出國報告（出國類別：其他）

『赴駐舊金山科技組進行資安查核計畫等工作』結案報告

服務機關：科技部
姓名職稱：薛大勇 處長
派赴國家：美國
出國期間：107 年 5 月 21 日至 107 年 5 月 27 日
報告日期：107 年 6 月 26 日

摘要

隨著政府機關、民間企業及個人等大量利用電腦儲存資料及應用網路傳遞訊息，使得數位化資訊的安全性日益受到重視。有鑑於此，行政院於 2001 年正式設立「國家資通安全會報」，肩負起政府資通安全防護工作的推動，並要求各政府機關落實執行，確實做好資安防護工作，尤其是對涉及國家外交最前線之各駐外單位有更嚴格的資安要求。

本部目前在全球各地共設有十六個駐外科技組，初期由本部協助建立資安防護體制而後納入外交部管理，非合署單位(駐舊金山科技組、駐德科技組)則由本部自行管控。惟因非合署單位並無專責資訊人員，且辦公環境資訊設備因時空變遷及人員異動離職，致相關維護工作逐顯斷層。

為使資訊安全防護工作持續推動，本部於本(107)年 5 月 21 日派員前往非合署單位駐舊金山科技組進行資安查核作業，同時協助該組改善網際網路、作業系統及資安防護等資訊環境，並對該科技組同仁辦理資訊教育訓練，期強化其資安防護意識，使其知悉資安相關規定並了解資安防護基本技能及落實資安應辦事項。

目錄

壹、 目的

本次資通安全業務查核除針對駐舊金山科技組之連網模式及隔離電腦等設備，進行深度資安檢測、軟體漏洞修補及病毒碼更新等項目進行作業外，亦針對該組同仁進行資安教育訓練，訓練內容包含資安觀念宣導、外交部駐外機構資通安全作業規則、政風法規宣導及分享相關案例等，期強化同仁資安防護及法規遵循之意識，提升駐外單位整體資安防護能量。

貳、 過程

一、 行程

本次資安查核行程自 107 年 5 月 21 日至 107 年 5 月 27 日止，共計五天，行程說明如下：

日期	說明
107 年 5 月 21 日	臺北→舊金山
107 年 5 月 22 日	駐美國舊金山科技組工作
107 年 5 月 23 日	駐美國舊金山科技組工作
107 年 5 月 24 日	駐美國舊金山科技組工作
107 年 5 月 25 日	駐美國舊金山科技組工作
107 年 5 月 26 日	舊金山→台北
107 年 5 月 27 日	抵達台北

二、 現況說明

本次至駐舊金山科技組進行資安查核，為求確實達成任務所需，於抵達後先與組長、秘書及雇員就現行資訊環境等狀況進行資訊設備概況及網路架構訪談，經實地瞭解需求後，彙整如下：

(一)網路需求

目前駐舊金山科技組上網僅租用一條 T1 線路進行連網，其所屬辦公室區域、會議室、有線及無線網路環境皆使用此線路進行連網，時而發生連線緩慢之情況，

科技組希望了解原因並協助規劃適宜之解決方案。

(二)使用者端電腦需求

1.所有使用者端電腦並無正版防毒軟體授權，皆使用免費版本並自行安裝，且無適用之 Office 軟體，希望能協助安裝並定期升級。

2.無適當之儲存媒介，作為隔離電腦與連網電腦間資料傳遞之用。

(三)應用系統需求

教導該科技組之在地雇員使用本部內網及 MOTP 系統操作。

(四)資訊安全需求

1.駐外同仁有使用 HiKey 登入本部內網連線與操作相關問題。

2.為加強同仁資訊安全知識，駐舊金山科技組亦期望辦理有關資訊安全之教育訓練。

三、 資安檢測項目

(一)辦公室資訊設備

- 使用者端電腦共 5 台
- Note Book 共 2 台
- 作業系統 Windows 7 共 5 套
- Windows 10 共 2 套
- 複合式影印機 1 台。

(二)機房設備檢測

- 網路頻寬：中華電信 T1(1.54Mbps)專線。
- Adtran Access 908e VoIP 路由器 1 台
- Cisco SF 200-24 24 Port 網路交換器 1 台
- AbovEdge 語音電話交換器 1 台、液晶螢幕 1 台
- NETGEAR 無線網路 AP 1 台
- 網路語音電話伺服器 2 台

參、 問題改善與協助事項

一、 使用者端電腦

(一)作業系統更新

本次共檢測 7 台使用者端電腦，並有 4 台電腦未將安全性作業系統修補程式更新至最新版，亦發現該 4 台電腦有更新功能異常之情形，相關問題均已進行修復並完成作業系統安全性更新至最新版，相關更新項目如下：

1.解決應用系統問題及重整補強作業系統。

2.協助更新微軟作業系統修補程式。

3.協助安裝及更新 Office 修補程式。

4.協助更新套裝軟體修補程式。

(二)防毒軟體更新

經檢測發現 5 台使用者端電腦均使用試用版本之防毒軟體，另 2 台完全無安裝任何之防毒軟體，已統一安裝趨勢雲端防毒授權版並更新至最新防毒碼版本。

(三)應用系統操作協助

1.因駐舊金山雇員無法登入 EIP 辦理公務，經了解其僅申請部內 AD 之帳號及權限，並未申請 EIP 登入權限，已協助申請及設定完成。

2.因部內導入 MOTP 行動動態密碼系統，為使駐外人員熟悉及了解其操作方式，已完成操作說明教學。

(四)資訊安全作業問題

駐舊金山科技組同仁反應無法使用 HiKey 登入內網進行作業，經確認其配發之 2 支 HiKey，其中 1 支遭鎖碼，已為其進行解鎖作業，另再進行 HiKey 登入應用程式重新安裝後，均可正常使用 HiKey 登入內網作業。

(五)實體隔離電腦作業問題

1.駐舊金山科技組反應現有之使用者端電腦僅 1 台作為實體隔離及公文系統作業用，但因無網路連線故依需求協助進行作業系統、防毒軟體等更新及相關資安審視。

2.因駐舊金山科技組現行之作業方式未完全依照「外交部駐外機構資通安全作業規則」，連外電腦及實體隔離電腦作業完全區隔，故於資訊安全教育訓練課程時，要求其若有相關公務之作業於實體隔離電腦完成資

料登打後，再以 USB 隨身碟進行資料傳遞作業，並於資料傳遞後清除 USB 隨身碟之相關資料。

(六)其它

依需求進行 Office 更新作業，惟因微軟 Office 軟體及實體隔離電腦資料傳輸所需之隨身碟依規定由外交部統一配發，已建議舊金山科技組向駐外機構資安官申請撥用。

二、 依資通安全稽核項目檢核表查核電腦及人員是否符合相關規定，並協助設定電腦設備。

三、建立現有環境防護機制。

針對現有環境及系統各項弱點與漏洞進行修補程式安裝。

四、 使用者端電腦惡意程式掃描。

(一)手動掃除病毒。

(二)重新設定防毒軟體定時排程工作與每週五中午自動進行完整掃描。

(三)掃描並刪除惡意程式(後門程式、間諜程式)。

五、 網路架構及環境審視

協助了解網路架構現況(如圖 1)及針對環境因素所造成之相關問題進行審視與最佳化調整。

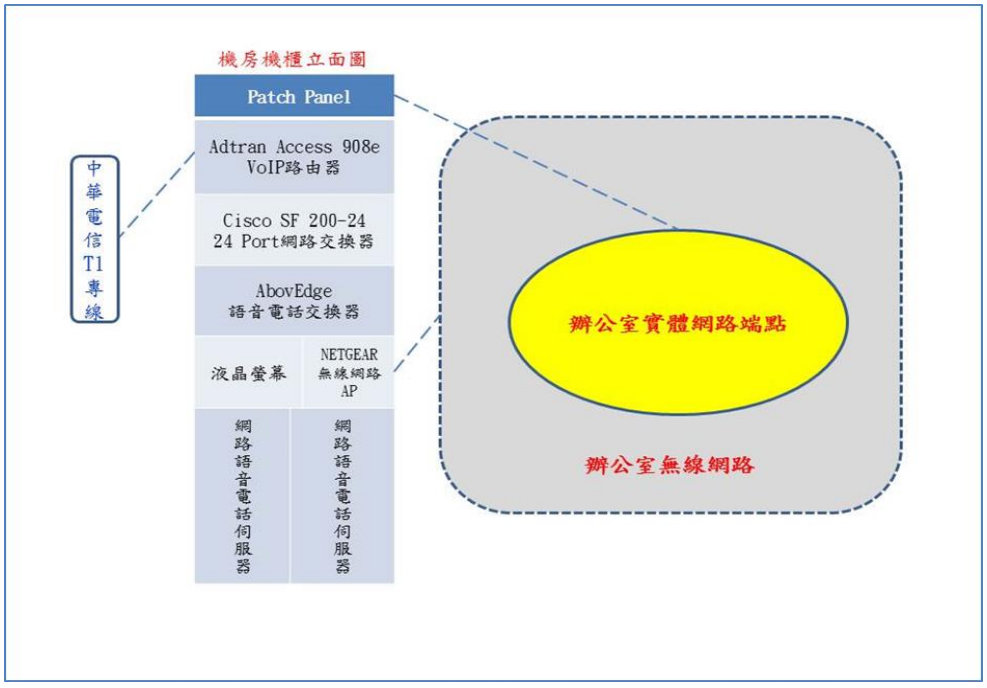

圖 1 駐舊金山科技組網路架構圖

六、 其它協助事項

(一)與該科技組討論其目前資訊設備維運與資訊架構等所遇到的問題，並提供協助或建議。

(二)為避免因印表事務機 WiFi 功能開啟且無掌控權限導致資安疑慮，已協助關閉印表事務機之 WiFi 或其它可能連網之功能。

肆、 應用系統與資訊安全教育訓練

一、主講人：薛處長大勇

二、參與人員：駐舊金山科技組所屬同仁

三、時間：107/05/22 (星期二)，上午 10 時至 12 時

四、授課內容(如附件)：

(一) 政府資安防護機制

(二) 駐外機構資安作業規則說明

(三) 資安事件應變標準作業程序說明

(四) 常易忽略之駐外資安規範提醒

(五) 非合署辦公之駐外單位資安強化措施

(六) Hi-Key 使用說明

(七) 問題與討論

圖 2 駐舊金山科技組資安教育訓練

圖 3 駐舊金山科技組資安教育訓練

伍、 建議

本次資安檢測作業可區分為「網路架構檢測」、「使用者端電腦檢測」及「安全設定檢測」等 3 項，依據檢測結果提出相關評估及改善建議如下：

一、 網路架構建議

經檢視網路架構後，發現駐舊金山科技組架構目前存在可能疑慮，相關說明如下：

(一)於辦公室內之無線網路介接於 T1 頻寬線路，若訪客使用無線網路上網且其設備有資安問題時，則易影響科技組內部網路安全。

(二)於辦公室內之整體網路僅使用一條 T1(1.54Mbps)專線，所有數據傳輸皆使用此 1.54Mbps 之頻寬進行作業，若訪客及辦公室同時上網使用，則易造成資料傳輸時頻寬阻塞。

(三)駐舊金山科技組於介接內部端點網路為直接進線，並無防火牆等類似設備，無法有效防止駭客入侵。

(四)未掌握網路交換器登入帳號、密碼，無法進行網路區域存取管理，易造成未授權人員入侵行為。

(五)已建議於辦公室另增一網路線路，以區分有線及無線網路使用，若訪客或會議室有連網需求時，則使用無線網路上網，除可避免影響辦公作業使用頻寬，亦可有效避免因外來之資安風險造成科技組之資安危害。除此之外亦建議新增防火牆等設備，完善網路防護及控管機制，降低駭客入侵之可能性。

二、 使用者端電腦建議

(一)防毒軟體

經檢視駐舊金山科技組之防毒軟體皆無完整授權(試用版本)，且其中 2 台並未安裝任何之防毒軟體，本次已統一安裝部內趨勢雲端防毒軟體，未來建議定期審查病毒防毒碼更新狀態。

(二)作業系統安全性更新

經檢測駐舊金山科技組之作業系統安全性更新狀態僅 3 台為正常更新，其餘 4 台作業系統安全性更新狀態異常，本次已進行修復並全面更新至 5 月份 Patch，建議未來每月定期審視其更新狀態。

(三)實體隔離電腦作業及機敏資料保存

經檢測駐舊金山科技組實體隔離電腦之桌面及資料夾，其中共 4 台具個資資訊之文件未妥善保存，已建議檔案勿存放於本機並進行加密封存，且若有相關公務之作業需先於實體隔離電腦完成後，再以 USB 隨身碟進行資料傳遞作業，並於資料傳遞後清除 USB 隨身碟之相關資料。

(四)電子郵件預覽關閉

經檢測駐舊金山科技組電腦之電子郵件預覽功能未設定關閉，已統一依部內規則進行 Outlook 設置，並說明社交工程電子郵件相關注意事項。

(五)非法軟體安裝

本次檢測駐舊金山科技組電腦並無安裝非法或未授權軟體，但共有 3 台安裝 Dropbox 程式，為避免資料因同步雲端時不小心外洩，已要求進行移除。

(六)安全設定檢視

因駐外同仁電腦並未套用部內群組應用原則，故此次檢測駐舊金山科技組電腦之安全性原則皆僅為預設狀態，已統一依部內「密碼及鎖定原則與螢幕保護程式安全設定」逐一設定完成。