財團法人公共電視文化事業基金會

資安監控及檢測服務案

徵求文件(RFP)

中華民國 110 年10月

第一章 專案概述

第一節 專案名稱及緣起

一、為強化資通安全防護能量，爰辦理「資安監控及檢測服務案」(下稱本專案)。

二、依據

本專案係依據資通安全管理法及其子法辦理，「資通安全責任等級分級辦法」中規範資通安全責任等級A級之特定非公務機關，應建立資通安全威脅偵測管理機制，並依據「資通安全事件通報及應變辦法」處理資通安全事件。

三、專案背景

依據本會資訊安全之防護需求，期透過本案計畫整合各項資訊安全防護機制，委由具整合能力之專業資安廠商，提出完整之資安防護與管理方案，以專業資安駐點人員，將資安防護效能達最佳化。為達到整體監控、整體分析之目標，部署端點偵測及應變機制(EDR)，並協助本會進行資通安全健診、弱點掃描、滲透測試服務等，以強化資通安全防護效能。

第二節 專案目標

一、強化資訊安全監控效能

依據本會資訊安全之防護需求，須設置SOC（Security Operation Center）監控防護措施。除SOC進行監控防護，亦須強化橫向及縱深資安防禦能量，期透過本案計畫整合各項資訊安全防護機制，委由具整合能力之專業資安廠商，提出完整之資安防護與管理方案，將資安防護效能達最佳化。

二、符合資通安全責任等級分級辦法規範，進行資通安全健診、弱點掃描、滲透測試等安全性檢測作業。

三、部署端點偵測及應變機制(EDR)平台

四、協助本會資安設備維運服務，提供資安專業人員派駐服務

第三節 專案範圍

一、SOC 監控範圍之整體處理效能需提供 3,000 EPS(Event Per Second)，EPS 以 PEAK 或 MAX 值計算。

二、資安健診範圍：

（一）網路架構檢視：一式

（二）網路惡意活動檢視-封包監聽與分析：2 台側錄設備

（三）網路惡意活動檢視(有線)_資安設備紀錄檔分析：10 台資安設備

（四）使用者電腦及伺服器主機共：1,000 台

（五）目錄伺服器：10 台

檢測頻率：每年檢測一次

三、弱點掃描範圍：

伺服器主機及使用者電腦共 1,000 台

網站：10URL

檢測頻率：每年執行 2 次，含初測與複測

四、滲透測試範圍：

10IP 或 URL

檢測頻率：每年檢測一次

五、人員派駐服務：

協助本會資安設備維運服務，專案期間內提供本會 1 名資安駐點人員

六、端點偵測及應變機制：

每年提供伺服器主機及使用者電腦授權共 1,000 台

第四節 專案期程及付款方式

一、專案時程

(一)本專案時程自專案工作計畫書驗收通過後開始執行服務起兩年，共計24個

月。

二、付款方式

本專案採分段驗收、分段付款：

(一) 第 1 期(自專案工作計畫書驗收通過後開始執行服務起6個月)：契約總金額25%。

a. 簽約日起 30 天內：提供專案工作計畫書

1. 內容資訊：各服務執行期間/執行項目/執行範圍/專案人員(資安證照資訊)。

2. 執行規劃：包含各項工作執行規劃：

(1) 監控設備部署規劃、監控、及警示作業之方式、通知本會資安聯絡人之時機、內容及方式、資安事件處理之作業、資安威脅預警之作業等。

(2) 資安健診規劃

(3) 弱點掃描規劃

(4) 滲透測試規劃

(5) 駐點人員安排

(6) 端點偵測及應變機制部署規劃

3. 各項報告(月報、季報、年報)提交時間及內容。

(1) 簽約日起次月，每月 10 日前：提供資安監控服務月報

(a) 資安監控分析

(b) 資安事件處理

(c) 資安威脅預警

(d) 總結。

(e) 駐點人員出勤狀況(出勤簽到簿)

(2) 每年 9 月 30 日：提供健診報告及滲透測試報告。

(3)每年 3 月 30 日及 9 月 30 日：提供弱點掃描報告。

b.簽約日起 30 天內提供 1,000 台端點偵測及應變機制(EDR)軟體授權，使用期間為 2 年。

c.完成本案交付項目專案工作計畫書、資安監控月報、弱點掃描服務報告及服務授權、端點偵測及應變機制(EDR)軟體授權並交付文件，通過第1期書面審查後，給付25%契約價金額。

(二) 第 2 期(自專案工作計畫書驗收通過後開始執行服務起6個月至12個月)：契約總金額25%。

完成本案「第四章、第二節 驗收及交付項目」之交付項目資安監控月報、資安健診服務報告、弱點掃描服務報告及服務授權、滲透測試服務報告及服務授權並交付文件，完成第2期書面審查通過後，給付25%契約價金額。

(三) 第 3 期(自專案工作計畫書驗收通過後開始執行服務起12個月至18個月)：契約總金額25%。

完成本案「第四章、第二節 驗收及交付項目」之交付項目資安監控月報、弱點掃描服務報告並交付文件，完成第3期書面審查通過後，給付25%契約價金額。

(四) 第 4 期(自專案工作計畫書驗收通過後開始執行服務起18個月至24個月)：契約總金額25%。

完成本案「第四章、第二節 驗收及交付項目」之交付項目資安監控月報、資安健診服務報告、弱點掃描服務報告及服務授權、滲透測試服務報告及服務授權並交付文件，完成第4期書面審查通過後，給付25%契約價金額。

第二章 專案需求

本專案主要需求為資安監控，其工作包含資安監控服務、資安威脅預警。廠商應依據資通安全責任等級分級辦法規定，依照本會需求，執行資通安全健診、弱點掃描、滲透測試、人員派駐服務及部署端點偵測及應變服務。

為確保本會的資訊安全及廠商所提供的服務水準，廠商具有之資訊安全監控中心（SOC）應符合下列條件，並於服務計畫書專章詳述並附相關佐證資料：

1. 在國內有實際運作之資訊安全監控中心（SOC）機房，提供專職人員輪值，以每日 24 小時全年無休之即時監控方式，協助管理相關主機與系統環境。
2. 廠商之資訊安全監控中心（SOC）符合國內或國際資訊安全標準（如 CNS27001 或 ISO27001 等）及個人資訊安全管理(如 BS 10012 或 ISO／IEC 27701 等)安全稽核認證（認證範圍應標示涵蓋 SOC）及必要之複驗（以確保認證之有效性），以確保廠商自身安全無虞。
3. 廠商需設置或與通過 ISO 17025 稽核認證數位鑑識中心實驗室合作。
4. 資訊安全監控中心（SOC）應須具有全負載長時間運轉發電機及 UPS 不斷電設備，以防止因跳電而產生服務中斷情形。
5. 資訊安全監控中心（SOC）應具有多層次安全門禁系統與全程監控的保全系統，以確保監控中心之實體安全。
6. 資訊安全監控中心（SOC）連接二家以上不同的國內 ISP 公司，提供備援服務，以防範意外狀況發生而導致監控服務中斷。
7. 資訊安全監控中心應擁有固定 IP，確保本會不會因為 ISP 之轉換而更改原有之設定。
8. 監控中心透過網際網路遠端監控，網路連線通道應有加密與防火牆管制，以確保本會安全。
9. 廠商之 SOC 監控平台，需提供可對外服務之合法證明文件（如 MSSP 合約或者原廠授權可以對外服務等證明文件或符合共同供應契約合格 SOC 服務廠商）。

10. 廠商須通過行政院國家資通安全會報技術服務中心聯防監控廠商連通測試，網址：https://www.nccst.nat.gov.tw/GSOC#tabs-2。

11. 本案相關服務不得轉包。

第一節 資安監控服務需求

一、資訊安全監控服務處理效能

SOC 監控範圍之整體處理效能總達 3,000 EPS(Event Per Second)，EPS 以 PEAK 或 MAX 值計算。資通安全威脅偵測管理(SOC)服務

（一） 資訊安全監控服務內容

1. 提供每週 7 x 24 全天候即時遠端資安事件監控服務。
2. 由廠商提供本會資訊安全監控軟硬體設備，所蒐集資安事件（故）透過資訊安全監控中心（SOC）綜合分析篩選出可疑網路活動，且需由全年無休專業人員即時遠端監控，偵測入侵攻擊行為。
3. 為發揮有效之資訊安全事件偵測能力，資訊安全監控中心（SOC）應根據所監控設備之紀錄，偵測有安全風險的行為。
4. 資訊安全監控中心人員在發現並確認為資安事故時，必須依事故管理流程進行通報與應變：
   (1) 依威脅性至少區分資安事故為低、中、高等三個風險等級(不限三個等級)。
   (2) 於資安事故發生 60 分鐘內依據本會需求採電話、傳真、手機簡訊、電子郵件等方式，通報本會資訊安全緊急聯絡人員，並立即協助事故的後續處理作業。
   (3) 通報內容至少應包含事故發生時間、風險等級、攻擊方法、路徑分析及事件內容描述，以及相對應緊急應變措施建議及損害控管措施，並協助提供修訂調整路由器、防火牆、入侵偵測系統的規則及存取清單，並避免網路安全監控範圍外的漏洞。

5. 資安事故分析追蹤

(1) 於資訊安全事故獲得控制後，廠商應協助追蹤調查事故來源與經過，適時蒐證與保存相關證據，並於事故排除後 5 天內提供書面報告，其內容應包含事故發生時間、來源與目標 IP、駭客所在位置、攻擊方法與路徑分析、損害控管與影響分析、處置情形以及一個月內提出改善建議報告。

(2) 分析追蹤過程中，發現須提升風險等級時，應依事故升級處理之機制，迅速回應處理。

(3) 提供資安事故發生後評估分析機制，包含事故類型歸納、投入處理成本量化及應使用增強或額外控制措施。

6. 每月月報應交付上個月之資訊安全事件（故）統計及入侵事件（故）分析等中文化報表彙整後編製「資安監控服務報告」予本會。

7. 安全紀錄傳輸過程須透過加密方式傳送。

8. 得標廠商應主動將最新資安訊息透過資安技術通告，同時迅速利用電話、簡訊、電子郵件或傳真等方式，提供本會預警與通報之服務，內容至少包括：

(1) 資訊安全威脅類型、說明、可能造成之影響。

(2) 各大原廠發布的最新修正檔。

(3) 微軟更新。

(4) 新發現資訊安全漏洞與補救措施。

(5) 資訊安全事故紀錄與報導。

(6) 客製化資安訊息。

9. 警訊通報以中文為主。

（二） SOC 監控環境部署

1. 廠商應於簽約日起算 30 個日曆天內，勘查機關現有網路環境與設備需求，廠商應與本會確認監控範圍已納入 SOC 監控範圍之相關設備與紀

錄，經溝通後仍未納入監控範圍者，應於工作計畫書說明資安風險，以盡告知之義務，並完成部署監控必要之事件收集器，所部署之設備不得影響現有各項安全設備之正常運作。部署工作應包含事件收集器安裝、網段部署、設定、系統調校與重要資安事件 Rule 導入等工作。

2. Event 數量計算以事件收集器所收集的數量為基準；廠商應每季檢視受監控設備之 EPS 情形，檢視監控部署執行情形，適時提出部署調整建議。

（三） 資安監控標的

本專案為強化及整合網路安全防護機制，其範圍包括強化本會重要資訊設備等，至少包含以下項目：防火牆、入侵偵測及防禦系統、防毒、防駭系統、重要伺服主機、端點偵測及回應等系統。

（四） 資安事件處理

1. 若發生資安事件，本會可向廠商提出事件處理服務需求，並於一個月內提出改善建議報告。處理件數時間合計共 40 小時，若請求件數超過處理件數額度，本會可請廠商提出服務費用報價或於下單前約定超出之資安事件處理(鑑識)處理費用。

2. 資安事件處理工作範圍

(1) 廠商必須進行受駭根因分析與影響範圍之確認，並協助本會將造成資安事件的漏洞關閉，以避免進一步擴散。

(2) 檢測疑似被入侵之主機系統，針對系統資訊、日誌檔及惡意程式進行資料蒐集，日誌檢視以 1 年為原則(含線上與離線日誌)。

(3) 應針對蒐集的資料進行資料保存、磁碟映像檔分析、惡意程式分析及網路流量分析。以動態或靜態方法分析惡意程式功能，了解駭客入侵之主要目的。

(4) 將磁碟映像檔、惡意程式及網路封包等分析結果加以彙整進行關聯分析，以研判駭客入侵手法、入侵時間、影響範圍及威脅程度等。

（五） 資安威脅預警

(1) 資安威脅預警服務範圍為廠商發現及蒐集國內外資安組織之資安威脅情資，至少包含：

A. 資安聯防情資：惡意中繼站清單、高危險惡意特徵情資及其他情資通報。

B. 病毒資訊警訊：如趨勢科技、Symantec 等防毒廠商中級以上病毒警訊。

C. 系統弱點公告：如 NCCST、Microsoft、Security Focus、各國 CERT(如 CISA(USCERT))及 MITRE 等國內外資安組織公告。

D. 網頁攻擊資訊：如 Zone-H、OWASP 資安組織公告等。

E. 新聞事件：如 CNN、Google 及 Yahoo 等資安新聞。

F. 廠商發現之威脅：如 Zero-Day 事件。

(2) 國內外資安威脅發表後 3 個工作日，整理相關訊息通知機關，內容包含資通安全威脅類型、說明、可能造成之影響、各大原廠發布的最新修正檔、新發現資通安全漏洞與補救措施、資通安全事件報導、漏洞分析、修補方式或對策。

(3) 資安威脅預警通報後 2 個工作日，廠商通知機關監控服務範圍設置防禦措施，並提供資安威脅預警處理紀錄予機關。預警處理包含：

A. 提供防火牆、IPS/IDS 等偵測規則諮詢。

B. 提供如中繼站清單、高危險惡意特徵之阻擋與規則更新資訊等。

C. 提醒更新系統安全或防毒軟體修正檔，或漏洞修補等。

第二節 資通安全健診服務需求

本專案執行期間應依本專案規劃範圍，協助本會依據「資通安全責任等級分級辦法」應辦事項中資通安全健診要求之內容與頻率，進行本會營運範圍之資通安全健診。廠商應自行準備完成下列項目所需之軟、硬體設備，本需求執行期間須提供諮詢服務，並配合辦理說明會議。資通安全健診項目規劃檢測設備數量如下。

- 使用者端電腦及伺服器主機共1,000台
- 目錄伺服器：10台
- 資安設備：10台

一、資通安全健診範圍

資通安全健診，每年執行1次，執行時間由本會指定，執行前30日通知廠商，執行範圍為本會營運範圍。

二、資通安全健診內容

(一)網路架構檢視

針對本會網路架構圖進行安全性弱點檢視，檢視項目須包含設計邏輯是否合宜、網路架構部署表現(網路架構設計、電腦設備配置、備援機制)、網路邊界安全管理(防火牆管理、存取控制)及網路設備安全表現(登入認證機制、安全性更新)、主機設備配置等，應詳列發現事項之風險等級、風險說明與改善建議，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，以利本會後續修補與調整。

(二)網路惡意活動檢視

1.封包監聽與分析

(1)觀察內部個人電腦及主機伺服器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主機伺服器應確認使用狀況與用途。

(2)在有線網路適當位置架設側錄設備，進行封包側錄至少 6 小時，觀察是否有異常連線。

2.網路設備紀錄檔分析

(1)檢視網路與資安防護設備(如防火牆、入侵偵測系統/入侵防護系統等)紀錄檔，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需確認使用狀況與用途。

(2)網路設備紀錄檔分析以 1 個月或 100Mbyte 內的紀錄為原則。

(三)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

檢視個人電腦是否存在惡意程式或檔案，檢視項目包含活動中與潛藏的惡意程式、駭客工具程式及異常帳號與群組。

2. 使用者電腦更新檢視

對個人電腦作業系統安全性更新、微軟(Microsoft)應用程式(含Office)安全性更新，與 Adobe Acrobat、Adobe Flash Player及 Java 應用程式更新檢視(包含檢視使用者電腦是否使用已經停止支援之作業系統或軟體，如 Windows XP 或 Office 2003)，對使用者電腦防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。更新狀態需追蹤至實地檢測前 1 個工作日。

3. 使用者電腦組態設定檢視

對個人電腦進行電腦組態設定檢視，依行政院國家資通安全會報技術服務中心官方網站「政府組態基準」專區公布的安全性檢視內容為主，確認電腦組態設定之落實情形。使用者電腦組態設定如有例外管理情形，應以文件記錄例外管理的組態項目。

(四)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

檢視伺服器主機是否存在惡意程式或檔案，檢視項目包含活動中與潛藏的惡意程式、駭客工具程式及異常帳號與群組。

2. 伺服器主機更新檢視

對伺服器主機進行作業系統安全性更新檢視、安裝的微軟(Microsoft)應用程式(含 Office)安全性更新檢視，與 Adobe Acrobat、Adobe Flash Player 及 Java 應用程式更新檢視(包含檢視伺服器主機是否使用已經停止支援之作業系統或軟體，如 Windows XP、Windows Server 2003 或 Office 2003)，針對伺服器主機防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。更新狀態需追蹤至實地檢測前 1 個工作日。

3. 伺服器主機組態設定檢視

對伺服器主機進行電腦組態設定檢視，依行政院國家資通安全會報技術服務中心官方網站「政府組態基準」專區公布的安全性檢視內容為主，確認電腦組態設定之落實情形。使用者電腦組態設定如有例外管理情形，應以文件記錄例外管理的組態項目。

應於本案工作說明書中規劃資通安全健診期程及工作計畫，工作計畫內容須包含：工作項目、執行程序(網路/個人電腦/伺服器主機)、時程說明、檢測範圍與影響、本會須準備事項。本會須準備事項建議包括：受測個人電腦清單(IP、安裝的作業系統與應用程式)、受測伺服器清單(IP、用途、安裝的作業系統與應用程式、管理人員)、網路架構圖(標示部署設備位址)、網路設備紀錄檔、協同檢測人員名單。

於資通安全健診結束後 30 日內應提交資通安全健診服務報告，報告內容應包含：執行結果摘要說明(依照檢測類別個別摘要說明)、執行計畫(執行期間/執行項目/執行範圍/專案成員)、執行情形(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。另須於資通安全健診服務報告附上執行紀錄檔，內容應包括： 各個人電腦資安檢測結果表、各伺服器主機資安檢測結果表、網路側錄封包資料、執行過程如果有發現惡意行為、惡意程式或外洩資料的過程紀錄，及惡意程式或外洩資料的列表。

第三節 弱點掃描服務需求

協助本會依據「資通安全責任等級分級辦法」應辦事項中安全性檢測要求，對本會指定範圍之網站、主機、伺服器、個人電腦、網路設備、資通安全設備及物聯網設備進行弱點掃描，評估掃描目標是否存在安全弱點，同時提供掃描結果，作為網站、主機、伺服器等等資通安全管理依據，並提供弱點修補建議，待弱點修正後提供複掃，確認弱點已經排除。

一、弱點掃描內容

弱點掃描包含系統弱點掃描與網站弱點掃描。

（一）系統弱點掃描

對作業系統與網路服務及其設定、帳號密碼設定及其管理方式等進行弱點檢測，系統弱點掃描的檢測項目須符合當時CVE(Common Vulnerabilities and Exposures)發布的最新弱點版本，且至少包含下列項目：

1.作業系統未修正的弱點掃描。

2.常用應用程式弱點掃描。

3.網路服務程式掃描。

4.木馬、後門程式掃描。

5.帳號密碼破解測試。

6.系統之不安全與錯誤設定檢測。

7.網路通訊埠掃描。

（二）網站弱點掃描

對網頁系統及網站主機進行弱點掃描，檢測項目須符合當年度 OWASP 官方網站公布之最新版 OWASP TOP 10 項目。

（三）執行範圍

每年執行2次，執行時間由本會指定，執行前30日通知廠商，執行範圍為本會營運範圍。

（四）執行方式

1.弱點掃描工具為合法授權之商用軟體，於每次弱點掃描前，須將工具之弱點資料庫更新至最新版本，並提供佐證資料，以確保本項服務之正確性。
2.應於弱點掃描初掃後協助提供弱點修補建議。

應於本案工作說明書中規劃弱點掃描期程及工作計畫，工作計畫內容應包含使用工具(須含授權)、執行掃描方式、時程(須含初測、弱點修補、複測、報告提交等)。

應於弱點掃描結束(即複測結束)後 30 日內提交弱點掃描服務報告，報告內容須包含初掃內容與複掃內容。

初掃內容應包含：執行結果摘要說明、執行計畫(執行期間/執行項目/執行範圍/專案成員)、掃描工具說明、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、IP/URL、Port Number、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如弱點無法修補，須說明原因與配套措施)。

複掃內容應包含：執行結果摘要說明、執行計畫(執行期間/執行項目/執行範圍/專案成員)、掃描工具說明、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、

IP/URL、Port Number、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如弱點無法修補，須說明原因與配套措施)、與初掃之差異化比較(例如未修補弱點及新發現弱點等相關描述與統計)。

第四節 滲透測試

廠商應對本專案指定範圍之伺服器主機作業系統、應用軟體、網路服務等安全弱點與漏洞，進行滲透測試， 設法取得未經授權之存取權限，並測試內部資料是否有遭受不當揭露、竄改或竊取之可能性，以找出可能的資安漏洞，並提出改善建議，並於協助修正資安漏洞後提供複測，以確認已經完成修正。

一、 滲透測試範圍

本會指定之專案 URL 或 IP 10 個

二、 滲透測試內容

（一）資料蒐集

對受測目標進行資料蒐集與資訊分析(如：嘗試至受測物聯網設備官方網站或透過網路資源取得該設備相關系統資料，及蒐集該設備已知弱點資料)，將取得之相關資訊做為執行滲透測試使用。

（二）分析報告

根據滲透測試結果，詳細記錄發現的弱點與測試過程，並對結果進行分析，提出相關建議與測試報告。

（三）風險管理

在滲透測試執行前，需評估可能發生非預期資料損毀或遺失的情形，以利本會應變。在滲透測試執行期間，執行具侵入性質的檢測作業皆需與本會進行確認，並於雙方議定之適當時間且具備適當應變措施與風險評估後，才進行相關檢測作業。

（四）測試內容

1. 測試項目

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
	本機服務	在已取得系統控制權限的條件下，可執行至少包含本機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
	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	電子郵件服務套件	至少包含 SMTP、POP3 及 IMAP 等常見對外郵件服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	網站服務套件	包含常見 WEB 套件弱點測試，如設定缺失、權

測試類型	測試類別	測試項目
		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
	網路服務套件	至少包含 DNS、PROXY 及 SNMP 等常見網路服務之弱點測試，如設定缺失、權限控管及套件弱點等測試項目
	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檢測項目
密碼破解	密碼強度測試	至少包含 WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC 及 Database 等常見對外服務之密碼字典檔測試
無線服務	無線服務弱點測試	到場服務的條件下，包含無線服務套件弱點測試與 WiFi 密碼字典檔測試等項目

2. 執行方式

(1) 廠商應組成滲透測試小組，模擬駭客行為，利用伺服器主機的作業系統、應用軟體、網路服務，以及防火牆、路由器、交換器等網路設備之安全弱點(如：網站設計不當，或防火牆、路由器等安全政策設定錯誤)進行滲透測試，設法取得未經授權之存取權限， 並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能。

(2) 應分別對本專案指定範圍之網路設備、資安防護設備、系統平台與網站進行滲透測試。外網(網際網路)滲透測試執行方式由本會依當年度需求決定，內網(企業網路)須於本會內部(on-site)進行。

(3) 應依本項服務排定之時間(須含初測、初測結果說明、複測、報告提交等)執行滲透測試作業。

(4) 應彙整分析滲透測試結果，提出測試報告，並依本會需求，安排滲透測試結果簡報，並應建議改善方法，對應修補之弱點進行追蹤管理。

應於本案工作說明書中規劃滲透測試期程及工作計畫，於滲透測試結束(即複測結束)後 30 日內提交滲透測試服務報告，報告內容應包含：摘要說明(受測目標風險等級與數量列表/受測目標風險漏洞名稱列表/風險漏洞分布列表)、專案執行計畫(執行期間/執行項目/執行範圍/專案成員)、執行結果(受測目標/漏洞名稱/問題URL 或IP/問題參數/測試語法/測試截圖/初測與複測結果比較等)、改善與建議、結論。

第五節 人員派駐服務

一、廠商應在簽約日起 10 日內提供本會資安專業駐點人員 1 人。

二、廠商應指派人員應具備所需之條件資料，惟廠商擬派駐之人員如具有相關專業證照或特殊經歷，經本會認可確具有所需之能力者，得不受學歷資格條件限制。

派駐人員由廠商完成招募及選用，本會得對廠商選用人員進行書面審核、面試或筆試，以驗證其專業能力，不符合標準之人員，本會得要求更換。於本專案執行期間，如發現有不符本會要求事項，本會有權要求廠商另派人員。

三、派駐人員未完成審核前，如有先行執行之必要時，廠商得先行派用，後續如與核定內容有所差異時，再予以修正。

四、派駐人員主要工作內容至少如下：

（一）派駐人員應填妥出勤簽到簿(格式如本徵求文件附件 1)。餘依勞動基準法規定辦理。

（二）派駐人員協助本專案監控範圍之資安監控、資安警訊通知、資安事件通報與即時處理追蹤。

（三）本會自行採購之防毒、防火牆、應用程式防火牆、進階持續性威

脅防禦措施、主機特權帳號存取控管設備等資安設備，指定辦理之資料分析與整合、資安防護失效檢查服務與持續導入服務。

（四）派駐勞工於派駐期間，立約商應指示派駐勞工，遵循本會工作規則等規定與其他交辦工作事項。

（五）本專案駐點人員變更時，應於 10 日前通知本會，駐點人員變更時並應安排 5 個工作天時間交接，交接期間前後任駐點人員應同時進行駐點服務。

(六) 本專案駐點人員須配合簽訂保密協定。

五、專案人員服務需求：

（一）投標廠商於計畫書所列之人力，僅係為完成本專案之基本人力，廠商有義務提供充分人力完成本專案之各項工作。

（二）廠商團隊成員名冊需納入「專案工作計畫書」提交。

（三）如專案組織工作進度連續兩週持續落後或交付項目經評估不符本會所需，本會得要求增加或更換妥適之駐點人員，並派駐處所，或其他矯正措施，在專責人員協助下，執行專案工作計畫。

（四）廠商於專案期間應協助本專案相關會議舉辦、溝通及準備相關資料。

（五）駐點或進入本會之工作人員並應依資安規範進行報到與權限申請作業。

第六節 端點偵測及應變機制(EDR)

提供 1,000 台使用授權，得安裝於本會伺服器主機與使用者個人電腦，將可疑行調查分析後，提出處理建議。

偵測與應變機制需求如下：

一、端點偵測與應變機制(EDR)，支援 Windows, Linux, macOS 作業系統。

二、端點偵測與應變機制(EDR)程式部署於端點後，可在背景執行，

不影響使用者日常操作，可依使用者需求自行調整設定，包含記憶體負載（Memory）、運算負載（CPU）、流量限制（Traffic）及延遲時間（Delay）設定。

三、支援無網路端點主機鑑識作業，使用可攜式儲存裝置(如 USB 隨身碟等)上載端點程式至端點主機，待執行結束再手動將掃描結果匯入中控平台進行分析。

四、端點程式具備自我保護功能，可防止遭到刪除、終止程序及惡意更改路由等阻止運作行為。

五、可偵測無檔案式攻擊（Fileless Attack），如 WMI command invocation 和 Powershell attack 等攻擊。

六、勒索軟體攻擊防護、可疑 Webshell 攻擊即時阻擋、可疑 Cmdline 攻擊即時阻擋、可疑 Registry 防護。

七、具備端點主機鑑識報告，內容包含記憶體鑑識分析、檔案分析、網路分析與主機記錄分析等。

八、具備網路分析功能，分析類型包含主機端發起與接收連線的應用程序，提供可視化圖表追蹤不同主機間網路連線的關連性。

九、具備自動威脅鑑識分析功能，可依惡意程式感染擴散行為，自動展開威脅事件分析拓樸圖。

十、可依時間軸分析統整威脅軌跡報告，分析端點電腦使用者記錄，及此端點設備執行過的程式、開啟過的檔案。

十一、可事件回溯分析並產生關聯分析報表，找出端點電腦感染惡意程式的途徑、使用過的工具及時間點。

十二、圖形化事件報告(Incident Report)呈現攻擊路徑與手法。

十三、具備自訂白名單設定例外，提供雜湊值（Hash）及動態規則（例如 Yara Rule）設定，針對檔案與記憶體內容進行設定。

十四、具備自訂威脅情資功能，內建業界標準 Yara Rule 編輯器。

十五、專案執行期間，需提供最新版本的EDR程式、Patch檔案、特徵碼或Firmware，且不得另行收費。

第三章 服務管理需求

第一節　需求內容

一、服務水準

本案各項服務水準協定(Service Level Agreement, SLA)，以達成該項服務需求為依據，透過客觀的證據或指標，做為品質管制，預防各項不符合作業的事項發生，降低風險，服務水準規範如下：

(一)資安監控服務

項次	項目	服務水準
1	資安監控環境部署	1.資安監控設備造成本會網路系統作業中斷或嚴重流量阻塞超過 30 分鐘且發生達 3 次，廠商須配合更換同等級以上效能較高之設備。 2.資安監控設備與資料收集器安裝故障，廠商須於 24 小時內修復完成或調換同等級以上之相容設備。
2	資安監控服務	1.本專案為 7x24 小時全天候監控，整體監控服務中斷一年不可超過 78小時，故障總時間。 2.整體監控服務全年中斷次數不超過5次。
3	資安事件處理	1.當發現資安事件時，廠商應於接獲通知後4小時內派員至本會。 2.當發現資安事件後，廠商應於「資通安全事件通報及應變辦法」規定時間內完成損害控制或復原作業。
4	資安事件之通知	1.經判斷為資安事件時通知本會資安聯絡人最大可容忍通知時限：每次1小時

(二)資安健診

項次	項目	服務水準
1	使用者端電腦惡意程式或檔案檢視	1.惡意程式檢測時，使用者電腦故障率須小於 1%。 2.因惡意程式檢測造成使用者電腦故障，須於 10 分鐘內完成通報，4 小時內修復完成。
2	伺服器主機惡意程	1.惡意程式檢測時，伺服器主機故障率需小於 1%。

	式或檔案檢視	2.因惡意程式檢測造成伺服器主機故障，須於 10 分鐘內完成通報，4 小時內修復完成。

第二節　違約及服務績效違約金

詳「資訊服務採購契約」第十五條。

第四章 管理需求

第一節 專案組織成員基本要求

專案成員基本要求

組別	角色	資格需求
委外資安監控、端點偵測及應變機制服務	資通安全專長人員	至少 2 位具備電腦稽核技術證照，如：ISO 27001 Lead Auditor 或CISA(Certified Information System Auditors)，以確保服務水準。
		至少 2 位具備經本會同意之電腦鑑識認證或病毒處理相關認證，如：EC-Council CHFI(Computer Hacking Forensic Investigation)或TWCERT/CC Certified Computer Forensics 等。
	網路專長人員	具備網路規劃專業認證，如：CCNA或同類資格認證。
	資安監控人員	資安監控服務團隊應具備下列技能，團隊中遠端資安監控人員至少1人，擇1證照，以確保服務水準。 ● CEH(EC-Council Certified Ethical Hacker)。 ● CND(EC-Council Certified Network Defender)。 ● CSA(EC-Council Certified SOC Analyst)。 ● CTIA(EC-Council Certified Threat Intelligence Analyst)。 ● CySA+(CompTIA Cybersecurity Analyst)。 ● 其他資安相關專業證照。
	資安專業駐點人員	資安專業駐點人員1人 須具備下列專業技能： 1.資安技術：接受過CEH(Certified Ethical Hacker)或其他類似相關課程訓練。 2.系統管理：接受過 MCSE(Microsoft Certified Solutions Expert) 、 LPIC(Linux Professional Institute Certification)、RHCE(Red Hat Certified Engineer)或其他類似相關課程訓練。

資通安全檢測服務	資通安全健診	1. 每位專案人員依服務項目應具備專業要求，擇1證照。 (1) 網路架構檢視、防火牆連線設定檢視：擇1證照 ● CCNA(Cisco Certified Network Associate)。 ● CCNP Security(Cisco Certified Network Professional Security)。 ● CND(EC-Council Certified Network Defender)。 ● CompTIA Network+。 ● iPAS 資訊安全工程師中級能力鑑定。 ● 其他網路安全相關專業證照。 (2) 網路(有線)、使用者端電腦、伺服器主機等惡意活動檢視：擇1證照 ● CEH(Certified Ethical Hacker)。 ● CHFI(Computer Hacking Forensic Investigator)。 ● CND(EC-Council Certified Network Defender)。 ● SSCP(System Security Certified Practitioner)。 ● CompTIA Security+。 ● 其他網路、系統安全相關專業證照。 (3) 目錄伺服器設定檢視、政府組態基準(GCB)檢視：擇1證照 ● Microsoft Certified: Azure Administrator Associate。

		● Microsoft Certified: Azure Security Engineer Associate。 ● CompTIA Security+。 ● SSCP(System Security Certified Practitioner)。 ● iPAS 資訊安全工程師中級能力鑑定。 ● 其他系統安全相關專業證照。
	弱點掃描、滲透測試人員	弱點掃描、滲透測試服務團隊應擇1證照，團隊人員至少1人，以確保服務水準。 • CEH(EC-Council Certified Ethical Hacker)。 • CPENT(EC-Council Certified Penetration Tester) 。 • CompTIA PenTest+。 • CPSA(The CREST Practitioner Security Analyst)。 • OSCP(Offensive Security Certified Professional)。 • 其他資安相關專業證照。

一、廠商專案組織成員應簽署下列文件：

(1)保密切結書。

二、驗收

1.廠商應充分配合本專案各項交付項目之確認及查驗流程。

2.廠商應於完成各階段交付工作後，備妥相關文件通知本會辦理驗收，並派員配合本會進行確認及驗收程序。

第二節 責任規範

1. 廠商於專案履約期間應遵循法律之規定及應負之保密責任。
2. 廠商因業務需求存取本會之資訊處理設施或資訊，應遵守資通安全相關規定。相關人員涉及資產完整性與機密性之資訊安全管理範圍者，廠商並應要求相關人員簽署保密切結書，併同工作計畫書提交。專案履約期間如相關人員異動，應於人員到任前提交，並於次年度專案工作計畫書更新版本進行更新。
3. 駐點或進入本會之工作人員並應依資安規範進行報到與權限申請作業。
4. 廠商提供或援用之軟體，應為經合法授權之軟體。
5. 本會得要求廠商出具原廠保證書或簽署聲明文件等，以確保廠商
6. 所提供之軟體、硬體及自行開發之程式確實符合其所宣稱之標準。
7. 廠商執行本專案所使用或提供之軟體、硬體及服務均不使用大陸廠牌資通訊產品；且不得僱用大陸籍人士辦理本專案。

附錄

一、 附錄 1：計畫書規定

（一） 計畫書製作

1. 投標廠商製作計畫書時，其內容編排請參考下一節「計畫書內容大綱」，並以本徵求計畫書中相對應之需求為依據。對於本文第二章「專案需求」中所列舉之各項需求，計畫書均必須提出說明或建議。
2. 計畫書應以 A4 規格紙張、14 號字型印製，文字以直式橫書方式編排並編頁碼採雙面列印，請於左側裝訂牢固及裝訂。
3. 製作服務計畫書之花費，由廠商自行負擔，本會不另支付費用。
4. 計畫書內頁依序應包括評選項目與計畫書內容對照表、目錄、本文及附件。
5. 投標廠商對於計畫書範圍如有額外建議或補充，得於計畫書中另作註解或另闢附件加以描述。增列之項目請於適當章節內說明，並標註「增列」字樣。
6. 本會如對服務計畫書內容有疑義時，廠商應配合解釋。
7. 倘有優規部分請表列 RFP 及優規對照。
8. 計畫書交付日期、地點及方式悉依照投標須知規定辦理。
9. 投標廠商須依照內容大綱，製作服務計畫書送本會審查。

（二） 計畫書內容大綱

壹、專案概述

貳、廠商經驗、實績及履約能力、組織與規模

參、專案管理

肆、專案需求建議

派駐人員技術能力、勞動條件與福利說明

伍、經費配置明細

陸、參與本專案優規說明

（三） 計畫投標廠商以具備資訊安全管理輔導經驗為佳，下列項目廠商提供相關證明文件納入計畫書，以納入評選項目一之評分參考

1. 投標廠商需於國內擁有資通安全監控中心，並通過 ISO27001 認證。(須檢附證明)
2. 投標廠商需至少有下列證照認證(須檢附證明)：CISSP、CEH 認證至少兩名以上。
3. 投標廠商必需具備資訊安全業務銷售與資訊安全維運服務經驗。
4. 投標廠商於國內需具有對外提供資通安全監控中心監控服務之專案實績。(須檢附實績證明)
5. 投標廠商於投標時，各設備應附型錄；如為技術手冊資料影本應加蓋公司大小章。