財團法人公共電視文化事業基金會
新媒體部「資安數據分析」採購案

需求說明

2021 年 4 月 22 日

壹、專案概述

一、專案名稱

財團法人公共電視文化事業基金會(以下簡稱本會)新媒體部「資安數據分析」採購案(以下簡稱本案)。

二、專案目標

本會「資訊安全監控」服務，乃透過廠商提供之數據專線或網際網路連結方式，由廠商具有之資訊安全監控中心(Security Operation Center，SOC)，達成以下目標：

1. 提供每週 7 日、每日 24 小時全天候即時遠端監控服務。以符合資訊服務機密性、可用性與完整性之要求。
2. 偵測本會網路環境、重要伺服器、系統環境與網際網路所產生的資安事件(故)，適時進行通報應變、鑑識分析、追蹤處理等回應。
3. 強化本會網路安全監控偵測及防禦機制，俾於受到入侵時能立即啟動通報、防護與緊急應變措施。
4. 健全本會電子化／網路化應用環境，確保網路服務品質。
5. 深層強化偵測與防禦能力，以確保對外服務網站之安全性。

三、服務範圍

1. 本案資訊安全監控防護之範圍為本會所建置之資訊安全相關設備，監控標的如下：包括本會 2 台 Juniper 防火牆（HA）、3 台 AD 主機(微軟 WIN2003)、1 台 WAF 設備(F5 BIG-IP)，及位於 IDC 機房 2 台 Juniper 防火牆、1 台 WAF 設備(F5 BIG-IP)、本會 1000 個端點防毒軟體 LOG 收集監控。
2. 須提供租借 2 台入侵偵測與防禦設備，硬體效能需符合本會網路流量使用，軟體需可定期更新，並須加入資訊安全監控防護。
3. AD 主機監控，偵測登入帳號異動情形。
4. 滲透測試服務一次（5 台主機），須提供複掃。
5. 提供全會 EMAIL 帳號(1200 個帳號上下)四次的社交工程演練與 REPORT。
6. 網頁弱掃服務一次（5 台主機），須提供複掃。
7. 專案期間提供資安教育訓練 12 小時(含)以上。

四、專案時程

本案期間自簽約之次日起為期一年。得標廠商於簽約翌日起算7個工作日內完成監控佈署，並啟動資安事件監控服務，以達到服務不中斷的精神。

貳、服務需求規範

一、資訊安全監控服務

（一）監控服務水平

1.提供 7*24 全天候即時遠端資安事件監控服務及提供異常資安事件(故)處理建議，協助進行線上緊急應變處理。

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記錄，偵測有安全風險的行為。

4.透過資訊安全監控中心預警與監控中心人員綜合分析篩選出資訊安全事故，並依資訊安全監控中心(SOC)之事故管理流程，即時通報並協助進行線上緊急應變處理或派員到場處理。

5.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 30 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、攻擊方法與路徑分析，以及相對應緊急應變措施建議，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。

6.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 日內提供書面報告，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、處置情形以及相對應的應變措施與建議。

（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。

7.當資安事故發生時，本會除依廠商通報內容之應變措施處置外，得要求廠商派員至本會協助事故處理，廠商應於接到通知後 4

小時內派員到場協助，廠商不得拒絕。

8.每月 15 日前並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「資安事件監控管理服務報告書」予本會，並應依本會要求派員說明。REPORT 請依監控區域(PTS、IDC)分為各自兩份提供，須於每季另提供季報告與派員簡報。

9.資安威脅警訊通報服務

（1）廠商可採電話、傳真、電子郵件等方式，適時提供資訊安全警訊通報服務，內容包括：資訊安全威脅類型、說明、可能造成之影響。
a.各大原廠發布的最新修正檔。
b.新發現資訊安全漏洞與補救措施。
c.資訊安全事故記錄與報導。
d.漏洞分析、修補建議或對策。
（2）警訊通報內容以中文為主。

10.監控資料、資訊安全事件(故)通報紀錄及處理紀錄至少保存 6 個月以上。

11.中文資安網站或管理介面

廠商應提供中文資安網站或管理介面，作為資安事件通報、處理追蹤、查詢及統計等功能，其功能至少須包含：
（1）至少提供三組登入帳號供本會使用。
（2）即時資安案件檢視及分析。
（3）歷史資安案件查詢及統計。
（4）資安預警通報作業。
（5）資安預警資訊查詢。
（6）案件處理狀況追踪。
（7）資安整體狀態。
（8）資安新聞。

（二）AD 監控

需偵測 AD 異常事件，主要在於發現異常的帳號登入與異動情形，偵測項目包括：單一來源 IP 持續登入失敗、對單一帳號持續登入失敗、非法 Administrators 群組帳號存取事件偵測、非預期帳號登入事件偵測及帳號異動事件偵測。

（三）租借網際網路入侵防護偵測暨整合 SOC 監控服務。

1.提供租借 2 台入侵偵測與防禦設備，硬體效能需符合本會網路流量使用，需可更新防護特徵值或韌體。

2.佈建於網際（骨幹）網路，並提供 7x24 安全監控與管理(SOC 監

控)服務，且由廠商自動更新防禦特徵，即時調整防護政策、監控及分析網路病毒及攻擊行為，並適時通報本會採取防範因應措施。如需配合變更本會相關網路設定或架構需提報經本會同意後方可執行。

二、滲透測試服務

以最新滲透攻擊程序(Exploit)進行重要資訊系統主機（5 個 IP）外部滲透測試服務，並且提供報告說明。

滲透測試服務完成後，提供「滲透發現報表」，其中應該說明與圖形化表示：例如：所發現的所有受測主機之作業系統版本、提供服務、以及滲透成功所利用的弱點或者漏洞資訊(含網路相關資訊鏈結)等報表資訊。

滲透測試服務完成後，提供「滲透測試過程流程圖」，其中應該說明與圖形化表示：至少包含滲透測試過程中的每個步驟的起迄時間、每個步驟使用的滲透測試模組、以及階層式滲透測試的關係。

滲透測試服務完成後，提供「滲透流程歷史報表」，針對每個步驟所使用的滲透測試模組詳細說明「動態結果/最後結果(Output)」、「執行過程紀錄與失敗紀錄(Log/Debug)」、「執行模組的環境參數清單(Context)」等。

上列各種報表輸出可轉為 HTML 與 XML 等格式。

滲透測試服務結束後，提供「滅跡(Clean-Up)」、「反安裝(Uninstall)」功能，讓滲透測試的受測主機系統恢復到原先未被滲透成功前的狀態。

廠商需提供 1 次滲透測試服務(初測、複測，計算 1 次)共 5 台主機，針對本會之伺服器／主機作業系統、應用軟體、或網路服務，進行滲透或穿透跳躍主機之入侵測試，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、竄改或竊取之可能性。

（一）資料蒐集

對受測目標進行資料蒐集與資訊分析，將取得之相關資訊做為執行滲透測試決策。

（二）分析報告

根據測試結果，將所發現之弱點與過程詳細記錄，並對結果進行統計分析，提出相關建議與測試報告。

（三）風險管理

在滲透測試執行期前，需提出對受測目標進行備份建議，避免發生非預期資料損毀或遺失等情形。

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

【表 1】滲透測試項目表

類型	類別	項目
作業系統	遠端服務	●在到場服務的條件下，可執行無線服務弱點測試項目。
	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(1)	●至少包含XSS 弱點測試、SQL Injection測試、LDAP Injection測試、XML Injection 測試、SSI njection測試、XPath Injection測試及Code Injection測試等項目。
	輸入驗證(2)	●至少包含XSS弱點測試、SQL Injection測試、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。

類型	類別	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、權限控管及套件弱點等測試項目。
	檔案傳輸服務套件	●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，在到場服務的條件 下，可執行WiFi密碼字典檔測試。

2.執行方式

（1）得標廠商應組成滲透測試小組，模擬駭客利用各伺服器／主機作業系統、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（例如網站設計不當，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）得標廠商應分別針對本會網際網路及內部網路進行滲透

測試。網際網路滲透測試係滲透測試小組直接由遠端進行，內部網路於本會內部（on-site）進行。

（3）得標廠商應依排定之日期執行滲透測試，於非公務時段或與本會協調取得適當時間進行測試作業。

（4）得標廠商應彙整分析測試結果，提出測試報告，並視需求安排測試結果簡報。

（5）得標廠商於檢測後，應針對修補之弱點提供建議，協助本會進行改善。

三、電子郵件社交工程演練

廠商應辦理 4 次本會內部網路之電子郵件社交工程演練，且應提供演練所需之軟硬體設備，並於演練前，與本會研議演練範圍、方式（須含測試信件樣本）、時程，以及軟硬體設備（須含合法使用證明）、執行人員等相關細節，並擬具演練計畫，經本會審核後據以執行。執行後須提供報告並簡報。

四、資訊安全諮詢服務

廠商應提供客服專線，以供本會做為資訊安全事件(故)諮詢與建議之聯絡窗口，並依本會要求派員至本會協助事件(故)處理，提供資訊安全相關議題之技術輔導及諮詢服務。

五、提供相關軟硬、體設備：

分析本會環境及作業需求，至少提供必要相關資安軟、硬體設備，並由廠商負責自行維護、更新及效能提昇。

廠商提供之相關軟、硬設備，須於服務建議書中詳述其規格及資訊安全確保方式並須經本會認可。

六、Web 網頁弱點掃描

廠商應辦理 1 次 5 個 IP 針對機關 Web 網頁系統進行安全弱點掃描，評估掃描標的物是否存在安全弱點，同時提供相關掃描結果，作為資訊安全的管理依據，並協助弱點修補方法之參考建議，待修正弱點後提供複掃，以確認弱點已經排除。

（一）執行方式

1.得標廠商應於需求訪談階段先分就本會之網路架構及本項服務之標的設備進行了解，如設備廠牌、系統版本等，以利後續進行弱點分析及修補建議。

2.掃描工具為取得授權使用的商用軟體，於每次弱點掃描前，將工具之弱點資料庫更新至最新版本，並應提供佐證資料，以確保本項服務之完整正確。

3.得標廠商應依排定之日期執行弱點掃描，於非公務時段或與本會協調取得適當時間進行掃描作業。

4.得標廠商應於弱點初掃後協助本會進行弱點修補，包括彙整本會之弱點修補情形，維護未修補清單中之未修補或排除原因等。

七、資安教育訓練

廠商應提供資安教育訓練供本會全體同仁上課使用，資安教育訓練須 12 小時(含)以上，專案期間總時數至少為 12 小時(含)以上。

參、其他規範事項

服務表現良好，專案範圍不變動之下，次年予以原條件直接續約採購。

一、付款條件

分四期，每季驗收合格後付款合約總金額之四分之一，月結九十天。

二、管理需求

A.得標廠商資格

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，並於服務建議書專章詳述：

（一）凡在政府機關登記合格，且不得為陸資企業(包括子公司、分公司、獨資或合夥事業及其轉投資事業)。本案涉及資通訊軟體、硬體或服務等相關事務，廠商執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。

（二）本案服務內容將涉及敏感資訊,得標廠商不得轉包或分包予其他經銷商執行。

（三）得標廠商須實施資訊安全管理制度(如由經銷商投標須代為提出)，通過 ISO 27001:2013 或其他類似驗證，並於專案執行期間持續有效，以保護本案服務所取得之資料。

（四）本案團隊人力至少應包含專案負責人/專案經理與資安監控服務人員。資安監控服務人員應具備以下所列舉之技能，且各類技能至少有一名成員，以確保服務水準，並於建議書中檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下:

1. 惡意程式檢視：接受過 CEH(Certified Ethical Hacker)、CHFI (Computer Hacking Forensic Investigation) 、OSCP(Offensive Security Certified Professional)或其他類似相關課程訓 練證明(以上訓練證明擇一)。
2. 資訊安全技術或管理：接受過 CISSP(Certified Information Systems Security Professional)、ISO/CNS 27001 Lead Auditor 或其他類似相關課程訓練證明(以上訓練證明擇一)。

B.服務水準協動(SLA)與罰則

(一)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	服務水準	未達水準罰則	罰則說明
1	資訊安全監控服務	本專案為7x24 小時全天候監控 ・整體監控服務中斷超過 4 小時後，每逾 4 小時扣 1 點。 ・若非歸究於乙方之責任時，則不列入計算。 2、 資安事件通報 ・監控系統須能偵測入侵事件、偵測登入帳號異動情形等均為監控範圍，於範圍內若機關入侵行為測試、機關「攻防演練」或遭入侵，監控系統未能發現者則扣 1 點。 ・得標廠商在資安事件發生時，應於監控人員分析確認為惡意攻擊後 30 分鐘內發布預警通報通知機關資安連絡人，通報中應至少包含受影響主機名稱、惡意程式及中繼站清單、遭竊取帳號、惡意程式來源及建議處置方式等，並於單位要求後 3 個工作天內，提供完整書面來龍去脈分析報告。若服務水準未達成每單一事件扣 1 點。	扣 1 點	若服務水準持續未達成，每 1 小時扣 1 點
2	滲透測試服務	提供滲透測試 5 台主機，並須提供複掃。	扣 5 點	
3	社交工程演練	提供全會 EMAIL 帳號(1200 個帳號上下)四次的社交工程演練與 REPORT。	扣 4 點	每次扣 4 點
4	網頁弱掃服務	提供網頁弱掃 5 台主機，並須提供複掃。	扣 5 點	

(二)相關說明

1. 承作廠商無法達成相關工作項目服務水準，SLA 罰則依每期付款時結算，其罰款(違約金)計算方式為每期罰則點數x契約總價千分之一。工作項目如遇有重複計罰狀況，以罰則較高者為準。
2. 應交付之項目或文件，如有超過完工交付期限，每延遲 1 日(以日曆天計，星期日、國定假日及其他休息日均應計入，不滿 1 祖以 1 日計算)，本會得按契約總價之千分之一計算懲罰性違約金，款項可自契約總價或履約保證金項中扣抵。
3. 違約金上限以契約總價之 20%為上限。如違約金逾 20%時，本會得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。

C.品質需求與驗收標準

（一）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。
4. 得標廠商於本專案服務使用之工具軟體，均應出具合法授權之證明。

（二）驗收標準

得標廠商應依貳、專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件與紀錄之交付。

（三）驗收方式

依據實際建置計畫與設備，詳細規劃驗收流程，由本會審查通過後據以進行測試及驗收。廠商依履約所供應或完成之標的，將符合契約相關規定，具備一般可接受之專業及技術水準，無減少或滅失價值或不適於通常或約定使用之瑕疵。

得標廠商應依進度完成各期工作，交付有關工作項目成果或文件通知本會辦理驗收，本會應於接獲承包廠商交付之成果或文件，兩星期內函送審查結果，如有問題，承包廠商應於接獲通知，兩星期內完成修正並函送機關辦理複驗。

（四）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，並簽定保密協議書。
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. 得標廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由得標廠商自訂)。
4. 契約終止時，得標廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本會或經本會同意後銷毀。
5. 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。
6. 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。

D.配合事項:

(一)得標廠商須無償配合提供：本會災難演練、主管機關或行政院災防演習之遠端技術協助或諮詢服務。

(二)需無償配合本會依 ISO 27001 之指定的第三方外部稽核或查核，進行實地或書面訪查作業，如有違反資通安全法規情事依合約條款處理，並不得續約。

(三)廠商應遵守行政院所頒訂之各項資訊安全規範及標準，並遵守機關資訊安全管理及保密相關規定。此外機關保有對廠商執行稽核的權利。

(四)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)，並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。

(五)廠商提供服務，如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。

(六)基於法令及合約需求，本會得要求實施定期或不定期稽查，以監督專案內各項安全管理執行情形。

(七)契約履約或終止後，廠商應刪除或銷毀執行服務所持有機關之相關資料，或依機關之指示返還之，並保留執行紀錄。

三、交付項目

A.交付項目與時程

（一）簽約翌日起算 7 個工作日內完成監控佈署。
（二）工作計畫書：決標日起 2 週(日曆天)內交付。
（三）監控服務(季)報告：每 3 個月後的 15 日前。

B.交付文件格式

（一）監控服務(季)報告以電子郵件或用戶服務網站等方式提供。
（二）必要時本會得要求派員親臨說明。

C.交付項目說明

交付項目	內容說明
1.工作計劃書	1.1 工作計畫書應以得標廠商投標時之「建議書」為基礎，並依本會需求作修改。 1.2 內容除包括對本專案之執行敘述，含專案管理、組織、人力、工作項目、時程說明及品質管理流程。
2.監控服務(季)報告	2.1 提供每季資訊安全事件(故)統計及入侵事件(故)分析等中文化報表。

肆、建議書製作規定

A.服務建議書格式

（一）紙張:宜用 A4 規格
（二）繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明投標廠商名稱、投標廠商地址、本案名稱及日期，裝訂線在左側。
（三）目次：應標示各章節之出處頁碼。
（四）投標廠商投標建議書之份數為一式三份。

B. 服務建議書內容

（一）專案概述
1.專案名稱
2.專案目標
3.專案時程
（二）投標廠商說明
1.投標廠商簡介
2.公司營運狀況，包含參與人員名單、能力證明及投標廠商經驗說明。
（三）專案工作規劃
1.資訊安全監控服務
（含租借網際網路入侵防護偵測暨整合 SOC 監控服務）
2.滲透測試服務
3.惡意電子郵件社交工程演練
4.Web 網頁弱點掃描
5.資安教育訓練
（四）專案組織與管理
1. 人力配置、資格及管理
2. 專案時程規劃
3. 專案管理規劃
4. 交付文件項目