國際影音平台技術部
資訊安全防護系統與授權採購案

需求說明書

中華民國113年3月

目　次

壹、　採購項目 3
一、交付項目 3
二、交付時程 3
三、驗收方式 3
貳、採購概述 4
一、採購名稱 4
二、採購範圍 4
三、契約時程 4
四、廠商資格 4
五、組織與人力需求 4
六、服務建議書撰寫格式 4
參、採購規格 5
一、資安弱點通報機制系統(VANS) 5
二、特權帳號管理服務 6
三、端點管理系統 7
四、網路資安風險平台服務 7
肆、保固與維護 5

壹、 採購項目

一、交付項目

項次	內容說明	數量	單位
1	**資通安全弱點通報機制** # VANs系統，一年授權 (200台電腦)	1	式
2	**特權帳號管理服務** # 提供特權帳號連線軟體，一年授權(25套授權) # 提供微軟 Server 授權 # 提供微軟Remote Desktop Service Device CAL， 一年授權 (25套授權)	1	式
3	**資安統一端點管理系統服務** # 端點管理系統，1年授權(280台電腦)	1	式
4	**網路資安風險評分平台授權及服務** #網路資安風險管理平台使用服務(1年授權)	1	式

二、交付時程

113年5月31日前。

三、驗收方式

得標廠商依交付項目、數量及時程完成交付相關文件後，辦理書面驗收。未於約定期限內完成驗收所需交付項目、數量和相關文件，則每逾期一日處千分之一懲罰性違約金。

貳、採購概述

一、採購名稱

國際影音平台技術部「資訊安全防護系統與授權」採購案 (以下簡稱本案)。

二、採購範圍

(一)資安弱點通報機制系統(VANS)

(二)特權帳號管理平台服務

(三)端點管理系統(UEM)

(四)網路資安風險管理平台服務

三、契約時程

113年5月31日以前交貨完畢，授權使用期間為113年6月1日起一年。

四、廠商資格

為確保資訊安全及得標廠商所提供之服務水準，投標廠商不得為經濟部投資審議委員會公告之陸資資訊服務業者。

五、組織與人力需求

(一)本團隊人員須具有中華民國國籍，不得為外籍勞工或大陸來台人士。於履約期間內，廠商團隊成員不得同時受僱於大陸地區，或有於大陸地區執業、工作等情形。

(二)為確保本案服務水準，團隊成員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。

(三)廠商應通過第三方驗證（ISO 27001 可被驗證版本）。第三方驗證機構須經財團法人全國認證基金會TAF認可 。

六、服務建議書撰寫格式

依本招標規範「採購設備數量表」各項次，逐項編製確認表（compliance table)。確認表再依項次展開答標，投標廠商應檢附設備型錄及相關證明文件，並以螢光色筆標示應答之規格，註明符合招標規範之 要求，以便本會逐項對照審核。若所附文件為外文內容，需自行翻譯成中文並加蓋公司章以便查驗。

(一)建議書及其附件之書面格式宜採直式A4尺寸（若有A3尺寸請摺頁為A4尺寸），橫式書寫，編妥目錄頁次並於左側裝訂成冊，儘量採雙面列印，建議書經提出後不得退換或更換補件。

(二)建議書封面標題統一為『國際影音平台「資訊安全防護系統與授權」採購案』，並標示廠商名稱及加蓋廠商及負責人印章，另註明本案聯絡人姓名與電話。

(三)投標廠商應於「服務建議書」內報列全案標價總額及依據工作項目內容，提送報價清單並分明列各項目單價及全案。

參、採購規格

一、資安弱點通報機制系統(VANS)

(一)需提供具有政府機關資安弱點通報機制(Vulnerability Alert and Notification System,簡稱VANS)管理功能之軟體授權 200 套，支援結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實資通安全管理法之資產盤點與風險評估應辦事項。

(二)在AD 的環境下可以進行軟體弱點掃瞄並比對出結果，無 AD 的環境下也可以獨立運作。需提供弱點掃描（VANS）服務

1. 依照「國家資通安全研究院」（簡稱「資安院」）之規定執行弱點掃描。
2. 定期與資安院連線取得最新弱點掃描標準，比對並產生需更新軟體報列表。
3. 依掃描結果派送軟體更新檔並以排程設定進行更新，確保軟體更新作業完成。
4. 提供符合規範之報表。

(三)該系統具有以下功能：

1. 部門總覽：可顯示該部門之階層、部門名稱、顯示名稱、清單檢視與報表輸出；清單檢視有電腦數量、軟體數量、作業系統數量與目前電腦KB 總數，當進行軟體與報表下載時可顯示進度。

2. 軟體總覽：顯示 CPE 軟體總攬統計，提供軟體名稱、版本號、CPE 編號、修補下載連結與各軟體安裝於那些台電腦並提供匯出與報表功能。

3. 電腦查詢軟體：可以電腦名稱、部門名稱、ip、作業系統版本作為過濾條件進行查詢該電腦安裝的軟體，執行相關的軟體弱點修補。

(四)CVSS 評分系統：顯示 CVSS 2.0、CVSS 3.0 分數、CPE 例外軟體提供計算器介面，由本單位自行計算 CVSS 分數。

(五)軟體更新server：可顯示軟體更新網址、須更新軟體自動下載更新、封裝、派送。

(六)報表功能：提供單位 VANS 總表、各部門分項 VANS 報表、管控軟體報表、非管控軟體報表、各電腦 VANS 報表。

二、特權帳號管理服務

(一)需提供Gartner Magic Quadrant Privilege Access Management 領導象限之特權帳號管理軟體，一年期 25 個採購用戶數。

(二)所提供之雲端產品須符合由 American Institute of CPAs (AICPA)驗證之 SOC Type 2 認證標準。

(三)提供經ICSA Labs 驗證之高安全性數位金庫。

(四)提供集中管理伺服器上的特殊權限帳號密碼功能，系統能定期偵測伺服器上與特殊權限管理系統不一致之密碼。

(五)具備一次性密碼、分拆密碼及密碼版本控管功能，可取得特定帳號、特定版本密碼。

(六)須提供遠端連線操作軌跡集中保存功能，對 Windows RDP、SSH、Telnet 之連線操作指令與畫面都能完整進行紀錄與留存，且不須於目標伺服器上安裝代理程式。

(七)須提供使用者操作歷程紀錄搜尋與播放功能，可使用瀏覽器介面依時間、使用者、目標伺服器或使用者操作指令內容等查詢條件搜尋側錄內容。

(八)內建稽核報表功能，報表內容可包含帳號申請核准使用、帳號登入登出時間、特殊權限帳號活動紀錄等相關資訊。

(九)提供整合Cloud 平台時連接使用規格如下：

1. 作業系統(Operating System)：提供一套Microsoft Windows Server 。

2. 提供Remote Desktop Service Device CAL 最新授權。 (25套授權)

三、端點管理系統

(一)廠商需提供一年授權之端點管理系統 280 套。

(二)可為本會提供一款整合式數位工作區平台，以協助集中管理所有應用程式、行動裝置使用情境，以及用戶自攜裝置和企業配發個人裝置。

(三)可在多個平台 (Windows 10、macOS、Android、iOS、Chrome OS 與 Linux 等) 上運作；透過單一管理主控台設定、控制與監控任何裝置。

(四)具備條件式使用者存取、自動化規則強制執行、合規方針與資料遺失保護等功能；還可自動且立即抵禦網路安全性威脅，以保護本會的敏感資料與應用程式；同時協助管理員識別裝置越獄與作業系統刷機等情況。

四、網路資安風險平台服務

(一)服務應含以下項目：

1. 提供專用儀表板網站，供本會查看最新資安風險評分平台資訊。

2. 系統採以非侵入的方式針對 Internet 之數位足跡數據(Digital footprint)進行收集、分析之技術，評估出甲方之資安風險問題。並可產出本會之資安風險係數報告及可能被利用的漏洞之報告。報告內容包括下列 10 個資安風險項目類別:

(1) NETWORK SECURITY

(2) DNS HEALTH

(3) PATCHING CADENCE

(4) ENDPOINT SECURITY

(5) IP REPUTATION

(6) APPLICATION SECURITY

(7) CUBIT SCORE

(8) HACKER CHATTER

(9) INFORMATION LEAK

(10) SOCIAL ENGINEERING

3. 系統評估之風險(Risk)等級可分類為:

(1) HIGH SEVERITY

(2) MEDIUM SEVERITY

(3) LOW SEVERITY

報告內容提供有關該風險問題的描述及修復建議。

4. 風險問題修復歷史紀錄：企業修補該風險問題弱點後，本系統服務需能提供風險問題驗證流程功能(Resolve)，驗證流程完成後，系統需能提供風險問題成功修復後的歷史修復紀錄以利備查，並快速更新成績資訊。

5. 本系統服務應能協助發現本會的資安盲點與資安弱點面相並提供有效的改善建議，提供可調查操作和客觀的分數變化與變更原因，以下包含但不限於:提供12個月的歷史檢視和趨勢資訊，於系統歷史紀錄中需能進行回溯性調查，可檢視過去發現的資安風險問題、可調閱已經修復的資安風險問題等紀錄。

6. 資料庫服務系統是本會儲存重要資料的數據保存系統，無論是人為疏失的設定問題或是其他問題等因素導致本會的資料庫直接曝露在internet 時造成資安漏洞盲點，為避免攻擊者利用該資安盲點進行網路攻擊與資料竊取。

7. 本系統服務需能檢測老舊的作業系統之資安風險問題為佳 如:(EOL:

End-of-Life Product)以及(EOS: End-of-Service Product)等作業系統，以避免攻擊者利用該資安盲點進行網路攻擊。

8. 針對本系統服務之資安風險評級，如遇誤報、錯評或者本會已經修正改善後，提供本會可以進行回應處理後更新評級，同時保存審核日誌備查，如有意外誤改或者修復錯誤時，系統可以電子郵件通知本會(指定管理員)，亦可恢復先前評級。

9. 系統評估之資安風險係數等級由 0 到 100 的分數方式呈現與量化，並可依照分數設定為告警條件，當觸發告警條件時，系統可自動發送 Email 告警的機制 ，即時以電子郵件通知本會(指定管理員)，並提供專用儀表板網站，供本會隨時查詢資安風險狀態。

10. 系統支援合規性框架確認功能：Compliance 如: ISO/IEC 27001，NIST SP 800 & PCI-DSS 3.1 & GDPR & NY DFS Framework 23 NYCRR 500。

11. 系統支援能夠直接在資安風險評分採購數量的解決方案內與第三方供應商溝通資安風險問題。

12. 系統須能支援不同報表種類及中文化報告。

13. 系統須能呈現事件修補歷史軌跡。

14. 系統須能提供降低風險及提高等級的修補建議清單。

15. 系統須能提供在全球各地對應的 IP 資產之數位足跡。

16. 系統須具備與同業比較之分析能力。

17. 系統支援 API 整合功能。

(二)廠商需提供1+5 Domains 一年授權。

肆、維護

(一)立約商交付授權有效期間至114年06月01日。

(二)立約商於授權期間內提供軟體5*8維護。

維護期間於上班時間提供電話或Mail維護服務，立約商須於4小時內回覆，8小時內提出解決方案。

(三)若立約商未依上述條款，每逾期一日按契約價金總金額千分之一計算逾期違約金，並連續處罰至立約商提出解決方案為止。