需求說明書（含驗收規範）

壹、購案名稱

「114 年資策會核心網站系統滲透測試服務」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 114 年 12 月 19 日止

二、 預算

新台幣 375,000 元整（含稅）。

參、需求說明

一、 本案滲透測試標的為財團法人資訊工業策進會資訊服務處（以下簡稱本會）內部資通系統(網站)共 3 套(各網站功能數量如下表，實際以滲透時的網站情況為準)，分別執行滲透測試（含初測與複測），得標廠商於得標後應依本專案需求之規定，於 114 年 10 月 17 日前完成滲透測試初測，並於執行完畢兩週內向本會簡報說明測試結果及修復建議，經本會確認後始交付初測結果說明簡報，以便本會視需要進行系統修正或調整。

若第一次測試發現網站系統弱點需進行修正或調整，得標廠商應於本會完成修正或調整後進行複測，並交付複測結果報告。

若初測結果無發現網站系統弱點，則免進行複測，本會並得依決標報價單扣減複測相關之費用價款，得標廠商不得異議。

網站	網站一	網站二	網站三
功能數量	58	55	180

二、 專案執行需求：

(一) 本案得標廠商應於決標次日後 14 日曆天(含)內繳交工作計畫書一份說明專案執行方式及期程規劃。

(二) 因本案內容涉及內部敏感資訊，得標廠商不得將本案轉/分包予其他廠商執行。

(三) 得標廠商需以公司名義與本會簽訂保密切結書（附件二）。

(四) 本案團隊人力至少應包含專案負責人／專案經理與滲透測試服務人員；為確保專案如期如質完成，得標廠商應針對本專案之需求，妥慎成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。

(五) 滲透測試服務執行之專案組織成員於執行期間不可任意變動，如有特殊情況，須於變動前 30 日曆天(含)提供書面說明，經本會負責人同意後始得更換，所替換的人員亦須符合本案之人員資格要求；如得標廠商未於一個月前提供書面說明，將依違約罰則計罰。

(六) 專案執行期間如有涉及資料傳輸皆須事先取得本會同意，並採加密連線方式傳輸。

(七) 品質需求

1. 得標廠商應訂定品質管理流程，本會並得視情況予以稽核。

2. 得標廠商於專案期間應辦理專案啟動會議，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本會備考。

三、 滲透測試專業需求：

(一) 本案滲透測試須至現場執行。

(二) 本會得視業務重要性及敏感度，提供滲透測試範圍之測試環境系統供得標廠商進行測透測試。

(三) 滲透測試內容須包含網路環境滲透，以黑箱測試模式，模擬外部駭客的角度嘗試找出現有測試範圍對外網路服務及設備的安全漏洞，並利用這些漏洞滲透與入侵至測試範圍主機，本會不提供相關資訊。

(四) 滲透測試內容須包含網頁應用程式滲透，採用黑箱及灰箱混合測試模式，針對測試範圍之網站服務系統，先模擬外部駭客在沒有帳號及不知系統架構進行測試；或經由測試帳號進入服務系統方式，以合法員工角度，從系統內部進行應用系統與程式之深入安全分析測試。

(五) 滲透測試項目須包含 OWASP（Open Web Application Security Project）網站暨其應用程式安全測試項目。

(六) 得標廠商執行滲透測試時，須使用固定來源 IP，並於執行前通知本會，以利本會監控執行進度及系統狀況，區分真實攻擊與測試流量。

(七) 廠商須自備執行本案所需之相關軟、硬體設備。若滲透測試過程中可能採用的工具具有商業性質，本會得要求隨時提供原廠軟硬體合法使用授權證明；如因前述原因造成之法律糾紛，其損害概由廠商承擔。

(八) 執行任何會影響系統正常服務之測試必須經本會同意方可進行。執行期間若發現有外部駭客入侵或內部人員不尋常行為，應立即告知本會並協助釐清權責。

(九) 滲透測試成功後，針對每一風險均需提供證據佐證，須採以下方式擇一提供：

1. 滲透成功之擷圖畫面與說明。
2. 重要資料採樣擷圖與說明。

除此之外，不得對現行系統、檔案及資料等任何資訊進行新增、刪除及修改等異動。如有執行上之必要，需與本會討論說明並取得同意後，始可進行。

(十) 於測試執行期及結束後，須依下列原則，協助維護或回復受測環境：

1. 測試過程中，對作業環境的任何變更必須以不影響現行系統作業為最高原則。
2. 除為了擷取證據所需，測試過程中，不可任意變更受測環境。如有其他變更需要，應對本會充份說明並取得其同意。
3. 執行流程中對作業環境的任何變更均需記錄，並條列於滲透測試報告中，包含新增帳號、目錄及檔案等。
4. 測試作業結束時，滲透測試服務團隊須逐條回復所進行的變更，並條列回復結果於滲透測試報告中。
5. 如有未能回復之項目，須告知本會說明原因，並協助處理回復。未能回復之項目亦須條列於滲透測試報告中。

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」(詳附件一)。

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	專案啟動文件	1. 委外廠商資通安全管理措施說明表 2. 工作計畫書： 依需求內容提供，包含測試範圍確認、時程規劃、人員權責說明 3. 專案啟動會議簡報（含工作計畫書相關內容）	各 1 份	電子檔	決標次日起 14 日曆天
2	滲透測試執行說明簡報（初測報告）	1. 測試範圍、時程 2. 測試執行方式 3. 系統弱點及弱點之風險等級說明（若有發現弱點）及修復建議 4. 整體安全建議	1 份	電子檔	114 年 10 月 31 日
3	滲透測試執行結案報告	1. 執行結果摘要說明 2. 執行計畫 3. 執行期間/執行項目/執行範圍/專案成員 4. 專案管理會議紀錄(若無則免) 5. 執行情形：針對服務說明之所有測試項目提出滲透測試結果，含初測發現之系統弱點與弱點風險等級說明，及弱點複測結果（若初測無發現弱點則免附），實際測試項目視受測主機或網站所提供的服務為主，並提出改善建議 6. 綜合結語與建議	1 份	電子檔	同本案履約期限
4	資安文件	資料返還、刪除、銷毀聲明書(詳附件三)	各 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：台北市民生東路四段 133 號 14 樓　資安科技研究所。

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、廠商特定資格

一、 廠商資格：

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件：

(一) 投標廠商須實施資訊安全管理制度，提供通過 ISO 27001：2022 版以上驗證之證明，並於履約期間內持續有效；如驗證之效期於履約期間內屆期，則開標時效期至少由開標次日起算，尚餘 30 天以上，且須於屆期 1 週前提供有效之證明留存本會備查。

二、 滲透測試服務人員資格：

本案滲透測試服務人員，應具備以下所列舉之技能資格，以確保服務水準：

(一) 滲透測試工具使用技能：至少一名具備 CEH（Certified Ethical Hacker）證照。

(二) 滲透測試服務專業技能：至少一名具備 GPEN（GIAC Penetration Tester）、GWAPT（GIAC Web Application Penetration Tester）、CPENT（EC-Council Certified Penetration Testing Professional）或 ECSA（EC-Council Certified Security Analyst）證照。

註：上述人員之專業證照，並於履約期間內持續有效；如專業證照之效期於履約期間內屆期，則開標時效期至少由開標次日起算，尚餘 30 天以上，且須於屆期 1 週前提供有效之證明留存本會備查。

(三) 提供上述人員之在職證明勞保文件（二擇一）

1. 投保資料明細（請至 https://edesk.bli.gov.tw/cpa/，勞保局網站「投保單位網路申報及查詢作業-e 化服務系統」被保險人投保資料查詢選項列印投保資料投標**（查詢日應於等標期間內）**，未及納入網站資料者得以勞保加保證明代之）。
2. 最近一期勞保清冊，未及納入最近一期清冊者得以勞保加保證明代之。

二、 購案聯絡人：

姓　名：資安科技研究所　蘇冠萍小姐

電　話：（02）6607-6331

Email：bearsu@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、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）**
		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 （1） 業務範圍 （2） 人力、資本額 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、資安證照等 4. 廠商履約實績：請詳述專案經驗及其成效；如有承接政府部門、財團法人、公協會等單位之「滲透測試」專案(請提供相關證明，例如合約或決標證明等)，或經國家資通安全研究院資安服務廠商評鑑 113 年度「滲透測試」B 級以上之廠商。
2	**整體服務建議與規劃** ●整體服務建議之內容可行度 ●執行進度之時程規劃 ●加值服務(有提供者為佳)	5. 說明滲透測試項目、執行方式及專案品質管理流程等 6. 提供時程進度規劃，說明相關工作預定進度、完成時點 7. 加值服務說明：除本專案需求滲透測試項目外之檢測項目
3	**經費合理性** ●相關執行費用估算與分配之合理性	8. 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；並分別標示初測及複測各所需之費用**）

【附件一】

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」。

【附件二】

保　密　切　結　書

立書人：

因與　貴會進行 114 年資策會核心網站系統滲透測試服務 之合作（下稱「合作案」），就　貴會機密資訊，願負保密義務如下：

一、 本切結書所稱「機密資訊」，係指　貴會交付立書人並註明為機密或其他同義文字之有形資訊，或以口頭方式揭露且於揭露時聲明其為機密，並於嗣後以書面追認其為機密之資訊。

二、 立書人對於下列資訊，不負保密責任：
（一）立書人於簽署本切結書前已為其合法持有或知悉之資訊。
（二）立書人自無保密義務之第三人合法取得或知悉之資訊。
（三）非因立書人之故意或過失而公開或為眾所周知之資訊。
（四）立書人（包括但不限於其員工、顧問或合作廠商）未使用任何機密資訊而自行研發或發現之資訊。

三、 保密義務
（一）立書人應盡善良管理人之注意義務，保管　貴會所揭露之機密資訊。未經貴會事前書面同意，不得以任何方式直接或間接交付或洩漏機密資訊予第三人，且不得為超出合作案目的範圍利用或使用機密資訊。
（二）立書人應負責使其員工遵守本切結書之保密義務。
（三）立書人因進行合作案而有揭露機密資訊予第三人之必要時，應事前取得該第三人同意依本切結書規定保守機密資訊之書面承諾並經　貴會書面同意，立書人並就該第三人承諾負連帶履行之義務。若該第三人違反保密義務，視為立書人之違反，立書人應依本切結書第五條之規定，對　貴會負損害賠償責任。
（四）立書人依法院或主管機關之命令而須揭露機密資訊時，應於收到該命令後立即通知　貴會，並配合　貴會採取合理必要之保密措施。
（五）本條保密義務之有效期間自　貴會向立書人揭露機密資訊時起算 3 年，不受本切結書有效期間屆滿之影響。

四、 機密資訊之所有權、專利權、著作權、營業秘密或技術秘竅（KNOW-HOW）係貴會或其原授權人所有，不因　貴會揭露予立書人而生任何讓與、授權或權利設定之效力，立書人不得據以自行實施或申請專利權、著作權或其他智慧財產權，或使第三人行使上述權利。

五、 立書人如有違反本切結書之任何條款，　貴會除得隨時要求立書人返還或銷毀機

密資訊及其所有之重製物外，並得請求賠償新台幣 10 萬 元作為懲罰性違約金，如另受有損害，並得請求立書人賠償。

六、 立書人如發現第三人未經授權而違法使用機密資訊，應立即通知　貴會，並配合採取必要之排除或防止措施。

七、 本切結書自簽署日起生效，有效期間至合作案終止或完成時止。

八、 本切結書為不可撤銷、撤回或終止。

九、 因本切結書所生爭議，立書人同意以臺灣臺北地方法院為第一審管轄法院，並以中華民國法律為準據法。

此致
財團法人資訊工業策進會

立書人：
統一編號（或身份證字號）：
代表人：
職稱：
地址：

中　　華　　民　　國　　年　　月　　日

【附件三】

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：