汉坤法律评述
2025 年 7 月 9 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

Reverse CFIUS 制度对套壳 AI 产品的适用性分析

作者：解石坡 | 任正奇[1]

2025 年 1 月 2 日，美国财政部制定的《关于美国在特定国家的某些国家安全技术和产品领域投资的规则》（Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern，**“Reverse CFIUS 规定”**）正式生效。（如需详细分析，请联系我们索取）

美国财政部 Reverse CFIUS 规定旨在限制中国半导体和微电子、量子信息科技和人工智能领域公司获得融资的能力。随着近年来中国人工智能领域不断发展，较多人工智能模型和产品公司以及投资人均高度关注公司是否受 Reverse CFIUS 规定限制。例如，近期即有媒体报道称某 AI 公司在接受美元基金投资时可能被美国财政部就是否可能违反 Reverse CFIUS 规定开展调查。

其中，一个市场较为关注的问题是，调用第三方 AI 大模型或基于第三方 AI 大模型开发产品（以下统称“**套壳 AI 产品**”）是否同样受制于 Reverse CFIUS 规定限制。

一、Reverse CFIUS 规定对“开发人工智能系统”的限制

根据美国财政部 Reverse CFIUS 规定第 850.217 条，开发特定人工智能系统（AI System）构成受限活动。其中，根据 Reverse CFIUS 规定第 850.202 条，“人工智能系统”是指：

(a) 以机器为基础的系统，能够针对人类确定的特定目标，对真实或虚拟环境作出预测、建议或决定—即该系统能够：

(1) 使用数据输入感知真实和虚拟环境；

(2) 通过自动或算法统计分析，将这些感知提取为模型；以及

(3) 利用模型推理进行分类、预测、推荐或决策。

[1] 实习生蔡经纬对本文的写作亦有贡献。

(b) 全部或部分使用(a)段所述系统运行的任何数据系统、软件、硬件、应用程序、工具或实用程序[2]。

根据该定义，套壳 AI 产品很可能落入(b)项范围，也属于 Reverse CFIUS 项下的 AI 系统。

根据美国财政部对 Reverse CFIUS 规定的解释说明[3]，Reverse CFIUS 规定征求意见时曾有意见提出应删除 AI 系统(b)段定义，即不将套壳 AI 产品纳入规制范围。但是，美国财政部未采纳该意见，并明确说明其有意将套壳 AI 产品也纳入 Reverse CFIUS 的规制范围。但是，美国财政部进一步说明，对于套壳 AI 产品，仅当相关主体的行为构成 Reverse CFIUS 规定第 850.211 条列举的“开发”活动时，才受到管辖。

二、套壳 AI 产品的“开发”

根据 Reverse CFIUS 规定第 850.211 条，“开发”是指参与批量生产前的任何阶段，如设计或实质性修改、设计研究、设计分析、设计概念、原型组装和测试、试生产方案、设计数据、将设计数据转化为产品的过程、配置设计、集成设计和布局[4]。

并且，Reverse CFIUS 规定第 850.217 条注释 2 对于套壳 AI 产品的“开发”提供了进一步说明 — 对于 850.202(b)条项下的套壳 AI 产品，“开发”是指对其使用的第三方 AI 模型或以机器为基础的系统进行了 850.211 条列举的活动，例如设计或实质性修改[5]。

此外，根据美国财政部在发布 Reverse CFIUS 规定时的说明，最终规则对“开发”（Develop）定义中的“修改”（Modification）加上了“实质性”（Substantive）的限制，即对于某一项 AI 技术或产品的实质性修改构成对其开发活动，而非实质性修改不构成开发活动。例如，美国财政部倾向认为，对于第三方产品的日常运维不构成实质性修改，相反，对于第三方技术或产品的性能、功能或能力提升或重新定位（Repurpose），或改变其安全功能（例如移除第三方 AI 模型的安全措施或者保护机制），则构成“实质性修改”，从而构成对其的开发活动[6]。

此外，根据公开消息，一位财政部高级官员称仅使用商业现成（Commercial off-the Shelf）的 AI 模型不

---

[2] The term AI system means:
(a) A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments—i.e., a system that: (1) Uses data inputs to perceive real and virtual environments; (2) Abstracts such perceptions into models through automated or algorithmic statistical analysis; and (3) Uses model inference to make a classification, prediction, recommendation, or decision.
(b) Any data system, software, hardware, application, tool, or utility that operates in whole or in part using a system described in paragraph (a) of this section.
31 CFR 850.202

[3] https://www.federalregister.gov/documents/2024/11/15/2024-25422/provisions-pertaining-to-us-investments-in-certain-national-security-technologies-and-products-in#page-90462。

[4] Except as used in § 850.210(a)(4), the term develop means to engage in any stages prior to serial production, such as design or substantive modification, design research, design analyses, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. 31 CFR 850.211。

[5] “[T]o develop an AI system defined at § 850.202(b) in a manner subject to these notification requirements, the relevant covered foreign person or joint venture must engage in the activities enumerated in § 850.211, such as design or substantive modification, with respect to the third-party AI model or machine-based system that is being used by a data system, software, hardware, application, tool, or utility to operate in whole or in part.” Note 2 to 31 CFR 850.217。

[6] “For example, the Treasury Department considers routine maintenance or repair of a third-party product to constitute a non-substantive modification. In contrast, the Treasury Department considers modification to advance or repurpose the performance, function, or capability of a third-party technology or product, or impact its security features (e.g., by removing security measures or safeguards from a third-party AI model), to be a substantive modification.” https://www.federalregister.gov/d/2024-25422/p-223。

会构成“开发”AI 系统，但是对其进行定制（Customization）、配置（Configuration）或精调（Fine Tuning）构成“开发”AI 系统。

但是，上述规定或表述中，提升、重新定位（Repurpose）、定制（Customization）、配置（Configuration）或精调（Fine Tuning）均没有明确的定义和进一步的解释，因此其认定存在较大的不确定性。

进一步的，对于构成“开发”活动的套壳 AI 应用而言，判断其训练所需的计算能力是否达到 Reverse CFIUS 规定项下受限活动的相关标准，也存在较大的不确定性。根据美国财政部在发布 Reverse CFIUS 规定时的说明，训练 AI 系统的计算能力是指加总或合并的计算能力；例如，在多个小规模预训练的 AI 模型基础上训练时，所有 AI 模型的训练计算能力（即包括该等小规模 AI 模型）均需被合并计算；又如，在通过另一个模型生成的知识训练 AI 模型的情况下，二者训练计算能力也需合并计算[7]。但是，该说明也未明确解释如何认定套壳 AI 产品训练计算能力（特别是是否和在何种情况下需将底层 AI 模型的训练计算能力合并计入）。此外，Reverse CFIUS 规定征求意见时曾有意见提出希望明确在通过其他模型生成输入为模型提供信息（Generate Inputs to Inform）的情况下应当如何确定训练计算能力，但美国财政部在上述说明中也没有直接回答这一问题。

三、结语

目前，使用第三方 AI 模型或基于其实现的套壳 AI 产品存在多种形态，既包括仅接入第三方模型 API 提供类似的对话服务的产品，也包括基于第三方模型调整开发的垂类应用，还包括基于 AI 模型开发的 AI 智能体产品等。不同产品类型涉及的具体技术操作不同，是否构成 Reverse CFIUS 规定下的“开发”人工智能系统不可一概而论，需要进行个案分析，且目前缺乏明确的法律依据或案例。

随着 Reverse CFIUS 规定的正式生效以及调查案例的出现，套壳 AI 产品是否受到 Reverse CFIUS 规定的限制，成为 AI 创业公司和投资人需要重点关注的问题。根据目前的信息，无法简单排除 Reverse CFIUS 规定对套壳 AI 产品的适用，需要结合具体产品和场景进行分析，以避免合规风险。

[7] The Treasury Department notes that the computing power thresholds refer to the aggregate or combined computing power required to train a given AI system. For example, the computing power required to train an AI system that is a combination of smaller, pre-trained AI models would be the summation of computing power required to train and combine each component model of the AI system. Similarly, developing an AI model based on the transfer of knowledge from one model to another would include the computing power required to train both models. https://www.federalregister.gov/d/2024-25422/p-79。

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：

解石坡

电话： +86 10 8524 5866
Email： angus.xie@hankunlaw.com