需求說明書（含驗收規範）

壹、購案名稱

「115 年資策會資安健診委外服務」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 1,650,000 元整（含稅）。

參、需求說明

一、 本案資安健診標的單位為財團法人資訊工業策進會（以下簡稱本會）全會（12 個部門）資安健診委外服務。投標廠商應於得標後依本專案需求之規定，於 115 年 12 月 15 日前完成資安健診檢視服務，提供資安改善建議，以提升單位網路與資訊系統安全防護能力。本資安健診專案，應於履約期限內辦理啟始與結案會議。

二、 專案執行需求：

(一) 本案投標廠商應於得標次日後 7 日內與本案負責部門（請購部門）召開會議說明與討論本案執行規劃內容，並將討論結果納入工作計畫書。

(二) 本案投標廠商應於得標次日後 14 日內繳交工作計畫書一份，須完整說明專案執行項目、方式及期程規劃。

(三) 本案團隊人力至少應包含專案負責人／專案經理與資安健診服務人員。

(四) 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，須於一個月前提供書面說明，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。

(五) 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。

(六) 品質需求

1. 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。
2. 得標廠商訂定品質管理流程，本會得以稽核。
3. 得標廠商於專案期間應辦理啟始會議與結束會議，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。

(七) 業務保密安全責任

1. 得標廠商基於本案需要，所取得各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任，並簽定保密切結書。
2. 得標廠商對特別以文字標示或口頭明示為機密資料者，非經本會書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，得標廠商應負完全責任。

3. 履約期間造成保密及安全事件，得歸咎於得標廠商之責任時，得標廠商應負所有法律及賠償責任。
4. 本會對得標廠商保留實地稽核權，以確保得標廠商於委外服務期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。

三、 資安健診專業需求：

(一) 專案範圍：

本案服務範圍包括本會的網路架構檢視（以本會 7 部門為上限，依實際需求為準）、有線網路惡意活動檢視（以本會 7 部門為上限，依實際需求為準）、使用者端電腦檢視（以 330 台為上限，依實際需求為準）、伺服器主機檢視（以 60 台為上限，依實際需求為準）、安全設定檢視（防火牆檢視以 7 台為上限；目錄伺服器以 5 台為上限，依實際需求為準）、核心資通系統資料庫安全檢視（以本會 3 個核心資通系統之資料庫為為主，依實際需求為準）等資安專業服務。

(二) 專案工作項目：

資安健診服務內容應涵蓋以下所列的所有服務項目，得標廠商應具備完成各項服務所需之軟、硬體設備，專案執行期間需提供 5x8 小時之專案諮詢服務，並配合資安健診標的單位辦理說明會議。

本會資安健診分為二個部分，第一部分執行範圍應包含但不限於下述資訊安全檢測，將由本會與得標廠商經評估後確認：

第一部分、資訊安全檢測：

1. 網路架構檢視
   (1) 針對資安健診標的單位網路架構圖進行安全性弱點檢視
      - 檢視網路架構安全設計、備援機制設計、網路存取管控、網路設備管理、主機設備配置等。
      - 須詳列發現事項之風險等級、說明與改善建議，於風險說明詳述問題範圍與可能之影響，並提出具體改善建議，以利後續修補與調整。
2. 有線網路惡意活動檢視
   (1) 封包監聽與分析
      - 針對資安健診標的單位有線網路適當位置架設封包側錄設備，觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站（Command and Control，C&C）或有符合惡意網路行為的特徵。
      - 發現異常連線之電腦或設備應確認使用狀況與用途。
      - 封包側錄至少以 6 小時為原則，且應涵蓋本會上班及下班時段，以觀察是否有異常連線。
   (2) 網路設備紀錄檔分析
      - 針對資安健診標的單位檢視網路／資安設備紀錄檔（如防火牆、入侵偵測／防護系統等），分析過濾內部電腦或設備是否有對外之異常連線紀錄。
      - 發現異常連線之電腦或設備應確認使用狀況與用途。
      - 網路設備紀錄檔分析以至少 1 個月或 100M byte 內的紀錄為原則。
3. 使用者端電腦惡意活動檢視
   (1) 使用者端電腦惡意程式或檔案檢視

針對資安健診標的單位個人電腦檢視是否存在惡意程式或檔案，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

(2) 使用者端電腦更新檢視

針對資安健診標的單位個人電腦進行以下檢視：

- Microsoft Windows 作業系統更新情形。
- 應用程式之安全性更新情形（包括 Office 應用程式舉凡 Word、PowerPoint、Excel、Access 等、Adobe Acrobat、Adobe flash player 及 Java 應用程式等）。
- 檢視使用者電腦是否使用已經終止支援之作業系統或軟體（如 Windows XP、Windows 7、Windows 8.1、Windows 10、Office 2003 、Office 2007、Office 2010、Office 2016、Office 2019、Adobe Acrobat、Adobe Flash Player 及 Java 應用程式等，依使用作業系統或軟體之官網公告資訊為主），針對使用終止支援之軟體，建議停用並移除。
- 針對使用者電腦防毒軟體安裝、更新及定期完整掃描結果之處理情形。

4. 伺服器主機惡意活動檢視

(1) 伺服器主機惡意程式或檔案檢視

針對資安健診標的單位伺服器主機檢視是否存在惡意程式或檔案，檢視項目至少包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與群組。

(2) 伺服器主機更新檢視

針對資安健診標的單位伺服器主機進行以下檢視：

- 作業系統更新情形。
- 應用程式之安全性更新情形（包括 Office 應用程式舉凡 Word、PowerPoint、Excel、Access 等、Adobe Acrobat、Adobe flash player 及 Java 應用程式等，依使用作業系統或軟體之官網公告資訊為主）。
- 檢視伺服器是否使用已經終止支援之作業系統或軟體（如 Windows Server 2008 R2、Windows Server 2012、 Windows Server 2012 R2、Office 2003、Office 2007、Office 2010、Office 2016、Office 2019、Adobe Acrobat、Adobe Flash Player 及 Java 應用程式等，依使用作業系統或軟體之官網公告資訊為主），針對使用終止支援之軟體，建議停用並移除。
- 檢視伺服器是否使用不合宜之作業系統（如使用 Windows 7、Windows 8.1、Windows10 等）
- 針對伺服器主機防毒軟體安裝、更新及定期完整掃描結果之處理情形。

5. 目錄服務系統設定檢視

檢視資安健診標的單位目錄伺服器群組原則中的密碼原則與帳號鎖定原則，例如 AD 伺服器有關群組原則（Group Policy）中之「密碼原則」與「帳號鎖定原則」設定。若無 AD 伺服器，可以其他目錄伺服器（如 LDAP）或以個別使用者端電腦檢視方式完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視（使用者端電腦以項次 3 的電腦為範圍）。

6. 防火牆連線設定檢視

檢視資安健診標的單位防火牆的連線設定規則（如外網對內網、內網對外網、內網對內網）是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性（至少包含設置「Permit All／Any」與「Deny All／Any」等 2 項防火牆檢測規則確認）。

7. 核心資通系統資料庫安全檢視

檢視資安健診標的單位核心資通系統資料庫，以強化資料庫安全防護角度，依據本會內部之資安管理機制（包含文件程序及紀錄等），檢視其適法性、防護強度及落實情形，並提供專業建議，至少包含下列 7 大檢視類別、30 項檢視項目，以訪談與實機檢視方式，確認資料庫防護狀況。

(1) 特權帳號管理

i. 變更資料庫預設管理帳號

- 訪談資料庫帳號權限管理機制。
- 實機檢視資料庫帳號權限列表，確認預設管理帳號已變更。

ii. 啟用帳號鎖定次數

- 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範。
- 實機檢視資料庫特權帳號鎖定次數，確認符合機關規定。

iii. 啟用帳號鎖定時間

- 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範。
- 實機檢視資料庫特權帳號鎖定時間，確認符合機關規定。

iv. 啟用密碼複雜度原則

- 訪談資料庫角色與權限劃分機制、帳號管理及密碼設定規範。
- 實機檢視資料庫特權帳號密碼複雜度（英數字、大小寫、特殊符號）設定規則，確認符合機關規定。

v. 啟用密碼長度原則

- 實機檢視資料庫特權帳號密碼設定長度，確認符合機關規定。

vi. 啟用密碼最長有效期限原則

- 實機檢視資料庫特權帳號密碼有效期限設定天數，確認符合機關規定。

vii. 限制管理者帳號透過遠端存取

- 訪談資料庫管理者遠端連線機制。
- 檢視資料庫遠端連線設定、連線授權紀錄，避免資料庫管理者從非管理網段進行管理作業。

(2) 資料加密

i. 資料庫資料具有適當保護機制（包含加密、不可識別處理）

- 訪談資料庫資料保護機制（如加密方式、保護資料範圍、不可識別處理之方式等）。
- 實機檢視資料庫資料之加密設定、加密結果、不可識別處理之結果。

ii. 資料庫資料具有安全傳輸機制

- 訪談資料庫傳輸保護機制。
- 實機檢視資料庫資料傳輸加密方式與設定狀況，避免採用不安全的資料傳輸方式。

iii. 資料庫加密金鑰具有適當保護機制

- 訪談資料庫加密金鑰管理機制（如使用狀況、保管情形等）。
- 檢視資料庫金鑰存取相關申請、審核紀錄及金鑰管理方式，避免遭非授權人員存取。

(3) 存取授權

i. 限制資料庫主機服務埠

- 訪談資料庫主機連線對象、連線目的及使用之服務埠。
- 實機檢視資料庫主機僅開啟允許之服務埠。

ii. 限制遠端存取來源

- 訪談資料庫遠端存取控管機制。
- 檢視資料庫遠端存取來源、連線授權紀錄，避免遭非授權來源 IP 進行連線。

iii. 限制遠端存取帳號

- 檢視資料庫遠端存取帳號與授權紀錄，避免遭非授權帳號進行遠端存取。

iv. 限制遠端存取操作

- 檢視資料庫遠端存取權限與授權紀錄，避免執行非授權之操作行為。

v. 資料庫帳號權限最小原則

- 訪談資料庫身分識別、存取管理及權限劃分機制。
- 檢視資料庫權限相關申請、審核紀錄，並實機檢視資料庫帳號權限遵循最小化原則。

(4) 稽核紀錄

i. 啟用資料庫帳號變更稽核

- 訪談資料庫稽核紀錄留存項目、保存期間及管理機制。
- 實機檢視資料庫帳號異動稽核紀錄設定結果、留存內容及管理方式。

ii. 啟用資料庫帳號登出／登入稽核

- 實機檢視資料庫帳號登入／登出稽核紀錄設定結果、留存內容及管理方式。

iii. 啟用資料庫結構變更稽核

- 實機檢視資料庫結構異動稽核紀錄設定結果、留存內容及管理方式。

iv. 稽核紀錄管理方式

- 檢視資料庫稽核紀錄之存取控制與保存紀錄

v. 資料庫主機時間校時

- 訪談資料庫主機校時管理機制。
- 實機檢視資料庫主機校時方式、來源及時間正確性。

vi. 稽核紀錄分析

- 訪談資料庫稽核紀錄分析機制及異常紀錄處理方式。
- 檢視資料庫稽核紀錄分析規則設定、分析紀錄或報告，以及針對異常事件處理方式。

(5) 委外管理

i. 委外廠商外部連線方式

- 訪談資料庫委外廠商連線存取控管機制。
- 檢視資料庫委外廠商外部連線方式設定、授權紀錄及相關防護機制。

ii. 委外廠商資料存取方式

- 檢視資料庫委外廠商資料存取方式、授權紀錄及相關防護機制。

iii. 委外廠商帳號授權方式

- 訪談資料庫委外廠商帳號權限管理機制。

- 檢視資料庫委外廠商帳號權限設定、授權紀錄，確認帳號權限之適當性。

(6) 備份保護

i. 資料庫定期執行備份
- 訪談資料庫備份管理機制。
- 檢視資料庫備份方式（如備份時間、週期、代數及方式等）與備份結果。

ii. 資料庫備份具有適當保護機制
- 訪談資料庫備份檔案之保護機制。
- 檢視資料庫備份之存取控制與保護方式（包含異地儲存、內容加密、不可識別之處理等）。

iii. 資料庫備份回復測試
- 訪談資料庫備份回復測試執行方式。
- 檢視資料庫備份回復測試演練執行結果與紀錄，確認演練之有效性。

(7) 弱點管理

i. 資料庫主機定期弱點掃描
- 訪談資料庫主機弱點掃描執行方式與頻率。
- 檢視資料庫主機弱點掃描紀錄。

ii. 資料庫主機弱點修補
- 訪談資料庫主機弱點修補與追蹤機制。
- 檢視資料庫主機弱點修補紀錄、相關審核紀錄及複測報告。

iii. 修補資料庫主機安全性更新項目
- 訪談資料庫與主機作業系統之安全性更新執行方式及頻率。
- 實機檢視資料庫與主機作業系統之安全性更新歷程紀錄，確認是否已落實執行更新機制。

第二部分、DNS 安全檢測：

針對指定 DNS 伺服器進行安全檢測，以確認 DNS 服務設定是否存在資訊洩漏、未授權存取、弱化配置或可被濫用等風險。檢測範圍至少應包含下列項目：

1. DNS 伺服器軟體版本與已知弱點檢查

檢測目的與風險：為避免 DNS 伺服器因採用過舊或已停止維護（End of Life）之軟體版本，存在可被遠端利用之已知弱點（如遠端程式碼執行、服務阻斷、快取毒化等），或因對外揭露版本資訊而便於攻擊者針對特定版本發動攻擊。

廠商應執行檢測內容：廠商需識別指定 DNS 伺服器所使用之軟體種類(如 ISC BIND、Microsoft DNS、Unbound、NSD、PowerDNS、Knot 等）及其版本，並比對 CVE／NVD 等公開弱點資料庫，確認是否存在已知弱點、修補程式套用情形，以及是否屬已終止維護之版本；檢測內容應包含但不限於版本識別、已知漏洞（CVE）對應、修補等級（Patch Level）確認，及各弱點對本機關之潛在影響評估。

2. 內外部 DNS 分離架構之合理性

檢測目的與風險：為避免因內部與對外 DNS 未妥適分離，導致內部主機名稱、內部 IP 位址規劃、網路區段或關鍵系統命名等敏感資訊透過對外 DNS 遭揭露，或使對外 DNS 得以解析僅供內部使用之紀錄，增加組織內部網路遭偵查之風險。

廠商應執行檢測內容：廠商需檢視指定網域之 DNS 架構是否採行內外分離（Split-horizon／Split-brain）設計，確認對外權威 DNS 是否僅提供對外

公開服務所需之紀錄、對外 DNS 是否可解析內部專用之名稱或位址，以及遞迴解析服務是否僅限內部來源使用；檢測內容應包含但不限於對外 DNS 所暴露紀錄之合理性檢視、內部名稱／位址外洩情形檢查，及內外 DNS 職責與存取範圍劃分之妥適性評估。

3. 子網域枚舉與資產清查（含過期或懸置紀錄（Dangling DNS）所致之子網域接管風險）

   檢測目的與風險：為避免組織存在未納入管理、未定期維護、未對外公開或已被遺忘之子網域資產，使測試環境、開發環境、暫存環境或其他邊界服務成為攻擊者入侵企業內部網路之入口點；並避免子網域指向已失效或未回收之外部服務（如雲端主機、CDN、物件儲存、SaaS 服務等），形成懸置紀錄（Dangling DNS）而遭第三方接管（Subdomain Takeover）。

   廠商應執行檢測內容：廠商需針對指定網域執行子網域枚舉與資產清查，檢測方式應包含但不限於公開資訊蒐集（如憑證透明度紀錄、被動式 DNS、搜尋引擎及網路空間搜尋）、字典比對及暴力破解等，以識別正式、測試、開發、暫存環境及其他相關網域資產；並就所發現之子網域逐一確認其解析目標之存活狀態與歸屬，判定是否存在因指向失效服務而可被接管之子網域接管風險。

4. 區域傳輸安全性檢測（Zone Transfer／AXFR）

   檢測目的與風險：為避免 DNS 伺服器因區域傳輸設定不當，允許未授權來源取得完整 DNS 區域資料，致使網域紀錄、伺服器名稱、IP 位址及服務對應關係遭一次性導出，供攻擊者據以推測組織網路拓撲及關鍵系統位置。

   廠商應執行檢測內容：廠商需針對指定 DNS 伺服器（含主要及所有備援名稱伺服器）測試是否允許來自未授權來源之完整區域傳輸（AXFR）及增量區域傳輸（IXFR），確認區域傳輸是否已限制於指定之次要伺服器並具備適當之來源存取控制；檢測內容應包含但不限於各名稱伺服器之 AXFR／IXFR 回應測試，及成功取得之區域資料範圍與敏感程度評估。

5. DNS 服務配置與遞迴查詢稽核（含 DNS 放大攻擊防護與回應速率限制（RRL）設定）

   檢測目的與風險：為避免 DNS 伺服器因配置不當導致敏感資訊遭揭露，或因遞迴查詢功能對外開放而淪為開放解析器（Open Resolver），遭濫用於 DNS 放大攻擊（DNS Amplification）、反射式阻斷服務攻擊（DRDoS）或其他惡意流量轉發行為。

   廠商應執行檢測內容：廠商需針對指定 DNS 伺服器執行服務配置與遞迴查詢稽核，檢測內容應包含但不限於版本資訊揭露檢查（如 version.bind 查詢）、Banner 資訊檢查、DNS 指紋辨識（Fingerprinting）、遞迴查詢功能是否對外開放（Open Resolver 檢測），以及是否已針對放大攻擊風險部署回應速率限制（Response Rate Limiting,RRL）或等效防護機制、其設定值是否合理有效。

6. DNS 快取毒化防護機制（含來源連接埠與交易識別碼隨機化）

   檢測目的與風險：為避免 DNS 伺服器因欠缺足夠之隨機化機制，使攻擊者得以猜測查詢參數並偽造回應，將惡意或錯誤之 DNS 紀錄植入快取（DNS Cache Poisoning，如 Kaminsky 類型攻擊），進而將使用者導向偽冒網站或攔截其連線流量。

   廠商應執行檢測內容：廠商需針對指定 DNS 伺服器（具遞迴解析功能者）檢視其快取毒化防護機制之部署與有效性，檢測內容應包含但不限於查詢來源連接埠隨機化（Source Port Randomization）及交易識別碼

（Transaction ID）隨機化之亂度是否充足、是否啟用查詢名稱大小寫隨機化（DNS 0x20 Encoding）等強化機制，以及是否部署 DNSSEC 驗證以確保應答完整性；並據以評估該伺服器對快取毒化攻擊之抵抗能力。

如需以自動化程式檢測，應事先與本會協調檢測時段，過程不得影響線上服務正常運作。檢測報告應逐項說明檢測方法、發現之弱點、風險等級（高、中、低）及可能影響，並針對每一項弱點提供具體可執行之改善建議，如：建議調整之組態設定參數、應更新之軟體版本或架構調整方案及改善優先順序等。本部分檢測應辦理啟始與結案會議，向本會說明檢測結果與建議改善方向。

(三) 廠商須自備執行本案所需之相關軟、硬體設備。若資安健診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，其損害概由乙方承擔。

四、 資安健診服務水準協定（SLA）：

服務水準規範

本案各項服務水準協定（Service Level Agreement，SLA），以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險，詳細服務水準規範如下表：

項次	項目	交付內容
1	網路架構檢視	檢視內容需包含網路架構部署表現（網路架構設計、備援機制設計、主機設備配置）、網路存取管控（防火牆管理、存取控制）及網路設備管理（登入認證機制、安全性更新）
2	封包監聽與分析	1. 在有線網路適當位置架設側錄設備，進行封包側錄至少以6小時為原則，且應涵蓋本會上班及下班時段，以觀察是否有異常連線 2. 封包側錄檔案的可用性達100%
3	網路設備紀錄檔分析	網路設備紀錄檔分析以至少1個月或100 Mbyte內的紀錄為原則
4	使用者端電腦惡意程式或檔案檢視	1. 惡意程式檢測檔案須提供安全性無虞之檢測證明 2. 惡意程式檢測時，因可歸咎於得標廠商之情形，致使用者電腦故障之比率需小於1% 3. 因惡意程式檢測所造成的使用者電腦故障，應於通報後8小時內協助修復完成
5	使用者電腦更新檢視	更新狀態需追蹤至實地檢測前1個工作日
6	伺服器主機惡意程式或檔案檢視	1. 惡意程式檢測檔案須提供安全性無虞之檢測證明 2. 惡意程式檢測時，因可歸咎於得標廠商之情形，致伺服器故障或服務中斷之比率為1% 3. 因惡意程式檢測所造成的伺服器主機故障或服務中斷，應於通報後8小時內協助修復完成
7	伺服器主機更新檢視	更新狀態需追蹤至實地檢測前1個工作日
8	目錄服務系統設定檢視	1. 目錄服務系統設定檢視時，因可歸咎於得標廠商之情形，致伺服器故障或服務中斷之比率為0% 2. 因目錄服務系統設定檢視所造成的系統故障，應於通報後8小時內協助修復完成

9	防火牆連線設定	防火牆開啟通訊埠檢視範圍需涵蓋0~65535
10	核心資通系統資料庫安全檢視	1. 檢視範圍應完整涵蓋「特權帳號管理、資料加密、存取授權、稽核紀錄、委外管理、備份保護、弱點管理」等7大類別共30指標 2. 執行訪談與實機檢視（含資料庫帳號權限、加密設定及日誌檢視等）作業時，不可對資料庫主機及服務造成影響 3. 檢視過程嚴禁異動資料庫內之資料及結構

五、 教育訓練

■無

六、 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)。

七、 保固需求

■有，本案自驗收合格之日起 6 個月保固期間內，若本會因弱點修補有複測需求時，得標廠商應協助複測，次數以 1 次為上限。

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	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。	1 份	紙本	決標次日起 7 日曆天
2	專案啟動文件	第一部分資訊安全檢測及第二部分 DNS 安全檢測專案啟動會議簡報（含完整專案執行規劃、期程）	2 份	電子檔	決標次日起 7 日曆天
3		1. 委外廠商資通安全管理措施說明表 2. 工作計畫書： (1)內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、工作項目、執行程序(網路／個人電腦／伺服器／防火牆／資料庫)、時程說明（包括起始會議與結束會議)、受測單位檢測範圍與影響、受檢測單位準備事項、工作進度稽核點及品質管理流程。 3. 「受檢測單位準備事項」建議包括：受測個人電腦清單(IP)、受測伺服器清單(IP、	各 1 份	電子檔	決標次日起 14 日曆天

		用途)、網路架構圖(標示部署設備位址)、網路設備紀錄檔、核心資通系統資料庫安全檢視配合事項等。			
4	資安健診服務報告	文件內容應包括：執行結果摘要說明(依照檢測類別各別摘要說明)、執行計畫(執行期間／執行項目／執行範圍／專案成員)、執行情形(需包含所有服務項目執行結果，不可直接以工具產生之原始結果交付)、改善建議、結論。	1 份	電子檔	依工作計畫書載明之交付時程
5	專案執行記錄檔	文件內容應包括：各個人電腦的資安檢測結果表、各伺服器主機的資安檢測結果表、網路側錄封包資料、發現惡意行為或惡意程式的過程紀錄(如果有發現)、外洩資料列表(如果有發現)、惡意程式(如果有發現)、核心資通系統資料庫安全檢視 30 項結果表(應詳細記錄每項檢測項目之檢視情形，除「符合、部分符合、不符合、不適用」勾選外，更要確實記錄每項檢視項目之機關現況與改善／建議事項，各項資料庫安全檢視結果判定原則)。	1 份	電子檔	同本案履約期限
6	DNS 安全檢測	DNS 檢測分析報告，文件內容應包含：檢測目標與範圍、檢測方法與工具說明、發現之風險項目與影響說明、風險等級評估、佐證資料(例如：截圖、查詢結果、封包或紀錄)、改善建議(須包含可執行內容)等。	1 份	電子檔	同本案履約期限
7	專案結案文件	第一部分資訊安全檢測及第二部分 DNS 安全檢測專案結案會議簡報(含完整專案總結)	2 份	電子檔	同本案履約期限
8	資安文件	資料返還、刪除、銷毀聲明書(詳附件) ※有保固者於保固期滿時交付。	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：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、廠商特定資格

一、 廠商特定資格

為確保資訊安全及得標廠商所提供的服務水準，投標廠商應符合下列條件：

(一)曾經服務過本會「資安健診」專案或經國家資通安全研究院資安服務廠商評鑑 114 年度「資安健診」B 級以上之廠商（國家資通安全研究院資安服務廠商評鑑可至 https://www.nics.nat.gov.tw/core_business/information_security_information_sharing/Cybersecurity_Service_Provider_Evaluation/查詢）。

(二)曾承接總人數達 600 人以上組織之資安健診服務實績證明（承接組織總人數請提供公開資訊如 104、1111 人力網資料；實績證明檢附如合約、決標證明、驗收證明等）。

(三)投標廠商須實施資訊安全管理制度，提供通過 ISO 27001：2022 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，須於屆期_1_週前提供有效之證明留存本會備查。

二、 本案執行人員資格：

1.資安健診服務執行人員資格（專案工作項目第一部分資訊安全檢測之 1~6 項），每位專案人員依各服務項目應具備專業證照如下：

(一) 網路架構檢視、防火牆連線設定檢視（第 1、6 項）：需持有下列 1 張以上證照。

1. CCNA（Cisco Certified Network Associate）
2. CCNP Security（Cisco Certified Network Professional Security）
3. CND（EC-Council Certified Network Defender）
4. CompTIA Network+
5. iPAS 資訊安全工程師中級能力鑑定
6. 其他網路安全相關專業證照（參考資安署公告之資通安全專業證照清單，需經本會認可）

(二) 網路（有線）、使用者端電腦、伺服器主機等惡意活動檢視（第 2、3、4 項）：需持有下列 1 張以上證照。

1. CEH（EC-Council Certified Ethical Hacker）
2. CHFI（EC-Council Computer Hacking Forensic Investigator）
3. CND（EC-Council Certified Network Defender）
4. NSPA（Network Security Packet Analysis）
5. SSCP（ISC2 System Security Certified Practitioner）
6. CompTIA Security+
7. 其他網路安全相關專業證照(參考資安署公告之資通安全專業證照清單，需經本會認可)。

(三) 目錄服務系統設定檢視（第 5 項）：需持有下列 1 張以上證照。

1. Microsoft Certified: Azure Administrator Associate

2. Microsoft Certified: Azure Security Engineer Associate
3. CompTIA Security+
4. SSCP（ISC2 System Security Certified Practitioner）
5. iPAS 資訊安全工程師中級能力鑑定
6. 其他系統安全相關專業證照(參考資安署公告之資通安全專業證照清單，需經本會認可)。

2.資料庫安全檢視（第 7 項)：每位專案人員需持有下列 1 張以上證照，且團隊中須持有資料庫管理及資通安全技術／管理證照各 1 張以上。

(一) 資料庫管理：

1. Microsoft Certified: Azure Database Administrator Associate
2. Oracle Database Administration 2019 Certified Professional
3. Oracle Certified Professional Oracle Database Security Expert
4. IBM Certified Database Administrator
5. Oracle Certified Professional, MySQL 8.0 Database Administrator
6. 其他資料庫相關專業證照(參考資安署公告之資通安全專業證照清單，需經本會認可）

(二) 資通安全技術／管理：

1. CISSP（ISC2 Certified Information Systems Security Professional）
2. ISO／CNS 27001 Lead Auditor
3. 其他資安技術／管理相關專業證照（參考資安署公告之資通安全專業證照清單，需經本會認可）

(三) 提供上述人員之專業證照／訓練證書；如專業證照／訓練證書之效期於履約期間內屆期，須於屆期_1_週前提供有效之專業證照／訓練證書留存本會備查。

(四) 專案人員須年滿 18 歲以上，具有中華民國國籍，不得為外籍勞工或大陸來臺人士，於履約期間不得同時於大陸地區工作。

(五) 提供上述人員之在職證明勞保文件（二擇一）

1. 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。
2. 各被保險人投保資料明細（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)。

柒、其他注意事項

一、 購案聯絡人：

姓　名：資安科技研究所　朱雅璿小姐
電　話：(02）6607-6330
Email：clairechu@iii.org.tw
地　址：105 台北市民生東路四段 133 號 14 樓

二、 發票資料：

抬　頭：財團法人資訊工業策進會
統一編號：05076416

【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】

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：