僅供委員問政所需參考
不代表本院意見或立場

編號：3218

議題研析

一、題目：美國人工智慧監管之法制發展及借鏡

二、議題所涉法規

人工智慧基本法

三、背景說明（緣起）

隨著人工智慧(AI)技術快速發展，其可能衍生之國家安全、網路安全、消費者權益及能源等風險日益受到關注。美國國會近期已有兩黨議員陸續提出相關法案，包括針對先進 AI 模型建立風險評估及監管機制、要求 AI 模型具備終止機制，以及由美國國家標準與技術研究院(NIST)制定相關安全指引等，顯示美國 AI 治理已逐漸由原則性討論轉向具體立法[1]。

四、問題爭點

美國近期已有不同黨派議員提出 AI 相關法案，內容聚焦於先進 AI 系統之風險評估、透明度及安全監督等議題。相關制度仍處於立法研議及調整階段，值得持續觀察其後續發展，並作為我國研議 AI 風險治理、監管機制及跨部門協調制度之參考。

五、探討研析

（一）FRONTIER Act

FRONTIER Act 全稱為《前沿風險監督、國家透明度、獨立評估與報告法案》(Frontier Risk Oversight, National Transparency,

[1] Nathan Worcester，監管 AI 美議員紛紛推法案，大紀元時報，2026 年 9 月 22 日，第 A4 版。

Independent Evaluation, and Reporting Act，亦即 H.R.9925)於 2026 年 7 月 23 日由美國眾議院提出，目前交由能源與商業委員會(House Energy and Commerce)及科學、太空與技術委員會(House Science, Space, and Technology)審議[2]。該法案旨在強化大型人工智慧開發商的透明度及問責，要求開發商提供模型卡(model cards)、風險管理框架、第三方獨立審計、重大安全事件及時通報機制，以及持續性評估等措施[3]。

該法案採取分級監管模式[4]，依開發商之規模及 AI 開發投入程度，區分為三個層級：第一層級，前沿開發商(frontier developers)[5]通常只需滿足基本的透明度和事件報告要求；第二層級，大型前沿開發商(large frontier developers)[6]需接受輕量級的合規性審計；第三層級，只有規模非常大的超大型前沿開發商(very large frontier developers)[7]須接受密集獨立驗證機構(IVO)較為密集的評估，以確定其風險控管措施是否充分有效[8]。

此外，該法案並授權商務部（Department of Commerce）部長於發生即時災難性風險時，發布緊急命令，暫停或限制前沿模型

[2] CONGRESS.GOV，H.R.9925 - FRONTIER Act，網址：https://www.congress.gov/bill/119th-congress/house-bill/9925，最後瀏覽日期：2026 年 10 月 8 日。

[3] Congressman Jay Obernolte (CA-23)，Obernolte, Trahan Introduce Bipartisan FRONTIER Act to Strengthen Oversight of Advanced AI，2026 年 7 月 23 日，網址：https://obernolte.house.gov/media/press-releases/obernolte-trahan-introduce-bipartisan-frontier-act-strengthen-oversight，最後瀏覽日期：2026 年 10 月 8 日。

[4] Congressman Scott Franklin (FL-18)，Franklin Celebrates Introduction Of Frontier Act To Advance American AI Leadership，2026 年 7 月 23 日，網址：https://franklin.house.gov/news/documentsingle.aspx?DocumentID=1922，最後瀏覽日期：2026 年 10 月 8 日。

[5] 前沿開發商(frontier developers) 指在州際或國際貿易中運作的實體，該實體已經使用符合可接受的災難性風險緩解水準的技術規範的計算能力對前沿模型進行了訓練或啟動了訓練。H.R.9925 SEC.2.(11)參照。全文詳見 CONGRESS.GOV，H.R.9925 - FRONTIER Act，網址：https://www.congress.gov/bill/119th-congress/house-bill/9925/text，最後瀏覽日期：2026 年 10 月 8 日。

[6] 大型前沿開發商(large frontier developers) 是指前沿開發商及其關聯公司在前 36 個月期間（以每個日曆月的第一天為準）同時符合下列二條件：（1）總收入超過 5000 萬美元；（2）在人工智慧相關開發支出方面不少於 10 億美元。H.R.9925 SEC.2.(15)參照。

[7] 超大型前沿開發商(very large frontier developers) 是指前沿開發商及其關聯公司在前 36 個月期間（以每個日曆月的第一天為準）同時符合下列二條件：（1）總收入超過 50 億美元；（2）在人工智慧相關開發支出方面不少於 100 億美元。H.R.9925 SEC.2.(22)參照。

[8] Daniel King，The FRONTIER Act Is Congress’s Best AI Bill Yet，FAI，2026 年 9 月 1 日，網址：https://www.thefai.org/posts/the-frontier-act-is-congress-s-best-ai-bill-yet，最後瀏覽日期：2026 年 10 月 8 日。

(frontier model)[9]之開發、運用或內部使用[10]，並對違反命令者設有民事罰款及刑事責任[11]。

（二）AI Risk Evaluation Act

美國《人工智慧風險評估法案》(Artificial Intelligence Risk Evaluation Act，亦即 S.2938)於 2025 年 9 月 29 日提出，目前已於參議院國土安全與政府事務委員會(Homeland Security and Governmental Affair)舉行聽證會[12]。該法案旨在建立先進人工智慧之測試與評估機制，提供國會經驗數據及風險資訊，作為聯邦政府制定 AI 監管政策之依據[13]。

該法案要求能源部(Department of Energy)部長於法案通過後 90 天內，建立「先進人工智慧評估計畫」(Advanced Artificial Intelligence Evaluation Program)[14] ，針對訓練時使用超過 10^{26} 次整數或浮點運算(integer or floating-point operations)之先進人工智慧系統(advanced artificial intelligence system)進行標準化測試及評估[15]。受規範之先進人工智慧系統開發商(advanced artificial intelligence system developer)[16]須參與評估計畫，並依要求提供程式碼、訓練資料、模型權重及其他相關資訊；未符合規定者，不得將該系統部署於州際或國際商業活動，並處每日至少 100 萬美元之罰款[17]。

---

[9] frontier model 是指使用超過 10^{26} 次整數或浮點運算的運算能力進行訓練的基礎模型。運算能力包括原始訓練運作所需的運算能力，以及開發者對先前基礎模型進行的任何後續微調、強化學習或其他實質修改所需的運算能力。H.R.9925 SEC.2.(12)參照。

[10] H.R.9925 SEC.8.(a)(1)參照。

[11] H.R.9925 SEC.8.(m)參照。

[12] CONGRESS.GOV，S.2938 - Artificial Intelligence Risk Evaluation Act of 2025，網址：https://www.congress.gov/bill/119th-congress/senate-bill/2938，最後瀏覽日期：2026 年 10 月 8 日。

[13] S.2938 SEC.2.(b)參照。全文詳見 CONGRESS.GOV，S.2938 - Artificial Intelligence Risk Evaluation Act of 2025，網址：https://www.congress.gov/bill/119th-congress/senate-bill/2938/text，最後瀏覽日期：2026 年 10 月 8 日。

[14] S.2938 SEC.5.(a)參照。

[15] S.2938 SEC.3.(1)(A)參照。

[16] 「受監管的高級人工智慧系統開發商」是指設計、編寫程式碼、生產、擁有或實質修改用於州際或國際貿易的高級人工智慧系統的人，包括採取措施啟動高級人工智慧系統的訓練運作。S.2938 SEC.3.(7)參照。

[17] S.2938 SEC.4.(a)、(b)參照。

此外，該計畫並要求能源部依評估結果提出風險預防、緩解策略及聯邦監管建議，並於法案公布之日起7年後終止，除非經國會延長[18]。

（三）結語

美國近期提出之FRONTIER Act及AI Risk Evaluation Act，分別從分級監管及事前評估機制著手，強化對先進AI系統之監督。前者依開發商規模及相關條件，課予不同程度之資訊揭露、審計及獨立評估義務；後者則透過政府建立評估計畫，蒐集AI系統之實證資料，作為後續監管政策之參考。上述法案反映美國對AI風險治理之政策關注，並顯現相關立法由原則性討論逐步朝向具體監管機制發展之趨勢。

惟上述法案目前仍處於立法研議階段，其最終內容及後續推動情形尚待觀察。未來美國如何在AI技術快速發展下，兼顧產業創新、國家安全及公共利益，以及分級監管、事前評估等機制之實際運作成效，均值得持續關注，並作為我國AI監管法制發展之參考。

撰稿人：林鈺琪

[18] S.2938 SEC.5.(d)參照。