僅供委員問政所需參考
不代表本院意見或立場

編號：2608

議題研析

一、題目：公部門引進 AI 相關法制問題研析

二、議題所涉法規

無

三、背景說明(緣起)

為促進政府服務 AI 化，數位發展部已著手規劃「政府 AI 發展戰略計畫」，預計 2026 年開始，5 年內斥資新臺幣 190 億元經費，推動發展智慧化為民服務、建構自動化行政服務、完備 AI 資料與模型、打造數位平權智慧服務、厚植 AI 應用基礎環境等五大目標[1]。藉由政府機關導入 AI，不僅能將重複且耗時之工作自動化，節省成本與時間，提升工作效率；透過精確之預測與感知，協助作為政策制定之依據；洞察與預測民眾需求，據以提供個人化服務、即時回應或預期性服務[2]，以迎合現代社會的多樣化需求。

四、問題爭點

政府除訂定公部門 AI 應用手冊、規劃 AI 風險分類框架，AI 育才策略外[3]，應著重關注資訊的安全和保護，建構雲端產品和服務的安全評估、授權和監控等標準化方法。外國制（訂）定雲端科技須遵循的安全與風險評估標準之相關法制規範，或可供借鏡參考。

五、探討研析

[1] 呂晏慈，數發部規劃戰略計畫，推動發展智慧化為民服務等五大目標 公部門導入 AI 5 年斥資 190 億，工商時報，2024 年 10 月 15 日，第 A4 版。
[2] 徐嘉臨，人工智慧如何增進公部門服務效能，考試院資訊處，2023 年 10 月 21 日，頁 6。
[3] 呂晏慈，同註 1。

（一）美國立法例

美國聯邦政府早在 2010 年即展開「聯邦政府風險與授權管理計畫」（Federal Risk and Authorization Management Program, FedRAMP），聯邦政府總務管理局（General Service Administration）於 2012 年 6 月 6 日宣布 FedRAMP 正式運作。該計畫是根據美國聯邦資訊安全管理法（Federal Information Security Management Act, FISMA），提供評估、監控和授權雲端運算產品和服務的標準化方法，以及加速聯邦機構採用安全雲端解決方案，其目的是建立一套全國政府機關可遵循的依據，提供標準化做法供相關人員對雲端產品和服務進行安全性評估、授權和持續監控。所有雲端產品與服務業者，都必須達到該計畫的標準規範，才能為美國政府機關提供雲端產品及服務。因此，所有聯邦機構的雲端部署作業和服務模型都必須符合相應風險影響等級（低等、中等或高等）的 FedRAMP 要求。雖然 FedRAMP 的目的是讓美國公部門受惠，但越來越多美國公家機關下的州立與地方組織也將 FedRAMP 架構應用於自身合約或評估機制，藉此實現標準化的安全性和法規遵循[4]。

此外，為回應拜登總統 2023 年 10 月 30 日關於安全、可靠和值得信賴地開發和使用人工智慧的第 14110 號行政命令[5]，FedRAMP 計劃建立一個框架，以優先考慮 FedRAMP 授權的新興科技（emerging technologies），因此，聯邦政府總務管理局於 2024 年 6 月 27 日發布新興科技優先審查框架（Emerging Technologies Prioritization Framework）[6]。雲端服務供應商（cloud service providers）若欲將其

[4] 郭俊仁，美國正式推行「聯邦政府風險與授權管理計畫」，stli 科技法律研究所，2012 年 7 月 31 日，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=5795，最後瀏覽日期：2024 年 10 月 28 日；Aruba Networks，什麼是 FedRAMP？網址：https://www.arubanetworks.com/zh-hant/faq/what-is-fedramp/，最後瀏覽日期：2024 年 10 月 30 日；Microsoft Learn，聯邦風險與授權管理計畫 (FedRAMP)，2024 年 1 月 12 日，網址：https://learn.microsoft.com/zh-tw/compliance/regulatory/offering-fedramp，最後瀏覽日期：2024 年 10 月 30 日。

[5] The White House，Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence，2023 年 10 月 30 日，網址：https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/，最後瀏覽日期：2024 年 11 月 1 日。

[6] FedRAMP，Emerging Technology Prioritization Framework，網址：https://www.fedramp.gov/et-framework/，最後瀏覽日期：2024 年 10 月 28 日。

產品提供予政府單位使用，需依 FedRAMP 相關規範等候審查，然而，新興科技優先審查框架則例外開放，使提供「新興科技」產品之雲端服務供應商得視情況優先審查[7]。該框架最初將應用於 AI，特別是第 14110 號行政命令中討論的四種生成式 AI 功能：聊天介面（chat interface）、程式碼生成器和除錯工具（code generation and debugging tools）、圖像生成器（prompt-based image generators）以及通用應用程式介面（general purpose API），並根據需要更新優先新興科技列表，以滿足行政命令的目標和機構任務需求[8]。這將確保聯邦機構可以在 FedRAMP 市場中輕鬆獲得最新工具，尤其是生成式 AI，並加速政府機關導入 AI 技術。

（二）參酌國外做法，建立雲端產品與服務之標準作業相關法制規範

美國 FedRAMP 旨在為雲端產品和服務提供標準化的安全性評估和授權流程，以加速聯邦機構採用安全的雲端解決方案。而新興科技優先審查框架特別針對生成式 AI 等新興科技進行優先評審，將使雲端服務供應商在提供新興科技產品時，能夠更快獲得聯邦機構的批准，促進 AI 技術的導入，確保政府能及時獲取最新的工具和技術。

為促進政府服務 AI 化，除預算編列、發展配套措施、引導政府機關評估、規劃、設計、建構與營運 AI 數位服務外，針對雲端產品和服務的安全評估、授權及監控，宜制（訂）定雲端科技須遵循的安全與風險評估標準之相關法制規範，以作為適用於政府機關的法規遵循依據，就機關處理未分類資訊的雲端產品和服務，提供標準化且可重複使用的安全性評估與授權方法，並促進 AI 技術能以更快的速度被引進政府服務之中。

撰稿人：林鈺琪

[7] 周景賀，美國發布《新興科技優先審查架構》 加速政府機構導入 AI 技術，stli 科技法律研究所，2024 年 10 月，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9254，最後瀏覽日期：2024 年 10 月 28 日。

[8] FedRAMP，同註 6；周景賀，同前註。