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

美國聯邦總務署（General Service Administration）於2024年6月27日發布《新興科技優先審查架構》（Emerging Technologies Prioritization Framework），該架構係為回應拜登總統針對AI安全所提出之第14110號行政命令，而在「聯邦政府風險與授權管理計畫」（Federal Risk and Authorization Management Program，以下簡稱FedRAMP）底下所設置之措施。

一般而言，雲端服務供應商（cloud service providers）若欲將其產品提供予政府單位使用，需依FedRAMP相關規範等候審查。《新興科技優先審查架構》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。

現階段《新興科技優先審查架構》所定義之「新興科技」係為提供下列四種功能的生成式AI技術：

1.聊天介面（chat interface）：提供對話式聊天介面的產品。允許用戶輸入提示詞（prompts），然後利用大型語言模型產出內容。

2.程式碼生成與除錯工具（code generation and debugging tools）：軟體開發人員用來協助他們開發和除錯軟體的工具。

3.圖片生成（prompt-based image generators）：能根據使用者輸入之文字或圖像而產生新圖像或影像的產品。

4.通用應用程式介面（general purpose API）：基於API技術將前述三項功能加以整合的產品。

美國政府為挑選最具影響力的產品，要求雲端服務供應商繳交相關資料以利審查，例如公開的模型卡（model card）。模型卡應詳細說明模型的細節、用途、偏見和風險，以及資料、流程和參數等訓練細節。此外，模型卡應包含評估因素、指標和結果，包括所使用的評估基準。

《新興科技優先審查架構》第一波的申請開放至2024年8月31日，且FedRAMP將於9月30日宣布優先名單。這項措施將使生成式AI技術能夠以更快的速度被導入政府服務之中。

相關連結

- Federal Risk and Authorization Management Program [FedRAMP], Emerging Technologies Prioritization Criteria and Guidance(2024)
- Federal Risk and Authorization Management Program (FedRAMP) - Artificial Intelligence, GitHub
- Emerging Technology Prioritization Framework, FedRAMP
- Release of Emerging Technology Prioritization Framework, FedRAMP
- Making access to AI a priority, U.S. General Services Administration

你可能會想參加

→ 【2023科技法制變革論壇】AI生成時代所帶動的ChatGPT法制與產業新趨勢
→ 「跨域數位協作與管理」講座活動
→ 新創採購-政府新創應用分享會
→ 【線上場】113年「新創採購機制及鼓勵照護機構參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 113年新創採購-照護機構獎勵說明會
→ 【南部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【北部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【中部場】113年「新創採購機制及鼓勵地方政府參與推動」說明會
→ 【臺北場】113年度新創採購-招標作業廠商說明會

→ 【臺中場】113年度新創採購-招標作業廠商說明會
→ 【高雄場】113年度新創採購-招標作業廠商說明會

周景賀 編譯整理

上稿時間： 2024年10月

資料來源：

Federal Risk and Authorization Management Program [FedRAMP], *Emerging Technologies Prioritization Criteria and Guidance*(2024), https://www.fedramp.gov/assets/resources/documents/Emerging-Technologies-Prioritization-Criteria-and-Guidance-V3.pdf (last visited Aug. 2, 2024).
Federal Risk and Authorization Management Program (FedRAMP) - Artificial Intelligence, GitHub, https://github.com/GSA/fedramp-ai (last visited Aug. 2, 2024).
Emerging Technology Prioritization Framework, FedRAMP, https://www.fedramp.gov/et-framework/#:~:text=This%20page%20describes%20the%20operational%20framework%20to%20prioritize%20certain%20cloud (last visited Aug. 2, 2024).
Release of Emerging Technology Prioritization Framework, FedRAMP, https://www.fedramp.gov/2024-06-27-release-of-et-framework/ (last visited Aug. 2, 2024).
Making access to AI a priority, U.S. General Services Administration, https://www.gsa.gov/blog/2024/06/27/making-access-to-ai-a-priority (last visited Aug. 2, 2024).

延伸閱讀：

Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, The White House, 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/#:~:text=(a)%20Artificial%20Intelligence%20must%20be%20safe%20and%20secure.%20Meeting%20this (last visited Aug. 2, 2024).
郭俊仁，〈美國正式推行「聯邦政府風險與授權管理計畫」〉，科技法律研究所，https://stli.iii.org.tw/article-detail.aspx?tp=1&d=5795&no=64（最後瀏覽日：2024/08/02）。

文章標籤

推薦文章