需求說明書（含驗收規範）

壹、購案名稱

「AI 協作之 API 及商業邏輯（BLA）研究案」採購案

貳、履約期限與預算

一、 履約期限（如遇假日，原則順延至次一工作日，有分階段交付者亦同；惟實際是否順延仍依本會需求為準）

■決標次日起至 115 年 3 月 31 日止

二、 預算

新台幣 2,800,000 元整（含稅）。

參、需求說明

一、 本案透過 AI 機制建立 API 及商業邏輯層的標準，以避免商業邏輯攻擊 (Business Logic Attack, BLA)，徵求建議報告書及展示研究環境

- 該報告需包含以下 4 個要點：

(一) API 開發建議

(二) API 盤點

(三) 透過 AI 自動學習與產出 API 商業邏輯成果

(四) 透過 AI 學習成果偵測與預防商業邏輯漏洞

二、 教育訓練

■至多 1 場（場次及時數依本會需求調整），讓相關人員確實瞭解履約標的之使用或操作。

三、 法令依據及相關規定

(一) 資通安全管理規定：

■得標廠商應遵守「委外廠商之資通安全責任事項」(詳附件)

四、 保固需求

■無

肆、交付說明

一、 交付項目、內容、期限如下：

項次	交付項目	交付內容	數量	交付型態	交付期限
1	工作計劃書	1. 執行方式規劃 2. 專業人力配置規劃 3. 工作時程規劃 4. 經費配置	1 份	紙本或電子檔	決標次日起 7 日曆天

2	AI 商業邏輯攻擊偵測研究結案報告書初稿及展示研究環境	1. 得標廠商需產出本案之結案報告，內容包含但不限於： (1)API 開發建議 (2)API 盤點 (3)透過 AI 自動學習與產出 API 商業邏輯成果 (4)透過 AI 學習成果偵測與預防商業邏輯漏洞 2. 得標廠商需進行本案之展示研究環境	1 份	電子檔	114/12/31 前
3	AI 商業邏輯攻擊偵測研究結案報告書總結報告書	得標廠商需產出AI商業邏輯攻擊偵測研究結案報告書總結報告書，內容包含但不限於 AI商業邏輯攻擊偵測研究結案報告書初稿的修訂與總結報告	1 份	電子檔	本案履約期限
4	教育訓練	課程教材	依實際狀況檢附，若無則免		同本案履約期限
5	資安文件	資料返還、刪除、銷毀聲明書(詳附件)	1 份	紙本	同本案履約期限

備註：得標廠商應依本會需求配合調整各階段交付期限，惟不可超過本案履約期限。

二、 交貨地點：台北市大安區和平東路二段 106 號 10 樓 。

三、 得標廠商應依上表提供履約標的，並提供履約通知文件予本會〔購案聯絡人〕確認。

四、 履約通知文件參考格式可至 http://www.iii.org.tw /綜合公告/採購資訊/檔案下載區下載，廠商亦可自訂格式（Email 亦視同履約通知文件，惟內容應足資識別本案）。

五、 履約通知文件僅為通知本會交付全部或部份履約標的，相關驗收事宜另依本會驗收程序辦理，本會驗收合格後方視為履約完成。

伍、驗收規範

一、 依本案需求說明書（若購案有服務建議書者亦併同納入）進行數量、內容點收。

二、 本會得要求得標廠商配合出席驗收會議，並做口頭簡報（須視本會需求提供會議文件）。

三、 本會得要求得標廠商依據本會驗收會議意見修訂調整交付項目內容，且應附上意見回覆對照。

陸、其他注意事項

一、 廠商特定資格

投標廠商不得為大陸地區廠商、第三地區含陸資成分廠商及經濟部投資審議司網站公告之陸資業者。

二、 購案聯絡人：

姓　名：資訊服務處　莊文德先生

電　話：(02)6631-8116

Email：peterchuang@iii.org.tw

三、 發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

柒、評選規範

■詳投標須知之「評選須知」內容；評選項目及建議書撰寫重點如下述。

過半數（不含半數）評選委員評定總分達 75 分以上，始為合格，方列入名次和之統計與優勝序位之排列。

項次	項目	服務建議書撰寫重點	配分
		封面、目錄	
1	**執行力與配合度** ●人力配置規劃 ●執行團隊之相關經驗、學經歷及過去績效 ●計畫執行及管理能力	1. 公司簡介（如業務範圍、營運狀況) 2. 執行團隊組織與工作分配 3. 專案負責人及執行團隊成員履歷：包含現職、學經歷等，團隊成員具以下資格者尤佳，並提供證照影本或驗證資料： ● 至少一名持有有效期間內之 ISO/IEC 42001(人工智慧管理系統)證照之專業人員 ● 至少一名具有三大公有雲(擇一)相關 AI 證照之專業人員 4. 廠商履約實績：請詳述專案經驗及其成效 ● 具備近一年(投標截止日)曾承辦研究、顧問或技術服務案等專案經驗，檢附合約、得標證明、驗收文件(擇一)等證明文件者尤佳	**20**
2	**整體企劃** ●企劃內容可行性 ●執行進度之時程規劃	5. 說明整體企劃內容、理念 6. 提供時程進度規劃，說明相關工作預定進度、完成時點	**60**
3	**經費合理性** ●相關執行費用估算與分配之合理性	7. 於服務建議書詳列報價內容（請詳列各物品／服務／人力……等之規格、數量、單價明細）	**20**
合計			**100**

【附件】

委外廠商之資通安全責任事項

一、 辦理受託業務之相關程序及環境，應填寫「委外廠商資通安全管理措施說明表」佐證具備完善之資通安全管理措施，或通過第三方驗證(TAF 認證機構)，如受託業務涉及提供雲端服務者，應提供原廠 ISO 27001 標準認證。

二、 應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員，負責推動、協調及督導資通安全管理事項。

三、 經本會同意，委外廠商始得將受託業務分包予第三人，委外廠商須要求並監督該第三人應具備與委外廠商同等之資通安全維護措施及標準，並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。

四、 辦理客製化資通系統之開發，若涉及利用非自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明。

五、 辦理受託業務，違反資通安全相關法令或知悉資通安全事件發生時，應立即通知本會承辦單位及採行必要之補救措施，並應配合本會之資通安全事件通報及相關處理作業。委外廠商未為通知或未配合本會相關處理作業者，應就本會因此所生之一切損害負賠償責任。

六、 委託關係終止或解除時，委外廠商就履行委託契約而持有之資料應返還、移交、刪除或銷毀，並填具「資料返還、刪除、銷毀聲明書」。

七、 委外廠商同意本會得定期或於知悉發生可能影響本案之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

八、 委外廠商受託業務涉及資通訊軟體、硬體或服務等相關事務者，執行本案之團隊成員不得為大陸籍人士，並不得提供及使用大陸廠牌資通產品或服務。

九、 受託業務涉及國家機密時，執行業務之相關人員應接受適任性查核，並受國家機密保護法規定之管制。

委外廠商應確保執行該業務之所屬人員及可能接觸該國家機密之其他人員，無下列事項：

(一)曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

(二)曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

(三)曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

(四)招標公告、招標文件或契約所載其他與國家機密保護相關之具體項目。

十、 委外廠商執行受託業務之人員進出本會範圍應受限制。且應遵守本會「資通服務廠商派駐人員資通安全同意表」之資通安全相關規定。

十一、委外廠商駐點人員若要更換或撤離，應填寫「資通服務廠商派駐人員撤離資料表」。

【附件】

資料返還、刪除、銷毀聲明書

填寫日期： 年 月 日

購案/委外資通作業名稱（下稱本案）		廠商名稱（下稱立書人）	（請加蓋廠商印鑑）
		立書人之負責人	（請加蓋負責人印鑑）

立書人因執行本案所持有之本案相關資料（包括但不限於開發需求規格書、原始碼、執行碼或程式等，詳如下表所列）及其影本、複製本或備份予以返還、刪除或銷毀，且將嚴格監督並確認立書人及其參與本案的相關人員（包括但不限於勞工、派遣人員、受任人或分包廠商等）未以任何形式為資料之私自留存、使用、竄改或洩漏，亦不得為自身或第三人的利益而使用。

立書人及其參與本案之相關人員若發生將資料私自留存、使用、竄改或洩漏等不利於 貴會的行為，立書人同意配合 貴會進行必要之查證行為及提供 貴會所需之協助，如經查證屬實，立書人願支付本案價金總額 20 %之懲罰性違約金及賠償 貴會所受之一切損害，並負一切法律責任，絕無異議。

編號	資料名稱	數量	檔案類型	執行方式
範例	需求/設計規格書	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
範例	程式原始碼	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
1.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀
2.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀

備註：表格不敷使用，請自行增加。

(資策會)點收人簽名：	(資策會)點收日期：