美國商務部就人工智慧模型與運算叢集開發之報告要求提出規則草案

文逢遠 編譯

摘要

今（2024）年 9 月 11 日，美國商務部工業與安全局就人工智慧模型與運算叢集開發、訓練與測試活動之報告要求新訂規則草案。此次修訂係源自拜登政府於去（2023）年 10 月發布之行政命令，旨在確保人工智慧之發展與使用安全。根據此次修訂，若位於美國之企業或自然人從事滿足特定標準之人工智慧模型或運算叢集的開發活動，將被要求定期向商務部提交報告。規則草案也列出適用報告要求之活動與其問題回覆內容及相關繳交期限，企業不合規時則有可能面臨相關罰則。此次修訂將有助於政府識別適合用於國防工業的人工智慧模型，同時掌握該些模型可能帶來之國家安全風險。

（取材資料：Adam S. Hickey et al., *US Department of Commerce Issues Proposal to Require Reporting Development of Advanced AI Models and Computer Clusters*, MAYER BROWN (Sept. 17, 2024), https://www.mayerbrown.com/en/insights/publications/2024/09/us-department-of-commerce-issues-proposal-to-require-reporting-development-of-advanced-ai-models-and-computer-clusters; Weslan Hansen, *Commerce to Seek Input on Dual-Use AI Reporting Requirements*, MERITALK (Sept. 10, 2024), https://meritalk.com/articles/commerce-to-seek-input-on-dual-use-ai-reporting-requirements/.）

美國商務部工業暨安全局（Bureau of Industry and Security, BIS）於今（2024）年 9 月 11 日提出一項規則草案（以下簡稱草案），強制要求特定人工智慧開發商與運算服務提供商提交報告，其內容包含人工智慧模型之開發、訓練與測試[1]。

以下先簡介草案背景，並就草案規範適用之活動範圍、問題回覆內容與相關繳交期限進行介紹，接著說明草案欲達成之國防安全目的與未來進展，最後以相

[1] Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters, 89 Fed. Reg. 73612 (Sept. 11, 2024) (to be codified at 15 C.F.R. pt. 702) [hereinafter Proposed Rule].

關評析作結。

壹、草案背景

去（2023）年 10 月，美國總統拜登發布第 14110 號行政命令，旨在確保人工智慧（Artificial Intelligence, AI）之安全發展與使用[2]。該命令第 4.2(a)條指示美國商務部根據「國防生產法（Defense Production Act, DPA）」授予總統之職權，向意圖開發軍民兩用基礎模型（Dual-Use Foundation Model，以下簡稱兩用模型）[3]，或意圖獲取或開發大規模運算叢集（Large-Scale Computing Cluster）之企業蒐集特定資訊[4]。根據 DPA 規定，美國總統有權採取相關措施，確保本國工業做足妥善準備，以提供國防所需之產品與服務[5]。

為履行該行政命令，BIS 行使 DPA 授予美國總統之權力，對特定美國企業進行資訊蒐集。該些企業包含正在開發、計畫開發兩用模型，或持有開發兩用模型所需之電腦硬體[6]。美國時任總統歐巴馬曾於 2012 年發布第 13603 號行政命令，將此項權力授予商務部，隨後並複授權所屬 BIS 執行[7]。

貳、草案之主要內容

該草案主要分為三個部分，首先是報告要求之適用活動與其繳交期限，接著是報告提交之形式與內容，最後則是相關名詞定義，惟該些定義與上述第 14110 號行政命令相同，故後續不再另行說明。本文另針對違反草案規定時可能面臨之罰則進行介紹，以下將分別闡述。

一、適用報告要求之活動

---

[2] Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 88 Fed. Reg. 75191 (Oct. 30, 2023) [hereinafter Executive Order 14110].

[3] 軍民兩用基礎模型係指透過廣泛的資料進行訓練，通常採用自監督（self-supervision）且包含至少數百億個參數，同時適用於廣泛情境且在安全、國家經濟安全、國家公共衛生或國家公共安全等構成嚴重風險之議題中具有（或透過輕易修改而具有）高性能之 AI 模型。*Id*. at 75194. AI 領域中，自監督學習（self-supervised learning）主要透過自監督任務（Pretext）由大量未經人工標記資料中自我建構監督資訊，並透過該些資訊進行預訓練（Pretrain），使得預訓練模型能承載具有價值的語義表徵或結構意義等，且能夠有益於下游任務（Downstream task），請參：楊偉楨，階層式預訓練：以自監督學習改良自監督學習，資策會數位轉型研究院，2021 年 9 月 17 日，https://www.find.org.tw/index/wind/browse/30ec5ccc59a28ef3132de5cb01a9e577/。

[4] 運算叢集為一系列電腦或伺服器的集合，該些元件透過相互連接與配置以提供一整體系統之運作，形成運算叢集，其主要特色係能夠輕鬆處理大量資料與複雜的計算問題，故適合作為不同領域資料處理之工具。*What is a Computing Cluster?*, SUPER MICRO, https://www.supermicro.com/zh_tw/glossary/computing-cluster (last visited Nov. 11, 2024); Executive Order 14110, *supra* note 2, at 75197.

[5] Proposed Rule, *supra* note 1, at 73613; 50 U.S.C. § 4533 (1950).

[6] *Id*. at 73613.

[7] *Id*.; National Defense Resources Preparedness, 77 Fed. Reg. 16651 (Mar. 16, 2012).

根據草案，適用活動共包含兩項，一是與 AI 模型有關，即使用大於 10 的 26 次方之整數或浮點數運算執行對 AI 模型的訓練；二是取得、開發或持有一運算叢集，該叢集用於 AI 模型的訓練並具備一組與資料中心網路相互連接之機器，在不考慮稀疏性（Sparsity）之情況下，其傳輸速率超過 300 Gbit/s，且理論運算能力大於每秒 10 的 20 次方之整數或浮點數運算[8]。

二、報告要求之繳交期限

根據草案，若任何位於美國之自然人或法人在未來 6 個月內從事或計畫從事適用活動，將被要求向 BIS 提交季度報告[9]。BIS 在收到適用活動通知後，將向從事適用活動者提出問題。從事者必須在收到請求後 30 日內提交所有問題之答覆[10]。該草案亦就答覆內容之修正設置 14 日的繳交期限。若 BIS 就答覆內容提出額外問題，則從事者必須於 7 日內完成答覆並繳交，惟其可向 BIS 要求延長繳交期限[11]。

三、問題答覆要求之內容

BIS 提出之問題包括但不限於[12]：1. 任何與訓練、開發或生產兩用模型有關之正在進行或計畫中的活動，包含實體與網路安全保護措施；2. 任何兩用模型中模型權重（Model Weights）之所有權與佔有權的歸屬，以及保護模型權重所採取之實體與網路安全措施[13]；3. 任何已開發兩用模型在其 AI 紅隊演練（Red-Team Testing）中之表現結果[14]；以及 4. 與兩用模型之安全性及可靠性有關之其他資訊，或可能對美國國家安全產生疑慮之活動或風險等其他資訊。

四、違反規定所面臨之罰則

違反該草案者將面臨相關民事與刑事處罰，包含強制履行報告要求的義務，且可能被處以不超過 10,000 美元的罰金或不超過一年之監禁[15]。

---

[8] Proposed Rule, *supra* note 1, at 73616.
[9] *Id*.
[10] *Id*.
[11] *Id*.
[12] *Id*. at 73616, 73617.
[13] 模型權重是定義機器學習模型之內部結構與決策邏輯之參數，並使 AI 系統能夠根據資料學習運算模式後作出預測或決策。Alice Hubbard, *Weighing the Options: How Model Weights Can be Used to Fine-tune AI Models*, ALL. FOR TRUST IN AI, https://alliancefortrustinai.org/how-model-weights-can-be-used-to-fine-tune-ai-models/ (last visited Nov. 11, 2024).
[14] 紅隊演練係指模擬現實世界中的對手及其工具、策略與流程的實踐，以識別風險、揭露盲點、驗證假設，並改善系統的整體安全狀態。Ram Shankar, Siva Kumar, *Microsoft AI Red Team Building Future of Safer AI*, MICROSOFT (Aug. 7, 2023), https://www.microsoft.com/en-us/security/blog/2023/08/07/microsoft-ai-red-team-building-future-of-safer-ai/.
[15] 15 C.F.R. § 702.5 (2015).

參、草案之規範目的與進展

隨著技術進步，該草案將就兩用模型與訓練模型所使用之運算基礎設施進行持續的監管。該草案為美國 BIS 近年來對 AI 採取之系列措施之一，旨在對先進 AI 模型之訓練與開發至關重要之設備與技術實施出口管制[16]。

基於此背景，草案中的報告要求旨在確保 BIS 與其他政府單位進行協調，提高對於 AI 模型之開發中、訓練、測試與取得等活動之能見度並做出更佳洞察，該些活動也可能進一步保證 AI 模型發照許可之實施[17]。

BIS 指出，必須對兩用模型進行持續評估，以確認是否能作為國防工業使用的基礎[18]，同時掌握該其安全性以及可能帶來的國家安全風險，故該作法對政府而言是必要的[19]。

因此，儘管草案僅規範報告義務，該些報告將為此領域之未來監管與政策發展的多個面向提供資訊。為此，BIS 在草案中提及其可能採取措施以確保國防工業基礎能夠生產全球最安全、最可靠的產品與服務，同時美國企業生產的兩用模型足以供應國防工業基礎需求[20]。

肆、相關評析及結語

BIS 次長 Alan Estevez 指出草案中的報告要求將幫助政府掌握最先進 AI 系統之能力與安全性。它將基於 BIS 長期以來進行的國防工業基礎調查，為美國政府提供有關美國重要產業中新興風險的資訊[21]。

商務部長 Gina Raimondo 亦提到 AI 的迅速發展帶來可觀前景之餘，亦伴隨著風險。此草案將幫助我們即時關注 AI 技術的最新發展，進而增強國防能力並保障國家安全[22]。

商務部出口管制助理次長 Thea D. Rozman Kendler 則提及該草案表明美國政府對先進 AI 技術中之兩用模型採取積極思考。BIS 正透過報告要求的設置，發

---

[16] Commerce Control List Additions and Revisions; Implementation of Controls on Advanced Technologies Consistent with Controls Implemented by International Partners, 89 Fed. Reg. 72926 (Sept. 6, 2024) (to be codified at 15 C.F.R. pt. 736, 738, 740, 742, 743, 772, 774).
[17] Proposed Rule, *supra* note 1, at 73616.
[18] *Id*. at 73614.
[19] *Id*.
[20] *Id*. at 73613.
[21] *Commerce Proposes Reporting Requirements for Frontier AI Developers and Compute Providers*, U.S. BUREAU OF INDUSTRY AND SECURITY (Sept. 9, 2024), https://www.bis.gov/press-release/commerce-proposes-reporting-requirements-frontier-ai-developers-and-compute-providers.
[22] *Id*.

展用以識別 AI 先進研究中新興風險之能力的系統[23]。

綜觀此次修訂，美國政府已充分展現其對兩用模型與運算叢集之先進技術進行管制的決心。為了確保國防安全並滿足國防工業需求，美國政府正透過要求特定企業或個人提供先進技術之相關資訊予以監督。數名商務部官員也提到，這項要求將幫助政府掌握先進技術的發展，進而識別該些發展可能伴隨之新興風險，俟相關資訊蒐集完備，將可進一步對該技術採取更為細緻之監管措施。

[23] *Id.*