

採購規範書 (A522001346)

請購案名：前瞻研究委託-AI 代理人資安應用技術與概念驗證環境規劃研析

1. 需求說明

因應前瞻計畫核心技術研發需求及技術落地規劃需求，本案擬針對資安 AI 代理人主題領域之技術及其應用，透過委託專業顧問執行技術研析與諮詢，聚焦國際關鍵核心技術的發展趨勢與研究方向，並深入剖析我國在其技術之應用方面所面臨的風險與挑戰。並擬以相關應用調研為主軸，蒐集與前瞻和新應用技術相關之軟硬體工具平台之關鍵技術發展方向，進行作業系統、軟硬體開發平台、應用與服務技術法規等方面的資訊調研，並透過此計畫彙應用情境相關之議題。

2. 規格/功能需求及交付驗收項目：

項次	執行項目	時間	執行說明
1	專案執行會議	得標後 7 個工作天內	- 廠商得標後，7 個工作天內與工研院召開起始會議，說明委託項目工作時程及繳交項目細項。 - 定期雙週會議。
2	前瞻技術相關議題研析	2026/11/30	前瞻技術議題研析 - 資安 (紅/藍/紫隊) AI 代理人應用主題介紹 1 份 - AI 代理人開放原始碼調研報告 1 份 - 小規模概念性驗證所需之測試平台環境規劃報告 1 份
3	其他配合事項	- 前瞻相關議題、核心技術研究重點請與工研院討論。 - 須配合工研院提供及繳交相關階段性研究資料及報告。	

3. 交付驗收項目及時程：

- 第一階段付款：廠商確認得標後7個工作天內召開專案起始會議，確認專案研析目標後經驗收得付款總額70%。
- 第二階段付款：2026/11/30前繳交結案研究成果【資安 (紅/藍/紫隊) AI代理人應用主題介紹 1份】、【AI代理人開放原始碼調研報告1份】、【小規模概念性驗證所需之測試平台環境規劃報告1份】經驗收合格後支付尾款(總額30%)。

4. 得標廠商需提供顧問諮詢，若有未詳盡事宜得標廠商得全力配合委託方進行補充。

5. 此案期具有相關經驗之廠商或學研接受委託尤佳。