

AI 雲平台建置案

資訊徵詢書

中華民國 115 年 9 月

一、背景說明

- (一) 專案名稱：AI 雲平台建置案（以下簡稱本案）。
- (二) 專案單位與使用者：
 - 1. 專案單位：數位發展部數位產業署（以下簡稱數產署）。
 - 2. 專案使用者：AI 資訊服務業者、各產業中小企業及數產署。
- (三) 專案背景與目標：本案為「115 年鏈結資服普及 AI 應用計畫」之建置項目，以鏈結 AI 資訊服務業者、孵化領域專業 AI 與本土 AI、提升各產業 AI 覆蓋率為目標。平台以三年（115 至 117 年）為整體規劃期程，架構涵蓋通用型 AI 應用市集、領域型產業試驗沙盒、開發型 AI 共享元件庫、公共型政府採購服務專區、政策資源專區等五大專區，以及跨專區 AI 智慧代理與共通基礎服務。
- (四) 本文件性質：本資訊徵詢書（Request for Information，下稱 RFI）參照政府採購法第 34 條第 1 項公開徵求之精神辦理，旨在蒐集 AI 服務平台、多租戶算力沙盒及 AI 元件託管之市場資訊與技術選型建議，供本案前期規劃參考，並作為後續形成招標規範（RFP）之依據。

二、需求項目簡述

以下說明五大專區之定位與關鍵功能（描述「做什麼」，技術實作方式為本 RFI 徵詢之標的），並於末項說明分階段建置範圍。

- (一) 通用型 AI 應用市集 | 市場擴散與供需媒合：遴選成熟 AI 服務上架，媒合中小企業採用。關鍵功能：服務遴選上架（線上遞案、資格審、技術審與產品審）、供需媒合（方案展示、數位診斷、搜尋與推薦）、試用及採用（試用憑證領取、導流與開通紀錄）、成效回饋（評價、定期複評、違規下架）。
- (二) 領域型產業試驗沙盒 | 領域專業 AI 與本土 AI 孵化：以機關提供之 GPU 算力，

採徵案機制核配算力配額，供資服業者結合領域資料開發與驗證 AI 模型。關鍵功能：

1. 算力配額管理：徵案申請與審議、依專案核配 GPU 配額與使用期間、用量計量與到期回收。
2. 模型訓練沙盒：多租戶隔離之線上開發環境，連結核定之領域資料集（唯讀掛載、存取稽核），支援模型微調與訓練。
3. 服務試用沙盒：將訓練成果部署於隔離試用區，媒合中小企業進行封閉測試並蒐集回饋。
4. 模型部署服務：將審查通過之模型部署為可透過 API 或 MCP 協定呼叫之服務，供開發者取用。

(三) 開發型 AI 共享元件庫 (AI Component Hub) | 元件共享與服務化加速：將 Hub / Registry 概念延伸至 AI 元件，針對 Model、Skill、MCP、Dataset、Agent 五類元件建立統一詮釋資料、發現、治理與重用機制。關鍵功能：

1. Repository 平台機制：元件註冊與版本儲存、詮釋資料檢核、審核發佈、檢索與詳情呈現、取用授權與紀錄。
2. 五類元件標準：Model 依模型卡規範並採通用開放權重格式；Skill 依代理技能開放標準；MCP 依官方伺服器描述檔驗證；Dataset 依資料集描述標準（如 MLCommons Croissant）；Agent 依代理卡規範並支援代理互通協定。

(四) 公共型政府採購服務專區：介接政府軟體採購網共同供應契約 AI 服務資訊，來源標籤化後與自有上架服務統一檢索。

(五) 政策資源專區：介接政策資源平台，於各專區服務流程中推薦相關政策資源。

(六) 跨專區 AI 智慧代理：引導上架、智能推薦與媒合、後台成效分析；以標準化

元件組裝，並具可擴充之架構。

(七) 共通基礎服務：單一登入、角色權限、通知、內容管理與稽核日誌。

(八) 分階段建置範圍：

1. 第一階段（115 年度計畫，履約至 116 年 4 月）：通用型市集全部功能；領域型之算力配額管理與模型訓練沙盒；開發型之 Repository 平台機制與 Dataset 類元件；公共型與政策資源介接；AI 智慧代理與共通基礎服務。
2. 後續階段（116 至 117 年）：領域型之服務試用沙盒與模型部署服務；開發型之 Model、Skill、MCP、Agent 四類元件。廠商應就後續階段提出架構延續與技術選型之規劃建議。

三、共通專案基本要求

- (一) 技術與介接：優先採用具通用性與互通性之開源技術，以開放標準與開放介面整合，降低廠商鎖定並確保可移轉；依國發會「共通性應用程式介面規範」提供 OpenAPI 標準文件；自行開發程式交付原始碼（含註解），使用開源或商用軟體須提交授權條款。
- (二) 資通安全：符合資通系統防護基準對應控制措施（等級以機關核定為準），完成原始碼檢測、弱點掃描、滲透測試及 SLA 效能測試，檢測結果不得含中高風險且不因驗收免除修復責任；留存資料異動與登入日誌，敏感資料加密儲存；配合資安稽核、營運持續演練及資安事件通報。
- (三) 品質測試：上線前依使用者旅程辦理功能、相容性與無障礙測試，辦理 AI 模型安全性與可信度測試，及壓力、負載與浸泡測試。
- (四) 教育訓練：依受訓對象階層提供訓練，教材電子檔提供線上下載並錄製數位影音，機關取得使用權。

- (五) 共通規範：遵循政府網站服務管理規範、政府數位服務指引、網站無障礙規範（等級以機關核定為準，含標章申請）、IPv6、ODF-CNS15251 及個人資料保護相關規範。
- (六) 陸資限制：不允許大陸地區、含陸資成分或在臺陸資廠商參與，不得聘用大陸（含港澳）地區人民；供應標的之原產地與品牌不得為大陸地區，AI 相關軟體與模組不得使用、介接或呼叫大陸（含港澳）地區開發之軟體、模型及 API。

四、徵求意見項目

本 RFI 聚焦技術方案與選型建議，無須提供報價、經費概估或專案期程。請廠商之建議納入分階段前提，確保第一階段成果可向後續階段延續。徵求課題包括但不限於：

- 系統架構建議：五大專區、AI 智慧代理與共通基礎服務之整體架構，雲端平台與地端算力之混合架構及既有系統介接方式，含後續階段擴充路徑。
- 各需求項目技術選型與設計建議：對應第二章各專區關鍵功能，逐項提出技術方案與設計作法，並敘明方案名稱與版本、開源或商用、授權條款、成熟度與導入風險。
- 運算資源估算建議：就領域型沙盒之模型訓練（微調）、服務試用（推論驗證）及模型部署（API 或 MCP 服務）三類工作負載，估算所需 GPU 資源規模與資源池切分方式、可同時支援之專案數、算力配額核配與排程策略，並敘明估算依據。
- 對本案需求項目之修正或補充建議。

五、回覆格式

- (一) 封面頁註明本案名稱與回覆單位；載明聯繫窗口之姓名、地址、電話及電子郵件。
- (二) 回覆意見摘要一頁；詳細回覆至多 50 頁，內文 12 號字，A4 版面。
- (三) 提供 WORD 與 PDF 電子檔。

六、聯絡窗口

- 本資訊徵詢由資誠創新諮詢股份有限公司辦理。
- 聯絡人：陳心昊經理
- 電子信箱：howard.h.chen@pwc.com

回覆文件請以電子郵件寄送至前述聯絡信箱。

七、其他

- (一) 本 RFI 僅為蒐集廠商參考資料，不構成任何採購之要約意思表示；本公司不負意見回復之義務，亦不對所交付資料付費。
- (二) 廠商提供之資料僅供本公司及數產署於本案規劃用途使用；廠商應確保資料之版權合法性。
- (三) 後續購案由數產署依政府採購法辦理公告，一切以正式招標文件為準；廠商是否回覆及回覆內容均不影響其參與後續採購之權利與資格。