美國國土安全部發布「2024人工智慧路線圖」，確保AI安全開發與部署

美國國土安全部（Department of Homeland Security, DHS）於2024年3月17日發布「2024人工智慧路線圖」（2024 Artificial Intelligence Roadmap）（下稱AI路線圖），設立三大目標，將偕同旗下機關與產官學研各界合作，確保AI的安全開發與部署，保護國家關鍵基礎設施安全，以強化國家安全。

美國拜登總統於2023年10月30日簽署的第14110號總統行政命令《安全可靠且值得信賴的人工智慧開發暨使用》（Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence）（下稱AI總統行命令），要求DHS應管理使用於關鍵基礎設施與資通安全的AI、制定全球AI標準並推廣、降低利用AI造成具有大規模殺傷力武器攻擊之風險、保護AI智慧財產權、以及吸引AI領域人才，以促使、加強AI開發與部署等事項。為踐行上述事項，DHS制定AI路線圖，其三大目標如下：

（1） 負責任的使用AI以推進國安任務（Responsibly Leverage AI to Advance Homeland Security Mission）：透過建置AI基礎建設、建立AI系統測試與評估（Testing and Evaluation, T&E）、推動AI人才培育計畫等行動措施，帶領主管機關負責任的使用AI，以保護國家安全及避免AI對關鍵基礎設施的風險，確保AI於使用過程中係尊重個人隱私、保護公民權利與自由。

（2） 促進AI安全與資安（Promote Nationwide AI Safety and Security）：利用AI技術改善與預防關鍵基礎設施之安全與資安風險、制定關鍵基礎設施之AI使用指引、以及成立AI安全與資安委員會（AI Safety and Security Board, AISSB），彙集產官學研各界專家意見。

（3） 透過擴大AI國際合作來引領AI發展（Continue to Lead in AI Through Strong, Cohesive Partnerships）：將透過與產官學研各界合作，擴大AI的國際合作，並持續與公眾進行意見交流與分享，推廣AI政策或相關行動措施；DHS亦將持續與參眾議院及其他主管機關匯報AI相關之工作進度與未來規劃，以提升部門AI的透明度，並建立公眾對AI的信任。

本文為「經濟部產業技術司科技專案成果」

相關連結

U.S. Department of Homeland Security, 2024 Artificial Intelligence Roadmap, Mar. 17, 2024

→ 【高雄場】113年度新創採購-招標作業廠商說明會

劉心妍
副法律研究員 編譯整理

上稿時間：2024年06月

資料來源：
U.S. Department of Homeland Security, *2024 Artificial Intelligence Roadmap*, Mar. 17, 2024, https://www.dhs.gov/sites/default/files/2024-03/24_0315_ocio_roadmap_artificialintelligence-ciov3-signed-508.pdf (last visited May 7, 2024).

延伸閱讀：
陳政陽，〈日本公布設立AI安全研究所與著手訂定AI安全性評鑑標準〉，資訊工業策進會科技法律研究所，2024/4，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9157〈最後瀏覽日：2024/5/7〉。
周晨蕙，〈日本經產省和總務省共同發布AI業者指引草案，公開徵集意見〉，資訊工業策進會科技法律研究所，2024/4，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9146〈最後瀏覽日：2024/5/7〉。
吳彬詣，〈歐盟執委會發布人工智慧創新政策套案〉，資訊工業策進會科技法律研究所，2024/4，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9143〈最後瀏覽日：2024/5/7〉。

文章標籤

人工智慧 | 產學研合作 | 人工智慧監管 | 人工智慧風險管理

科法觀點
實現「負責任的AI」的關鍵在於強化數位資料歷程「證明」

推薦文章