數位發展部
Ministry of Digital Affairs

行政院第 3938 次院會

公務機關使用生成式AI相關管理規範

報告人：數發部數產署 林俊秀署長

114 年 2 月 6 日

01 背景：建構我國AI可信任環境

- 鑑於人工智慧帶來的機會與可能面臨的風險，**國科會於113年預告人工智慧基本法草案**。
- 為促進AI的應用具有可靠、公平、隱私等原則，**數發部於113年建立AI評測機制**。
- 為協助公務機關測試評估適合導入AI的業務及服務，**數發部於114年公布公部門人工智慧應用參考手冊**。
- 為推動資通安全管理法所定資通安全整體防護事宜，**數發部於111年修訂各機關對危害國家資通安全產品限制使用原則**。

02

數發部三大管理措施

AI評測環境建構 - AI 評測制度

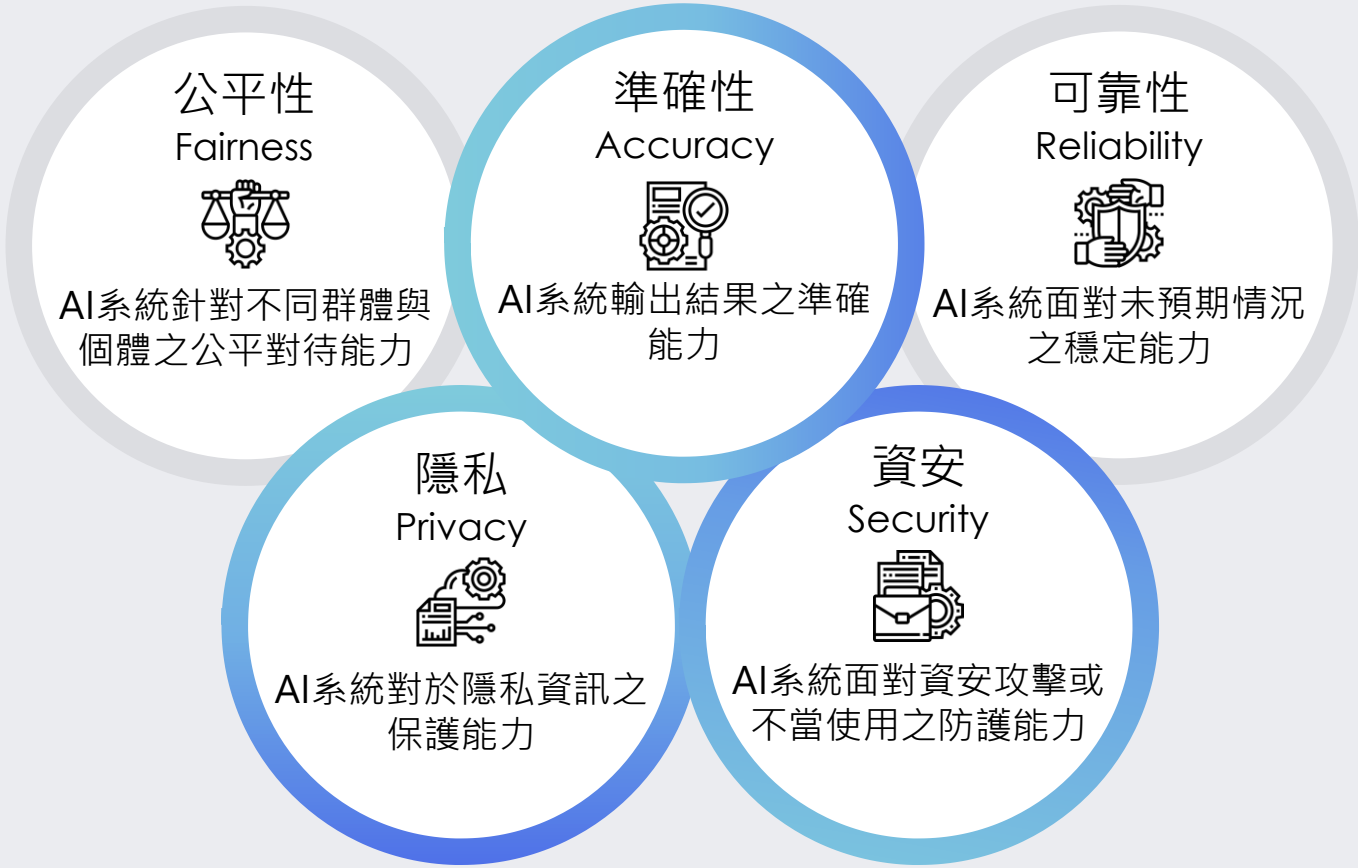
AIEC: AI Evaluation Center，AI評測中心

02

數發部三大管理措施

AI評測環境建構 - AI 評測項目

參考國際 ISO 標準、美國 NIST AI RMF、歐盟 Trustworthy AI 等相關規範，擬定評測項目，包含公平性、準確性、可靠性、隱私及資安。



02

數發部三大管理措施

AI評測制度環境建構 - AI 評測制度實施(公部門)

協助項目

諮詢輔導

- 協助相關部會建立自身領域的評測機制。
- 預計3月辦理說明會

規劃協助

- 協助相關部會規劃AI評測題庫與工具
- 視其需求整合於AIEC評測流程

推動作法

透過辦理**領域座談會**或**說明會**，協助相關部會建立該領域評測機制。

諮詢輔導 ⋁ ⋀ 交流回饋

相關部會及其主管領域

AIEC官網： https://www.aiec.org.tw/
聯絡信箱：AIECService@aiec.org.tw
聯絡電話：02-6631-6418 / 02-2771-2171 ext. 3808

02

數發部三大管理措施

AI評測制度環境建構 - AI 評測制度實施(私部門)

透過所建構之AI評測體系(AIEC、測試實驗室、驗證機構)協助我國企業進行AI產品與系統評測

1 諮詢輔導

協助送測前準備工作、輔導作業(如：模擬評測資源等)

2 中小企業投入開發

建立評測示範案例，提供中小企業開發AI產品技術參考

3 評測工具在地化

發展在地化、可接軌國際之AI評測工具

4 接軌國際

以AIEC為hub，進行國際交流與合作

02

數發部三大管理措施

公部門人工智慧應用參考手冊

數發部**為引導政府機關發展為民服務AI應用所訂定，屬參考性質之行政指導。**

AI法制架構

法律
人工智慧基本法【國科會】

操作指導
各項AI管理指引或技術指南

行政指導
公部門人工智慧應用參考手冊

行政規則
行政院及所屬機關(構)
使用生成式AI參考指引
【國科會】

實線：已公布、實施
虛線：正在擬訂或將擬訂

AI參考手冊辦理時程

2024年6月
完成國際資料蒐集與彙整

2024年10月
確認草案內容(Alpha版)

2024年12月
訂頒試行版本 (Beta版)

2025年1-10月
各機關試辦AI手冊，並回饋建議

2025年12月
增補AI手冊內容，訂頒正式版本

數發部三大管理措施

公部門人工智慧應用參考手冊(續)

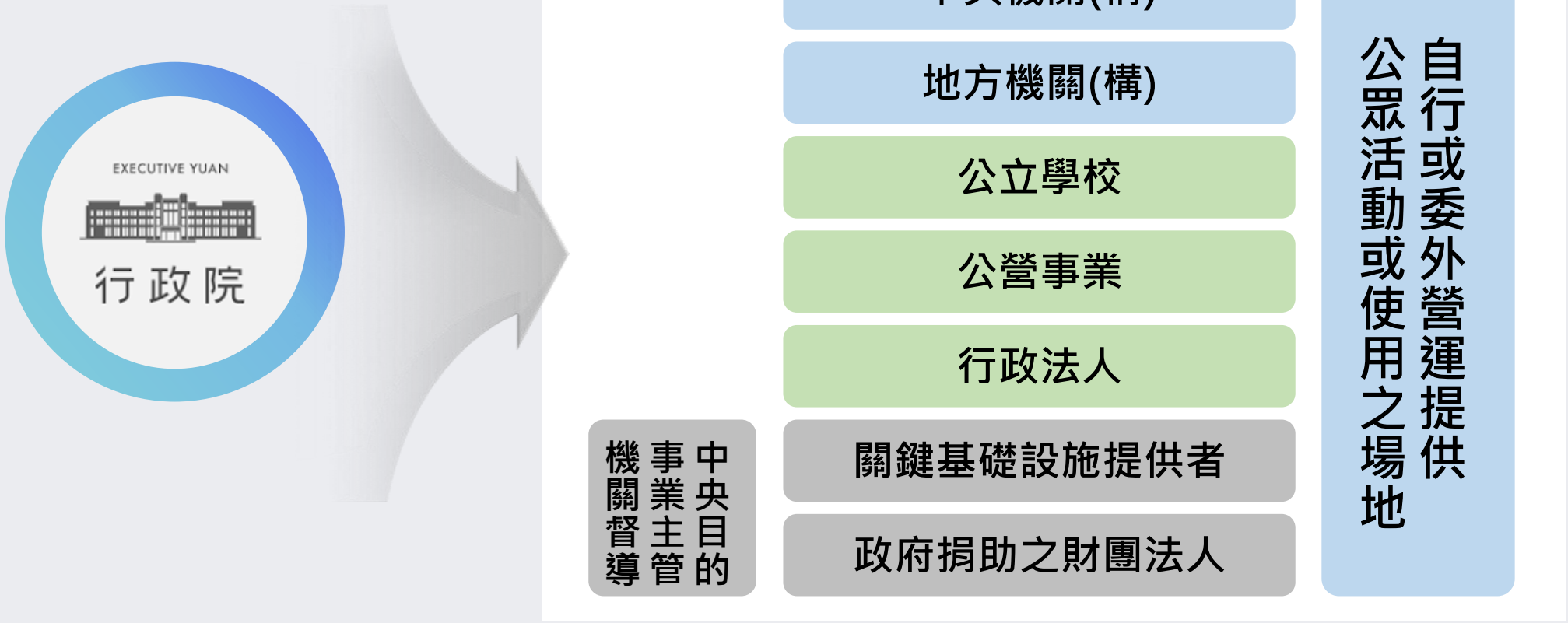
提供10個語言模型及20個AI Bots (AI Bot機器人係指透過人工智慧技術與程式設計完成特定任務的軟體應用程式)，讓**行政院所屬二級機關同仁**試用，並將配合全球LLM排名調整及 AI Bots 發展趨勢，適時調整平臺。

02

數發部三大管理措施

危害國家資通安全產品限制使用原則 - 限制使用原則規範對象

各機關對危害國家資通安全產品限制使用原則【發布日: 108/04/08、修正日: 111/11/28】



02

數發部三大管理措施

危害國家資通安全產品限制使用原則 -學術研究使用需求之處理作法

依據「各機關對危害國家資通安全產品限制使用原則」第四條

因業務需求且無其他替代方案，應具體敘明理由，經機關資安長及其上級機關資安長逐級核可，函報數位發展部核定後，以專案方式購置列冊管理，及遵守以下規定：

- **指定特定區域及特定人員使用**
- **使用理由消失應立即停止使用**
- **以不含個資及資料的電腦單機將其下載並斷網使用較為安全**

03 結語

- 公務機關導入AI的業務及服務，應經過AI評測，數發部已訂定公部門人工智慧應用參考手冊及建立評測機制。
- 為降低國家資通安全風險，數發部已訂定各機關對危害國家資通安全產品限制使用原則，供公務機關遵循。