

行政院公共工程委員會 115 年度單位預算評估報告

行政院公共工程委員會(以下簡稱工程會)115 年度預算案編列歲入 4,811 萬 6 千元，較 114 年度預算數 4,785 萬 9 千元增加 25 萬 7 千元(增幅 0.54%)；歲出 5 億 9,761 萬 2 千元，較 114 年度預算數 5 億 3,448 萬 2 千元(含追加預算數 798 萬 7 千元)增加 6,313 萬元(增幅 11.81%)。謹就工程會 115 年度預算案評估如下：

三、新增編列「運用 AI 創新應用分析及強化政府隱私資料計畫」，允宜審慎規劃及管控，以維公共建設計畫審議之專業性，並落實保護敏感資訊

工程會 115 年度預算案「公共工程技術業務-04 公共工程技術資訊體系推動」項下新增編列辦理「智慧政府數位化精進發展計畫」之「運用 AI 創新應用分析及強化政府隱私資料計畫」有關公共工程技術業務之系統建置及精進等所需經費 2,335 萬 8 千元。經查：

(一)計畫編列內容

工程會為配合數位發展部 115 至 119 年「智慧政府數位化精進發展計畫」，提報「運用 AI 創新應用分析及強化政府隱私資料計畫」，希透過 AI 創新應用與隱私強化基礎建設，推動政府資料治理模式創新，並促進公私協力發展多元應用機制，以兼顧資料利用與保護，提升資料價值。依該計畫書所載，預估總經費 2 億 2,800 萬元，期程自 115 至 119 年度；115 年度預算案編列項目主要包括系統運作所需資安維護與雲端資源支出之資訊服務費 440 萬元、委託第三方單位執行獨立之資安檢測、滲透測試與功能驗證等作業之委辦費 560 萬元、導入 AI 技術用於輔助公共建設計畫審議之開發費 835 萬 8 千元及建置隱私強化技術(Privacy Enhancing Technologies, PETs) 機制 500 萬

元，合共 2,335 萬 8 千元(詳表 1)。

表 1 工程會 115 年度預算案「運用 AI 創新應用分析及強化政府隱私資料計畫」編列情形表

單位：新臺幣千元

項目	115 年度 預算案數	說明
業務費	10,000	
資訊服務費	4,400	系統運作所需資安維護與雲端資源支出，包含資訊安全費用 140 萬元及雲端主機與 AI 服務租用費用 300 萬元。
委辦費	5,600	委託第三方單位執行獨立之資安檢測、滲透測試與功能驗證等作業，以提升系統可信度與符合資安合規要求。
設備費	13,358	
AI 創新應用開發費	8,358	用於開發智慧化公共建設計畫審議助手，導入 AI 技術輔助計畫內容分析、重點提取、經費與期程合理性評估，提升審議效率與決策品質。
建構政府隱私資料強化部署環境費用	5,000	用於建置隱私強化技術(PETs)機制，確保資料分析過程之安全與合規，符合國內法規及國際隱私保護標準。
合計	23,358	

資料來源：工程會 115 年度預算案及提供資料；本中心整理。

(二)導入 AI 輔助公共建設計畫審議，允宜參酌「行政院及所屬機關(構)使用生成式 AI 參考指引」辦理，以維計畫審議之專業性及機密性

工程會「運用 AI 創新應用分析及強化政府隱私資料計畫」主要辦理導入 AI 建置智慧化公共建設計畫審議助手及建置隱私強化技術(PETs)機制等，洽據工程會說明略以，智慧化計畫審議助手運用生成式 AI 技術，並結合知識遷移後之計畫審議準則，將既有審查規範與專業經驗轉化為系統化規則，AI 可依據此準則比對計畫書內容，迅速提取關鍵資訊，並提出具建設性

與可行性之建議，有效減少人工逐項檢視所耗費之時間，提升審議效率。

導入 AI 輔助公共建設計畫審議有助於行政效率之提升，惟為保持計畫審議之專業性及機密性，允宜參酌國家科學及技術委員會所訂「行政院及所屬機關(構)使用生成式 AI 參考指引」¹辦理，於應用 AI 技術輔助公共建設計畫審議時，包括協助掌握內容重點、提出建議及評估經費與期程合理性，須由業務單位就其風險進行客觀且專業之最終判斷，不得以未經確認之產出內容作為決策之唯一依據，且資料蒐集、處理、分析等應確實管控存取權限及隱私資料去辨識化，落實保護敏感資訊等。

綜上，工程會配合數位發展部政策，於 115 年度預算案新增編列「運用 AI 創新應用分析及強化政府隱私資料計畫」，導入 AI 建置智慧化公共建設計畫審議助手及建置隱私強化技術(PETs)機制等，運用 AI 輔助計畫審議，雖有助於行政效率之提升，惟宜審慎規劃及管控，以維計畫審議之專業性，並落實保護敏感資訊。

¹ 國家科學及技術委員會所訂「行政院及所屬機關(構)使用生成式 AI 參考指引」內容包括：生成式 AI 產出之資訊，須由業務承辦人就其風險進行客觀且專業之最終判斷，不得取代業務承辦人之自主思維、創造力及人際互動；業務承辦人不得向生成式 AI 提供涉及公務應保密、個人及未經機關（構）同意公開之資訊，亦不得向生成式 AI 詢問可能涉及機密業務或個人資料之問題；各機關不可完全信任生成式 AI 產出之資訊，亦不得以未經確認之產出內容直接作成行政行為或作為公務決策之唯一依據；使用生成式 AI 應遵守資通安全、個人資料保護、著作權及相關資訊使用規定，並注意其侵害智慧財產權與人格權之可能性，各機關得依使用生成式 AI 之設備及業務性質，訂定使用生成式 AI 之規範或內控管理措施等。