终用户 (UVEU) 和国家验证最终用户 (NVEU) 授权。总部设在或其最终母公司总部设在第 740 部分第 5 号补充条款 (a) 款所述目的地的公司可申请通用验证最终用户授权。在某些限制条件下, 总部设在或其最终母公司总部设在除澳门或国家组 D:5 中指定的目的地以外的全球所有目的地的公司, 如希望获得出口、再出口或转让 (在国内) 大量先进计算集成电路的资格, 可申请国家验证最终用户授权。

对于第 748.15 节的新条款所述的所有国家验证最终用户, 每个公司、每个国家的总运算性能 (以受 ECCN 3A090.a、4A090.a 或相应.z 款约束的物项的集体计算能力衡量) 安装基数分配如下:

季度	每个公司、每个国家的累计总运算性能分配额
2025年第1季度	633,000,000
2025年第2季度	949,500,000
2025年第3季度	1,266,000,000
2025年第4季度	1,582,500,000
2026年第1季度	1,899,000,000
2026年第2季度	2,690,250,000
2026年第3季度	3,481,500,000
2026年第4季度	4,272,750,000
2027年第1-4季度	5,064,000,000

这些总运算性能分配额是通过对训练最大人工智能模型所需的人工智能计算集群规模以及这些集群在未来三年可能的增长速度进行广泛分析后确定的。这些分配额的集群规模与工业和安全局认为训练最先进的两用人工智能模型所需的集群规模相差约 12 个月或一代。通过提供三年期路线图，工业和安全局旨在为行业提供可预测性，同时降低最先进的人工智能模型和最大集群在任何特定时间无节制扩散所带来的风险。这些总运算性能分配额代表的是特定季度内允许的累计安装基数，而不是前一季度安装基数之外的新可用总运算性能，并且不计入或影响国家分配额。此外，多个国家验证最终用户可以在一个国家运营，每个国

家验证最终用户都要遵守上述季度分配规定。由于丢失、损坏、故障、搬迁和转售等因素造成损耗的先进计算集成电路将不再计入分配额度。鉴于国家安全需求、地缘政治格局和人工智能产业的不断变化，工业和安全局目前尚未确定未来几年的具体总运算性能分配额。工业和安全局将与国务院、能源部和国防部一起，每年审查随后几年的拨款情况，以确定未来的拨款。

D.许可申请

对于不符合许可例外使用条款和条件的交易，以及最终用户没有参加数据中心验证最终用户授权的交易，可根据《出口管理条例》第 748 部分采用传统的许可申请程序。鉴于国家安全需求、地缘政治格局和人工智能产业的不断变化，工业和安全局目前尚未确定未来几年的具体总运算性能分配。工业和安全局将与国务院、能源部和国防部一起，每年对未来几年的分配情况进行审查。

4.增加人工智能模型权重的管制措施

自本规则于 2025 年 1 月 13 日生效之日起，除了扩大对先进计算集成电路的管制外，工业和安全局还将对最先进的人工智能模型的模型权重实施新的管制。模型权重是“人工智能模型中的数字参数”，“有助于确定模型的输出对输入的响应”。缺乏训练有素的模型权重的人工智能模型会产生毫无意义的输出。此外，

最先进的人工智能模型的开发通常会采用技术保障措施，帮助防止基于模型的应用程序（如聊天机器人或通过应用程序接口提供服务的应用程序）完成某些危险任务，如协助开发核、化学、生物或网络武器。模型权重可能是人工智能模型中最有价值、最受严密保护的要素。

鉴于模型权重对先进人工智能模型运作的重要性，工业和安全局决定，为了保护美国的国家安全和外交政策利益，有必要对最先进的人工智能模型的模型权重实施全球许可要求。工业和安全局与美国政府的技术专家共同确定，人工智能模型性能的一个合理替代指标是用于训练模型的计算量，即计算操作的次数。

通过这项措施，工业和安全局要求出口、再出口或（在国内）转让任何封闭式权重人工智能模型（即权重未公布的模型）的模型权重必须获得许可，而该模型是在超过 10^{26} 次计算操作中训练出来的。由于以少于 10^{26} 次计算操作训练的模型权重已存储在全球各地，而且此类模型可从国外来源获得，因此对此类模型实施管制将是无效的。

此外，工业和安全局没有对开放式权重模型的模型权重进行管制。据工业和安全局评估，在实践中，最先进的封闭式权重模型由其开发者密切掌握。因此，工业和安全局及其机构间合作伙伴今天不会对开放式权重模型实施管制。

为了减少对封闭模型开发者的经济影响，工业和安全局还将不要求出口、再出口或（在国内）转让封闭模型的模型权重的许可，这些封闭模型的模型权重不如最强大的开放式权重模型（由人工智能安全研究所和美国能源部确定）。

A. 人工智能模型权重技术管制

在《商业管制清单》（CCL）中，本规则为先进人工智能模型的“参数”增加了新的 ECCN 4E091 分类，先进人工智能模型被定义为利用 10^{26} 次或更多次“操作”进行训练。“参数”是指训练过程中学习到的任何值（如网络权重、偏差等）。“操作”包括任何后续训练，例如微调预训练模型，但不包括收集和整理输入训练数据。

B. 人工智能模型权重的外国直接产品规则

如上所述，获取先进人工智能模型的模型权重可能使恶意行为者能够推进军事最终用途、开发大规模毁灭性武器、部署进攻性网络行动以及实施侵犯人权行为。例如，直接获取模型权重可能会使恶意行为者利用模型提供制造化学或生物武器的逐步指导，或开发能够进行高级网络攻击的人工智能代理。这种风险适用于在美国境外使用美国技术生产的模型权重，也同样适用于在美国境内生产的模型权重。为应对在美国境外生产人工智能模型权重所带来的国家安全和外交政策风险，本规则在第 734.9 (1)

节中适用了新的外国直接产品规则（FDPR）。根据这一新的人工智能模型权重外国直接产品规则，根据产品范围标准，归类于新的 ECCN 4E091 下的物项在全球任何地点均须遵守《出口管理条例》。许可要求和许可审查政策与 ECCN 4E091 相同。

为符合新的外国直接产品规则产品范围，4E091 物项必须由位于美国境外的完整工厂或工厂的“主要组件”生产，而该完整工厂或工厂的“主要组件”，无论是在美国或外国制造，均受《出口管理条例》管制，并在 ECCN 3A001.z、3A090、4A003.z、4A004.z、4A005.z、4A090、5A002.z、5A004.z 或 5A992.z 中指明。这些 ECCN 分类中所述的集成电路、服务器和其他电子设备，在外国直接产品规则中被视为工厂的“主要组件”，对生产 4E091 中指明的模型权重至关重要。外国直接产品规则还包括一项说明，明确指出 ECCN 4E091 包括任何经过进一步训练的外国生产的物项，包括通过微调和量化等初始训练后的技术。因此，使用 ECCN 3A001.z、3A090、4A003.z、4A004.z、4A005.z、4A090、5A002.z、5A004.z 或 5A992.z 中未指明的物项对外国生产的 4E091 物项进行进一步训练，不会影响该 4E091 物项是否受《出口管理条例》限制。

C. 人工智能模型权重的许可例外资格

新 ECCN 4E091 分类的唯一许可例外是第 740.27 节中新创建

的人工智能授权许可例外。人工智能授权许可例外授权将 ECCN 4E091 下的物项出口、再出口和（在国内）转让至第 740 部分第 5 号补充条款（a）款所列目的地内的实体。本许可例外还授权向总部或其最终母公司总部位于第 740 部分第 5 号补充条款（a）款所列目的地且位于澳门或国家组 D:5 所列目的地以外的任何目的地的实体出口、再出口和（在国内）转让人工智能模型权重，包括 ECCN 4E091 中规定的最先进人工智能模型。

D. 人工智能模型权重红旗警示和指南

在第 732 部分第 3 号补充条款——工业和安全局的“‘了解你的客户’”指南和红旗警示——中，本临时最终规则增加了一个新的红旗警示，以提供合规指南，协助人工智能模型权重的出口商、再出口商和转让商遵守工业和安全局的管制。新的红旗警示第 28 条将帮助位于美国的基础设施即服务（IaaS）云计算提供商识别在为外国实体的美国子公司客户培训先进人工智能模型并将由此产生的模型权重转让给该客户时，会产生潜在的转移问题。在某些情况下，从美国出口模型权重很有可能违反工业和安全局的管制。新的红旗警示第 28 条规定，总部位于第 740 部分第 5 号补充条款第（a）款所列目的地之外的实体的美国子公司使用美国基础设施即服务提供商的产品或服务来训练 ECCN 4E091 范围内的人工智能模型时，根据《出口管理条例》会引发红旗警

示，即模型权重可能会在未经必要授权的情况下出口到相关实体。例如，如果美国基础设施即服务提供商以先进集成电路集群的形式提供基础设施，为单独的人工智能开发组织训练人工智能模型，一旦训练运行完成，由此产生的人工智能模型的模型权重将被转让给到人工智能开发组织。如果美国基础设施即服务提供商为总部位于适用 ECCN 4E091 许可要求的目的地的外国公司的美国子公司提供此服务，则执行培训运行和转让模型权重将产生很大风险，即模型权重将被转让给该实体的最终母公司，从而违反《出口管理条例》，并且基础设施即服务提供商可能协助和教唆了违反《出口管理条例》的行为。

工业和安全局鼓励出口商、再出口商和转让商以及为国内客户提供服务的基础设施即服务提供商，作为其合规计划的一部分，采取更多措施，以确定有关模型权重是否将出口、再出口或转让给受许可要求限制的目的地，如果是，则在出口前申请许可或告知其客户有义务这样做。

译自：*Export Control Framework for Artificial Intelligence Diffusion,*
January 2025 by Bureau of Industry and Security, Department of
Commerce.

译文作者：赛迪工业和信息化研究院 曹智超

联系方式：18632027335

电子邮件：caozhichao@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 15 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：yuansy@ccidtrans.com

