僅供委員問政所需參考
不代表本院意見或立場

編號：3246

議題研析

一、 題目：美國「促進先進人工智慧創新與安全」規範簡介

二、 議題所涉法規

人工智慧基本法、刑法、資通安全管理法

三、 背景說明（緣起）

隨著人工智慧（Artificial Intelligence，下稱AI）技術快速發展，安全與監管問題日益受到關注。微軟總裁Brad Smith呼籲各國應儘速建立全球性安全規範，要求企業設置緊急停機機制、通報事故，並在必要時接受獨立機構審查，以防AI失控危及人類安全，尤其部分AI代理（AI Agent）可能脫離人類控制，功能強大的模型也可能對全球網路安全構成威脅，因此各國應開始合作制定共同標準，而不是等到重大事故發生後才採取補救措施[1]。

四、 問題爭點

AI加速導入企業營運，除了提升工作效率，如何有效管理AI帶來的潛在風險，也成為企業面臨的重要課題[2]。我國是全世界半導體及AI基礎建設生產的主要來源地，跟世界AI相關產業都有一定程度的關係。但輝達公布「Open Agent安全平台」，全球有100多家企業參與，卻未見台灣企業[3]，作為AI產業的重要參與者，我國對於AI安全監管相關議題更應重視。爰簡介美國「促進先進人工智慧創新與安全

[1] 林聰毅，牛奶都有人驗、AI 卻沒人管！微軟總裁籲全球速訂安全規範，經濟日報，115年10月12日，網址：https://money.udn.com/money/story/5599/9810242，最後瀏覽日期：115年11月11日。
[2] 邱巧貞，台灣企業AI應用加速、風險管理卻亮警訊 2大指標跌入收縮區，自由時報，115年11月4日，網址：https://ec.ltn.com.tw/article/breakingnews/5629707，最後瀏覽日期：115年11月11日。
[3] 黃齊元，AI失控風險升高！台灣不能只顧著賺半導體財，遠見雜誌，115年10月13日，網址：https://www.gvm.com.tw/article/133701，最後瀏覽日期：115年11月11日。

」規範，以供委員問政參考。

五、探討研析

（一）美國發布「促進先進人工智慧創新與安全」行政命令背景

川普政府上任後，美國 AI 政策整體基調偏向「創新優先」，避免過度監管影響產業發展，以維持 AI 產業競爭優勢為目標。然而，隨著尖端 AI 模型逐漸具備更先進之網路攻防及自動化代理能力，政策關注範圍亦由產業發展與技術競爭，進一步延伸至國家安全、政府資訊系統防護及關鍵基礎設施韌性。白宮指出，先進 AI 能力雖可強化國家實力，亦帶來新的國家安全考量，須由行政部門各機關及其所屬單位協調因應[4]。

因應新一代 AI 模型能力快速提升所引發之國家安全與資安議題，白宮於 2026[5]年 6 月 2 日發布第 14409 號總統行政命令「促進先進人工智慧創新與安全」（Promoting Advanced Artificial Intelligence Innovation and Security）（下稱行政命令），宣示聯邦政府將透過與私部門合作，促進 AI 創新與安全，藉由現代化政府及私部門資訊系統、防禦外部網路威脅、保護美國創新成果與智慧財產，以及培養先進 AI 賦能能力，維持美國在 AI 創新領域之領先地位[6]。行政命令的核心並非建立全面 AI 監管制度，而是要政府與 AI 業者合作，把先進模型的網路安全能力用於防禦政府資訊系統與關鍵基礎設施，並保護美國技術與智慧財產[7]。

（二）重點概述

[4] 柯郁萱，美國發布先進 AI 創新與安全總統行政命令，強化 AI 資安防禦並建立尖端模型自願性架構，資訊工業策進會科技法律研究所，115 年 8 月 10 日，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9548#_ftn1，最後瀏覽日期：115 年 11 月 11 日。

[5] 本文有關年分之使用，原則以民國紀年表述，惟涉及外國法制或立法例部分，改採西元紀年表述。

[6] The White House, Promoting Advanced Artificial Intelligence Innovation And Security-Executive Order 14409, June 2, 2026, available at：https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/, last visited on Nov. 11, 2026.

[7] The White House, Fact Sheet: President Donald J. Trump Promotes Advanced Artificial Intelligence Innovation and Security, June 2, 2026, available at：https://www.whitehouse.gov/fact-sheets/2026/06/fact-sheet-president-donald-j-trump-promotes-advanced-artificial-intelligence-innovation-and-security/, last visited on Nov. 11, 2026.

「促進先進人工智慧創新與安全」行政命令聚焦三項重點：

1、強化政府與民間關鍵基礎設施資訊系統網路防禦能力：

著重在先進 AI 能力強化美國資訊系統之網路防禦，包括優先強化政府相關資訊系統之防禦，並透過導入 AI 賦能防禦工具、完善弱點管理與修補協調等措施及資源分配，提升整體資安防護能力。具體措施包含（1）優先強化政府資訊系統防禦，並擴大 AI 資安資源之取得；（2）成立 AI 網路安全資訊交換中心（AI cybersecurity clearinghouse），並啟動「金鷹計畫」（Gold Eagle），由相關聯邦機關與 AI 產業合作，依其重要性排定優先處理順序，並協調軟體弱點掃描與後續驗證作業，以確保美國軟體與網路之安全[8]。另外，行政命令也要求行政管理預算局（Office of Management and Budget, OMB）和網路安全與基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）協調，盤點可用資金，以資助、擴大資安人才任用。

2、建立「受規範的尖端 AI 模型」（covered frontier models）自願性安全部署架構：

對於符合標準之模型，透過自願性架構，開發者得於向其他可信任夥伴發布模型前，提供聯邦政府最長 30 日之模型近用權限。此類近用須受適當保密、資安、內部人員風險、智慧財產權保護、使用及不揭露要求之拘束。行政命令並進一步規劃，AI 開發者得與聯邦政府合作選定可信任夥伴，使該等合作夥伴取得尖端模型提前近用權，以促進安全創新並強化關鍵基礎設施資安[9]。

3、加強防制 AI 相關資安犯罪：

從刑事執法面來因應 AI 的濫用風險。其要求司法部長應

[8] The White House, White House Launches Gold Eagle Initiative for Unprecedented Cybersecurity Vulnerability Coordination, July 14, 2026, available at：https://www.whitehouse.gov/releases/2026/07/white-house-launches-gold-eagle-initiative-for-unprecedented-cybersecurity-vulnerability-coordination, last visited on Nov. 11, 2026.

[9] The White House, 同註 7。

優先執行《美國法典》(United States Code)第 18 編第 1028 條、第 1030 條、第 1343 條及其他適用之聯邦刑事法律，嚴懲未經授權利用 AI 非法入侵或損害電腦系統之行為，或在進行前述非法入侵時利用 AI 進一步實施其他犯罪之行為。

（三）可供我國借鑑之處

《人工智慧基本法》第 4 條指出，政府推動 AI 之研發與應用的七大遵循原則，其中就包括「資安與安全」，AI 研發與應用過程，應建立資安防護措施，防範安全威脅及攻擊，確保其系統之穩健性與安全性。而數位發展部則於 115 年 9 月 4 日發布「政府因應先進 AI 資安風險政策」，成立「先進 AI 資安風險因應小組」，建立跨部會、公私協力的推動機制，同時訂定階段性戰略防護對策，包括短期策略：加速防禦，降低當前曝險；中期策略：提升資通訊產品與供應鏈安全；長期策略：深化國際合作，建立自主 AI 資安防禦能力。整體措施展現出更快的防禦、更強的韌性，提升面對先進 AI 時代的資安風險控管能力[10]，與時俱進的完整政策內容，值得嘉許。但隨著 AI 技術的不斷創新，政府及企業的安全責任也隨之提高，因此，建議主管機關可在《人工智慧基本法》已確立的基本架構下，參考前述美國的行政命令，借鏡其「創新與安全並重」的取向，滾動式檢討現行法令，研議制定相關 AI 安全規範，及進一步建立專門的安全評估機制，隨時因應 AI 發展所面臨的資安及安全問題，以利我國 AI 的整體發展。

撰稿人：黃嘉文

[10] 數位發展部資通安全署，因應先進 AI 資安新挑戰 資安署發布「政府因應先進 AI 資安風險政策」強化國家數位防護網，115 年 9 月 4 日，網址：https://moda.gov.tw/ACS/press/news/press/20572，最後瀏覽日期：115 年 11 月 11 日。