需求說明書（含驗收規範）

壹、購案名稱

「AI 工具產品測試與安全檢測」採購案

貳、履約期限與預算

一、 履約期限

決標次日起至 115 年 12 月 15 日止。

二、 預算

新台幣 800,000 元整（含稅）。

參、需求說明

為促進「Edge AI Mini Data Center 架構建置與邊緣 AI 應用推廣」計畫開發之工具成果推廣與業者落地應用，擬委託得標廠商針對四項 AI 工具進行產品測試與資安檢測，建立未來推廣所需之品質證據，並提供相關測試結果以確保工具品質受檢核。

一、 AI 工具推廣及上架所需文件

(一) 文件準備及製作：得標廠商應依本會指定之 AI 工具上架平台相關申請規範及文件格式，協助辦理本案四項 AI 工具推廣及上架所需文件之準備、撰寫、彙整及檢視，文件項目包含

1. AI 工具上架申請書。
2. AI 工具上架申請切結同意書。
3. AI 工具規格與上架說明文件。
4. AI 工具實績證明文件。
5. 其他經本會確認屬本案上架申請必要之相關文件。

(二) 文件內容確認及調整：文件編製所需之工具資訊及相關佐證資料，由本會提供；得標廠商應配合本會審閱意見進行必要之補充及調整，以符合本案上架申請之文件需求。

(三) 成果交付：標廠商應於 115 年 11 月 30 日前交付本案 AI 工具推廣及上架所需文件電子檔各一式，包含可編輯格式及 PDF 格式，供本會後續辦理上架申請作業；本項工作以完成上述文件並經本會確認為限，不包含上架申請送件及取得上架核准。

二、 AI 工具資安檢測

(一) 檢測範圍：得標廠商應針對本案以下四項 AI 工具進行程式源碼安全檢測，檢測範圍以本會提供之送測版本及程式碼為準：

1. AI 設備維修知識通。
2. AI 全流程客訴通。
3. AI 差勤智配通。
4. AI 技術知識跨語通。

(二) 檢測執行方式：

1. 應委由通過「資訊安全服務機構能量登錄」且登錄服務項目包含程式源碼檢測項目之第三方廠商執行檢測。

2. 應使用具合法授權之程式源碼掃描工具。
3. 檢測所發現之弱點，應經人工檢視及確認，辨識可能之誤判情形，以確保檢測結果之合理性及正確性，並彙整及報告交付。

(三) 檢測報告內容：每項 AI 工具分別交付中文程式源碼安全檢測報告，報告至少包含下列內容但不限於：
1. 受測版本（受測 AI 工具名稱、程式碼版本及檢測範圍）。
2. 檢測掃描工具名稱、版本及檢查規則。
3. 經人工確認之弱點清單，包含弱點類型、風險等級及所在位置。
4. 弱點風險說明修補建議。
5. 如有弱點誤判項目須排除誤判。
檢測報告中如出現密碼、金鑰或其他機敏資訊，應予遮蔽。

(四) 成果交付：得標廠商應於 115 年 11 月 30 日前完成四項 AI 工具之程式源碼安全檢測，並分別交付中文檢測報告電子檔各一式，共計四式。

三、 AI 工具產品測試

(一) 測試規劃及執行：得標廠商應依本會提供之四項 AI 工具功能清單，擬定測試項目、操作步驟及預期結果，測試計畫須經本會確認後執行。測試以確認各項功能可正常操作、輸入與輸出結果正確為原則。

(二) 測試報告內容：每項 AI 工具應分別提出中文測試報告，報告至少包含但不限於：
1. 受測 AI 工具名稱及版本。
2. 測試項目、操作步驟及預期結果。
3. 逐項列出測試項目、實際結果及是否通過。
4. 未通過或無法完成測試的項目，應說明實際情形及原因。
5. 測試結果彙整及相關建議。

(三) 成果交付：標廠商應於 115 年 12 月 15 日前完成四項 AI 工具之程式源碼安全檢測，並分別交付中文檢測報告電子檔各一式，共計四式。

四、 法令依據及相關規定

(一) 資通安全管理規定：
1. 得標廠商應遵守「委外廠商之資通安全責任特別約定事項」(詳附件)。

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	服務建議書	內容包含但不限於： 1. 推廣及上架所需文件 2. 工具資安檢測規劃 3. 工具產品測試規劃 4. 時程規劃 5. 執行團隊 6. 經費預算	1 份	紙本或電子檔	決標次日起 5 個日曆天
2	資安文件	得標廠商簽署之「委外廠商資通安全管理措施說明表」	1 份	紙本	決標次日起 5 個日曆天

		※格式請向購案聯絡人索取。			
3	AI 工具推廣及上架申請文件	依「參、需求說明、一」完成之各項工具申請文件	4 套，每項工具 1 套	電子檔	115 年 11 月 30 日
4	AI 工具資安檢測	依「參、需求說明、二」完成 AI 工具之中文檢測報告	4 份	電子檔	115 年 11 月 30 日
5	AI 工具產品測試	依「參、需求說明、三」完成 AI 工具各別測試報告	4 份	電子檔	115 年 12 月 15 日
6	資安文件	資料返還、刪除、銷毀聲明書	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：同購案聯絡人。

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、 購案聯絡人：

姓　名：人工智慧研究院 孫小姐
電　話：(02)6607-2519
Email：betsysun@iii.org.tw
地　址：台北市松山區民生東路四段 133 號 13 樓

二、 發票資料：

抬　頭：財團法人資訊工業策進會
統一編號：05076416

柒、審查須知

■詳投標須知之「審查須知」內容；審查項目及建議書撰寫重點如下述。

項次	項目	服務建議書撰寫重點 **（請依下列章節序參考製作）**
1	**執行力與配合度** ● 人力配置規劃	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

	● 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	3. 專案負責人及執行團隊成員履歷：包含現職、學經歷等 4. 廠商履約實績：請詳述專案經驗及其成效
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
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**）

【附件】

委外廠商之資通安全責任特別約定事項

一、委外廠商應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守本會、本會業主之資通安全管理及保密相關規定。此外，本會、本會業主保有依本會與委外廠商同意之適當方式對委外廠商及其分包廠商以派員稽核、委由資通安全管理法主管機關籌組專案團隊稽核或其他適當方式執行相關稽核或查核的權利，稽核結果不符合本採購案約定、資通安全管理法、其相關子法、行政院所頒訂之各項資通安全規範及標準者，於接獲本會通知後應於期限內完成改善，未依限完成者，依本採購案之契約或履約相關規定「違約罰則」約定計罰逾期違約金。

二、委外廠商執行本採購案應依行政院、本會及本會業主資通安全要求，執行必要之系統設定及修補等改善措施。

三、委外廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，提出安全性檢測證明。涉及利用非委外廠商自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明，委外廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

如履約項目涉及資通系統且(1)屬本會、本會業主之核心資通系統，或(2)採購金額達新臺幣一千萬元以上，委外廠商交付之軟硬體及文件，應接受本會、本會業主，或本會、本會業主所委託之第三方進行安全性檢測：

□ 系統主機弱點掃描

□ 網頁弱點掃描

□ 滲透測試

□ 原始碼檢測

□ 其他_____

四、委外廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

五、委外廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性，以符合本會、本會業主對系統品質及資通安全的要求。

六、委外廠商提供服務，如違反資通安全相關法令、知悉本會或自身發生資安事件時，均必須於 30 分鐘內通報本會，並於 4 小時內提供資安事件等級評估、處理應變規劃及建議；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。

七、資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。

八、委外廠商如有下列情形，應依下列約定負責：

1. 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。如造成第三人損失者，亦同。
2. 本會業主為**經濟部產業發展署或數位發展部數位產業署**時，履約期間內委外廠商提供之資訊服務，如有未達本會所定服務水準及績效，除有不可抗力或不可歸責於委外廠商事由外，依本項約定計算違約金。屬遲延性質之損害賠償，且已依本採購案之契約或履約相關規定「違約罰則」約定計罰逾期違約金者，不再依本項計算違約金。但屬

遲延性質之項目依本項計算違約金數額較高者，改依本項計算。

(1) 依本項計算違約金之總額，以本案契約價金總額之 20%為上限。

(2) 服務水準及績效違約金計算方式詳下表：

〔表 1-1〕

評估項目	評斷方式	要求基準	違約金計點	是否須符合要求？	每點違約金金額
定期維護	未依契約規定維護	每次統計	每逾 1 日(或小時)，計 1 點	□是。 ■否，本案無資通系統。	依本表計罰之違約金，每點為新臺幣 5,000 元
故障排除、系統修復	系統中斷時間，不得高於 24 小時	每次統計	每次計 1 點		
系統可用率	系統各項功能，可正常提供使用者之時間百分比，不得低於 95%	每季統計	每不足 95%，計 1 點		
	單日累計故障時數(不滿 1 小時，以 1 小時計)	每日不得超過 4 小時	每逾 1 小時，計 1 點		
資安指標	對於所維護之系統，未於規定期限取得認證日數	每次認證超過期限	每逾 1 日，計 1 點	□是。 ■否，本案無資通系統。	
	資安事件之通報及應變：自知悉或接獲資安事件通知或即時警示(不滿 1 小時，以 1 小時計)	應至遲於 30 分鐘內通報本會，並於 4 小時內提供資安事件等級評估、處理應變規劃及建議	1. 資安事件每次計 1 點。每逾 1 小時未通報本會 1 點。 2. 每逾 1 小時未提供資安事件等級評估、處理應變規劃及建議計 1 點。	無論是否有資通系統，如知悉資安事件，均須配合通報。	
	完成損害控制或復原作業之時效(不滿 1 小時，以 1 小時計)	應於知悉資通安全事件後 72 小時(重大資安事件為 36 小時)內完成損害控制或復原作業	每逾 1 小時，計 1 點		
	調查及處理資安事件之時效	完成損害控制或復原作業後，應於 1 個月內送交調查、處理及改善報告(或協助本會調查處理)	每逾 1 日，計 1 點		

評估項目	評斷方式	要求基準	違約金計點	是否須符合要求？	每點違約金金額
	本會、本會業主資料之機密性及完整性	本會、本會業主擁有之敏感資料應採取適當之防護措施，以避免不當外洩或遭竄改	委外廠商於本契約承接範圍內，因未採取適當防護，致本會、本會業主敏感資料外洩或遭竄改時，按受影響資料筆數，每筆計1點/按次數計1點	□是。 ■否，本案無資通系統。 □不適用，本案資通系統無敏感資料。	
	個人資料之機密性及完整性	資通系統所擁有之個人資料應採取適當之防護措施，以避免不當外洩或遭竄改	委外廠商於本契約承接範圍內，因未採取適當防護，致個人資料外洩或遭竄改時，按受影響資料筆數,每筆計1點/按次數計 1點		
其他	違反契約約定委外廠商應履行之項目	每季統計	每次計1點		

九、本採購案履約完畢或提前終止、解除後，委外廠商應刪除或銷毀執行本採購案所持有本會、本會業主之相關資料，或依本會指示返還或移交之，並保留執行紀錄。

十、其餘涉及資通安全事項，由本會及業主視個案實際需要，依國家資通安全研究院（網址：www.nics.nat.gov.tw）共通規範辦理，例如「政府機關雲端服務應用資安參考指引」、「政府資訊作業委外安全參考指引」與資通安全有關事項。

十一、 本附件規範與附件「委外廠商之資通安全責任事項」衝突部分，應優先適用本附件。

【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：