

## 拜登政府之“Eleventh Hour”出口管制规则浪潮：《人工智能扩散框架》与《先进计算芯片额外尽职调查措施》

作者：袁帅琦

2025年1月13日，美国商务部工业与安全局（“BIS”）生效了《人工智能扩散框架》（Framework for Artificial Intelligence Diffusion）的临时最终规则（“1月13日《临时最终规则》”），对美国《出口管理法规》《Export Administration Regulation》（“EAR”）进行修订。该1月13日规则新增对人工智能（“AI”）模型实施出口管制，并基于2022年10月、2023年10月、2024年3月、2024年12月四次对先进计算芯片的出口管制规则修订，再次扩大了出口管制措施范围。《临时最终规则》目前已经生效，但相关合规要求将于2025年5月15日才开始正式适用于出口、再出口以及（国内）转移行为，并且在此之前公众可以就此提交评论。此外，1月16日，美国BIS生效了《实施针对先进计算芯片的额外尽职调查措施；修订和澄清；以及延长评论期》（Implementation of Additional Due Diligence Measures for Advanced Computing Integrated Circuits; Amendments and Clarifications; and Extension of Comment Period）（简称“《额外尽职调查规则》”），主要对1月13日《临时最终规则》涉及有关先进芯片的管制规则进行补充。

本文对上述两项规则的重点内容进行讨论与浅析。

### 一、1月13日《临时最终规则》对先进AI模型权重实施出口管制

#### （1）通过新增ECCN对模型权重实施出口管制

1月13日《临时最终规则》在美国《商业管控清单》（Commerce Control List, CCL）中新增一项出口管制分类编码（Export Control Classification Number, ECCN），即ECCN4E091，基于训练人工智能模型的操作次数实施管制，以此对高性能AI模型权重的出口进行施加许可证措施。“模型权重”是AI模型中的数值参数，有助于确定模型对输入的响应输出，属于人工智能模型中最有价值且受到严密保护的核心要素。

具体而言，根据ECCN4E091，美国对出口、再出口或（国内）转移任何训练超过 $10^{26}$ 次计算操作（operation）的“封闭式（closed-weight）权重AI模型”（即权重未被公布的模型）的模型权重时，必须获得许可证。任何后续训练，如微调预训练模型，将被计算至操作次数，但是该计算不纳入收集和整理输入训练数据。另外，由于开放式权重模型的训练计算操作次数较低，并且具备经济和社会效益，因此ECCN4E091的管制不包括对开放式权重模型。但美国政府将继续监控开放式权重模型可能产生的风险，并评估在风险加剧时可能需要采取的行动。

#### （2）新增“外国直接产品”规则对AI模型实施管控

由于BIS发现非美国实体正在使用美国技术生产的高级计算芯片及相关物项训练AI模型，因此《临时最终规则》新增列一项外国直接产品（Foreign Direct Product, FDP）规则，扩大对AI模型出口管制的域外管辖。也就是说，除美国原产的AI模型权重之外，上述出口管制还可能适用于外国生产的、被归类为ECCN 4E091的AI模型权重。

在满足以下“外国产品范围”和“美国有关设备”的条件的前提下，外国生产的AI模型将受到美国EAR的管辖与管制。首先外国产品范围为：外国生产的AI模型属于ECCN 4E091的技术参数范围。其次，美国有关设备的条件为：（i）该AI模型由美国境外完整设备或设备的主要部件生产，（ii）而该完整设备或设备的主要部件受EAR管辖（无论是否在美国制造）且该完整设备或设备的主要部件属于ECCNs

3A001.z, 3A090, 4A003.z, 4A004.z, 4A005.z, 4A090, 5A002.z, 5A004.z, 或5A992.z。上述ECCN所涉及的芯片、服务器和其他电子设备都将被BIS自动认定为一台设备的“主要部件”，而非次要部件。使用上述ECCN以外的物项对该外国生产的AI模型进行进一步训练（包括微调、量化）后，该外国直接生产的AI模型依然受EAR

管制。

## 二、对ECCN3A090.a等物项的扩大管制

### （一）建立对先进计算芯片物项的“三级管控”框架

根据1月13日《临时最终规则》的规定，BIS现对ECCNs 3A090.a、4A090.a及 742.6(a)(6)(iii)(A)中规定的相关.z 段落下的先进计算芯片物项实施全球性的许可证要求。此前，相关许可证要求仅针对涉及中国以及少数国家的情形。新的出口管制框架基于出口、再出口、（国内）转移先进计算芯片的目的地，建立了三级管制。

#### （1）第一级：白名单国家

基于存在预防物项被转移的措施和共同的国家安全和外交政策利益，美国向EAR第740部分5号补编（a）段所列澳大利亚、比利时、加拿大、丹麦、芬兰等，包括美国自身共19个国家的目的地的最终用户无限量出口、再出口、（国内）转移先进计算芯片相关物项将适用许可证推定批准政策或适用许可证例外。

#### （2）第二级：23个美国实施武器禁运的国家

对于包括中国在内的23个美国实施武器禁运的国家或地区，先进计算芯片相关物项出口、再出口、（国内）转移将适用推定拒绝政策。向总部或最终母公司总部位于上述任何国家的实体出口、再出口或（国内）转移先进计算芯片物项，也将适用拒绝推定。

#### （3）第三级：所有其他国家

2025年到2027年，每个国家能安装的芯片的总处理性能（Total Processing Performance, TPP）不超过790,000,000，相当于每个国家最多获得相当于约5万块 GPU的计算能力。在TPP未超出限额时，相关许可证的政策将为推定批准，TPP超出限额后，将为推定拒绝。经过申请获得NVEU授权（如下所述），则最高可获得5,064,000,000 TPP，相当于最多32万块先进GPU的计算能力。

### （二）出口、再出口或（国内）转移ECCN3A090.a的不利推定

为防止前端制造商（front-end fabricator）和OSAT（外包半导体组装和测试，Outsourced Semiconductor Assembly and Test）公司的客户（即芯片设计商）对其设计的芯片性能进行虚假陈述，以逃避相关出口管制，BIS对ECCN 3A090.a规定了一项不利推定，加强了对相关芯片的许可要求。该项规定将对未获得美国政府授权、批准的芯片设计商造成限制。

《额外尽职调查措施》在ECCN 3A090.a中新增“注释1”：当前端制造商或OSAT公司计划出口、再出口或（国内）转移任何“应适用的先进逻辑芯片（applicable advanced logic integrated circuit）”时，将推定该物项为ECCN 3A090.a，并推定该物项是为数据中心设计或销售。“应适用的先进逻辑芯片”是指，采用16/14纳米节点及以下工艺，或采用非平面晶体管架构生产的逻辑芯片。除非前端制造商和OSAT公司可成功克服该“不利推定”，否则针对ECCN 3A090.a的更为严格的出口管制要求将自动适用于相关芯片。

《额外尽职调查措施》为出口、再出口或（国内）转移ECCN 3A090.a物项推翻“不利推定”提供了如下途径：

（1）先进芯片设计商已经获得BIS的“批准”或“授权”。《额外尽职调查措施》在EAR第740部分新增6号补编，“经批准（approved）的芯片设计商”名单。商务部经过综合考虑，将英特尔、诺基亚、英伟达、索尼等公司列入经批准的芯片设计商清单。而“经授权（authorized）的芯片设计商”，在2026年4月13日之前包括：（a）位于台湾或国家组A:1或A:5所列目的地，其总部或最终母公司总部均不在澳门或国家组D:5目的地，以及（b）其交易受EAR第743.9节中的报告要求约束的人员（《额外尽职调查措施》于EAR第743.9节规定，为经授权的芯片设计商制造芯片的前端制造商，需向BIS报告与经授权的芯片设计商的交易情况等信息）。商务部认为，上述目的地在打击先进节点芯片的转移方面存在共识，因此风险较低。该授权于2026年4月13日之后，满足前述条件的芯片设计商还需再提交申请、经批准后可重新成为经授权的芯片设计商。

(2) 所封装的先进计算芯片 (final packaged IC) 的“晶体管总数近似值”低于一定数值。如果芯片由“前端制造商”在澳门或国家组D:5目的地以外的地点进行封装, 或者芯片由“经批准 (approved) 的OSAT公司”封装, 则根据最终封装的先进计算芯片是否包含高带宽存储器以及不同时限, 前端制造商或OSAT公司需证明最终封装的“晶体管总数近似值”低于不同的数额标准, 才能成功推翻上述推定。具体而言, OSAT公司或前端制造商需要证明:

(a) 最终封装芯片的“聚合近似晶体管数量”低于300亿个晶体管; 或者 (b) 最终封装芯片不包含高带宽存储器, 并且最终封装芯片的“聚合近似晶体管数量”低于以下任一标准: (i) 2027年或之前完成的任何出口、再出口或 (国内) 转移不超过350亿个晶体管; 或者 (ii) 2029年或之后完成的任何出口、再出口或 (国内) 转移不超过400亿个晶体管。《额外尽职调查措施》在EAR第740部分新增7号补编对应“经批准的OSAT公司”, 这一清单目前包括英特尔、台积电、IBM等。

### 三、经验证的最终用户授权

“经验证的最终用户授权 (the Validated End-Use, VEU)”旨在方便将某些受管制物项出口、再出口和 (国内) 转移给经过BIS预先批准的、受信任的最终用户。在2024年10月BIS对EAR的修订中, BIS扩大了VEU项目的范围, 新增了一项“经验证的最终用户数据中心授权” (Data Center VEU)。Data Center VEU授权允许出口和再出口某些受管制物项给经验证的最终用户, 并在特定数据中心使用该物项。“数据中心”是指容纳多机架联网计算机系统的设施, 其中包括服务器、存储设备和网络设备。1月13日《临时最终规则》将Data Center VEU进一步分为“通用VEU” (Universal VEU) 和“国家VEU” (National VEU), 并进一步规定了VEU所需要适用的若干安全标准合规要求。

#### (1) 通用VEU

通用VEU允许总部或其最终母公司总部位于美国白名单国家的实体, 获得在澳门和D:5国家组以外的任何地点建设数据中心的授权, 而无需申请额外许可。但是通用VEU面临如下限制, 通用VEU不允许将其超过25%的AI总计算能力 (包括所有子公司和母公司拥有的计算能力) 转移或安装到白名单国家以外的地点, 且不允许转移或安装超过7%的AI总计算能力到任何单一国家。此外, 总部位于美国的UVEU不能将其超过50%的AI计算能力转移或安装到美国以外的地方。

#### (2) 国家VEU

国家VEU允许总部或最终母公司总部位于A、B或D:1-D:4国家组所列目的地的实体 (澳门和D:5国家组除外), 获得澳门和D:5国家组以外的任何地点建设数据中心的授权, 而无需申请额外许可。国家VEU面临如下限制, 每个公司、每个国家获取ECCN 3A090.a、4A090.a或相应.z 段落物项的TPP总和不能超过一定限额。

### 四、许可证例外AIA

1月13日《临时最终规则》规定, 对于位于美国白名单国家的用户, 且该用户的总部或最终母公司的总部也位于美国白名单国家, 出口、再出口或 (国内) 转移EAR§720.27(a)(1)规定的先进芯片物项, 可适用许可证例外AIA。

1月15日《额外尽职调查措施》对许可证例外AIA范围内的有关物项进一步提出了额外的尽职调查要求, 以匹配对于ECCN 3A090.a物项的“不利推定”。ECCN 3A090.a; ECCNs 5A002.z.1.a, z.2.a, z.3.a, z.4.a, z.5.a; 以及ECCN 5A992.z.1的物项的出口、再出口和或 (国内) 转移, 只有在由上述经授权或批准的芯片设计商设计的情况下才有资格适用许可证例外AIA。对于向总部或最终母公司的总部位于美国白名单国家的用户出口、再出口或 (国内) 转移ECCN 4E091的AI模型, 也可以适用许可证例外AIA, 但需要遵守更多限制, 包括该用户不能位于澳门和国家组D:5的目的地。

### 五、新增红旗行为

《临时最终规则》在EAR第732部分的3号补编“了解你的客户”（Know Your Customer）指南和警示信号中新增了一项警示信号28。警示信号28指出，在为总部或其最终母公司总部位于美国白名单国家以外的任何目的地的实体，提供基础设施即服务（IaaS）产品或服务或其他计算产品或服务，用于协助训练参数符合ECCN 4E091的AI模型时，将可能产生合规风险。因为此类AI模型可能会未经必要授权被违规出口至相关实体。在此情况下，IaaS提供商将可能面临协助和帮助违反EAR的不利后果。