需求說明書（含驗收規範）

壹、購案名稱

「滲透測試檢測&弱點掃描服務」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 12 月 15 日止

二、 預算

新台幣 2,700,000 元整（含稅）。

本案採複數決標，各得標廠商之預算上限為新台幣 1,350,000 元整（含稅）。

（得標廠商家數上限 2 家，決標結果未達前述預計決標家數時，本會得決定從缺或續行辦理招標作業。）

參、需求說明

一、 重點需求

(一) 因承接數位發展部數位產業署「數位服務採購環境躍升計畫」，依「計畫資通系統資通安全稽核作業」規定，進行弱點掃描及滲透測試檢測服務。

(二) 遠端弱點掃描項目說明

1. 主機系統弱點掃描-針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定、帳號密碼設定及管理方式等進行弱點掃描，系統弱點掃描的項目，應符合 Common Vulnerabilities and Exposures(CVE)發布的弱點內容(最新版)，至少包含以下項目：a.作業系統未修正的漏洞掃描、b.常用應用程式漏洞掃描、c.網路服務程式掃描、d.木馬、後門程式掃描、e.帳號密碼破解測試、f.系統之不安全與錯誤設定掃描、g.網路通訊埠掃描。
2. Web 網頁弱點掃描-針對機關網頁安全弱點進行掃描，掃描項目應符合 OWASP TOP 10 項目(以官方網站公告最新資訊為主，請廠商以最新內容掃描)。

(三) 遠端滲透測試項目說明如下表：

測試類型	測試類別	測試項目
作業系統	遠端服務	至少包含遠端服務套件弱點測試等項目
網站服務	設定管理	至少包含應用程式設定測試、檔案類型處理測試、網站檔案爬行測試、後端管理介面測試及 HTTP 協定測試等項目
	使用者認證	至少包含機敏資料是否透過加密通道進行傳送及使用者帳號列舉測試等項目

測試類型	測試類別	測試項目
	連線管理	至少包含 Session 管理測試、Cookie 屬性測試、Session 資料更新測試、Session 變數傳遞測試及 CSRF 測試等項目
	使用者授權	至少包含目錄跨越測試、網站授權機制測試及權限控管機制測試等項目
	邏輯漏洞	至少包含網站功能測試、網站功能設計缺失測試及附件上傳測試等項目
	輸入驗證	至少包含 XSS 漏洞測試、SQL Injection 測試、LDAP Injection 測試、XML Injection 測試、SSI Injection 測試、XPath Injection 測試、Code Injection、OS Commanding 測試及偽造 HTTP 協定測試等項目
	Web Service	至少包含 WSDL 測試、XML 架構測試、XML 內容測試及 XML 參數傳遞測試等項目
	Ajax	至少包含 Ajax 弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目
應用程式	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	檔案傳檔服務套件	至少包含 FTP、NETBIOS 及 NFS 等常見檔案傳輸服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	遠端連線服務套件	至少包含 SSH、TELNET、VNC 及 RDP 等常見遠端連線服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目

測試類型	測試類別	測試項目
	其他	包含 Firewall、IDS/IPS、Database、LDAP、SMB、LPD、IPP、Jetdirect 及 RTSP 等常見應用程式或網路套件之弱點掃描項目

二、 完成以下計畫網站【遠端弱點掃描項目、遠端滲透測試項目】，並提供服務報告。

網站	弱點掃描	滲透測試
產品徵求系統（含雲端服務檢測管理系統）	初測 1 次、複測 2 次	初測 1 次、複測 2 次
詢價訂價系統	初測 1 次、複測 2 次	初測 1 次、複測 2 次
新版開標系統（資格／價格審查）	初測 1 次、複測 2 次	初測 1 次、複測 2 次
服務評選系統	初測 1 次、複測 2 次	初測 1 次、複測 2 次
政府軟體採購網	初測 1 次、複測 2 次	初測 1 次、複測 2 次
履約管理系統（含電子契約簽章）	初測 1 次、複測 2 次	初測 1 次、複測 2 次

*上述測試次數得依實際狀況進行調整

三、 修補諮詢會議

■至少 2 場（每場場次 1 小時）。

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事項」(詳附件)。
2. ■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.工作計畫內容 2.工作進度 3.工作團隊組織與工作分配 4.經費配置	1 份	電子檔	決標次日起 7 日曆天
2	個資文件	得標廠商簽署之委外廠商個資安全管理措施說明表 ※格式請向購案聯絡人索取。	1 份	紙本	決標次日起 7 日曆天

		（若需求未涉及蒐集、處理或利用個人資料則免）			
3	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」 ※格式請向購案聯絡人索取。 ※若需求非屬資通作業委外則免	1 份	紙本	決標次日起 7 日曆天
4	弱點掃描初、複測報告	6 個計畫網站弱點掃描報告。(對應需求說明第二點(一)~(六)系統)	各 1 份	電子檔	115 年 11 月 20 日
5	滲透測試初、複測報告	6 個計畫網站滲透測試報告。(對應需求說明第二點(一)~(六)系統)	各 1 份	電子檔	115 年 12 月 10 日
6	修補諮詢會議	提供弱點修補建議簡報	2 份	電子檔	115 年 12 月 10 日
7	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：高雄市苓雅區中華四路 2 號 3 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

1.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資訊服務業者。

2.需具有能量登錄表(資訊安全能量登錄 | SECPAAS | Security platform as a service.)

二、 購案聯絡人：

姓　名：數位轉型研究院　　吳坤達 先生

電　話：(07) 966-7328

Email：kundawu@iii.org.tw

地　址：高雄市苓雅區中華四路 2 號 3 樓

三、 發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

柒、評選須知

■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 70 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 **（請依下列章節序參考製作）**	配分
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 4. 廠商履約實績：請詳述專案經驗及其成效	**20**
2	**專業執行能力及完整性** **●進度時程控管、資料管制與品質保證** **●資訊安全及保密之規劃及執行方式** **●執行進度之時程規劃** **●各項服務項目及交付項目的規劃完整性**	1.說明整體專案內容、執行時程 2.資訊安全、個資安全及保密之規劃及執行方式 3.提供時程進度規劃，說明相關工作預定進度、完成時點 4.各項服務項目及交付項目的規劃說明，含使用工具及方法	**60**
3	**經費合理性** ● 相關執行費用估算與分配之合理性	5. 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、 委外廠商辦理受託業務之相關程序及環境，應依廠商類型填寫適用之「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，或通過第三方資安驗證，如受託業務涉及提供雲端運算服務(IaaS)者，應提供原廠 ISO 27001、ISO 27017、ISO 27018 或 CSA STAR 等同質性證書或 SOC 2 報告。如委外廠商為國外廠商，或經由代理商委託國外廠商辦理受託業務，具備前述證書、報告或資安相關管理措施者，得免填之。

二、 委外廠商受託業務內容如涉及資通系統委外開發、維護或維運，應辦理「主機資通安全管理要求檢核表」適用之檢核內容，並於該表說明辦理情形，交由本會委外業務負責人確認。

三、 委外廠商應建立資通安全管理制度。

四、 委外廠商(除自然人外)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。

五、 委外廠商專案人員應定期接受資通安全教育訓練。

六、 委外廠商專案人員使用之電腦應安裝防毒軟體，並定期更新病毒碼及執行病毒掃描，電腦作業系統亦應定期更新。

七、 委外廠商應對專案相關資料建立存取管控機制。

八、 經本會同意，委外廠商始得將受託業務分包予第三人並對其資安管理全權負責。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或標準，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。

九、 辦理資通系統開發/維護/維運作業，應依受託業務指定之系統防護需求等級落實「資通系統防護基準控制措施」。

十、 辦理資通系統開發/維護作業，應制定安全軟體開發生命週期程序，並建立資安檢測機制(源碼掃描、應用系統弱點掃描)、原始程式碼備份及版本控管機制，且應用系統開發測試及正式環境應區隔在不同作業環境。

十一、 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。

十二、 辦理資通系統維運作業，如主機所在實體環境由委外廠商提供者，應具備消防設備、備援電力設備、溫溼度監控設備及監視設備，並定期保養與檢查以確保正常運作。

十三、 委外廠商應就受託業務建立資通安全事件通報機制，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、應變、調查及改善等相關處理作業。委外廠商未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。

十四、 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」。

十五、 委外廠商同意本會得於履約期間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委外廠商資通安全管理措施完善性與受託業務之執行情形，

如有稽核發現事項或不符合委託契約資安要求之情形，應於履約期限內完成改善，並提報改善措施執行情形及相關佐證予本會確認。如無法於履約期限內完成改善，委外廠商應說明原因並經本會同意。

十六、 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。

十七、 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。

十八、 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「資通服務駐點人員資通安全同意表」之資通安全相關規定。

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

【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

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，以新臺幣契約總金額之 20% 為上限。

（2）服務水準及績效違約金計算方式詳下表：

〔表 2-1〕

評估項目	評斷方式	要求基準	違約金計點	每點違約金金額
故障排除、系統修復	經本會通知(不限形式)後，未依契約規定，修復或提供相同系統供本會暫時使用	每次統計	每逾 4 小時，計 1 點	依本表計罰之違約金，每點為新臺幣 1,000 元
資安指標	知悉發生資安事件之通報、損害控制或復原作業時效	應於 30 分鐘內通知本會（或接獲本會通知 30 分鐘內），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，降低資通安全事件對本會業務之衝擊	每逾 30 分鐘計 1 點	
	完成損害控制或復原作業之時效	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	

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：