行政院所屬各機關因公出國人員出國報告書

（出國類別：其他公務）

『赴駐美科技組進行資訊服務重整及資安檢測計畫等工作』結案報告

服務機關：行政院國科會資訊小組

出國人　職　　稱：主　任

姓　　名：李筱瑜

行政院研考會/省(市)研考會編號欄

出國地點：駐美國華盛頓科技組

出國期間：100/10/27 至 100/11/7

報告日期：100/11/30

目　　錄

壹. 前言

近年來政府機關、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更有嚴格的資安要求。

本會目前在全球各地共設有十六個科技組，初期由本小組協助建立資安防護體制而後納入外交部管理，至於郵件服務則使用國科會提供的郵件服務。而駐美國代表處科技組則係使用由其同仁自行建置電子郵件服務系統，惟多年下來因時空環境變遷及人員異動離職，目前後續維護工作已漸力不從心。

駐美國代表處科技組遂於本(100)年7月19日致函本小組，希望本小組派員前去協助改善其網際網路及電子郵件等相關資訊系統運作，並對同仁辦理教育訓練，加強其資訊通訊安全知識。

貳. 工作範圍:

一. 協助駐美代表處科技組解決電子郵件及網路維運問題。

二. 協助駐美代表處科技組解決個人電腦與周邊設備及應用系統問題。

三. 辦理教育訓練。

參. 行程

日　　期	說　　明
100/10/27(星期四)	台北 → 洛杉磯 → 華盛頓
100/10/28(星期五)	駐美國華盛頓科技組工作。
100/10/29(星期六)	駐美國華盛頓科技組工作。
100/10/30(星期日)	假日
100/10/31(星期一)	駐美國華盛頓科技組工作。
100/11/01(星期二)	駐美國華盛頓科技組工作。
100/11/02(星期三)	駐美國華盛頓科技組工作。
100/11/03(星期四)	駐美國華盛頓科技組工作。
100/11/04(星期五)	駐美國華盛頓科技組工作。 華盛頓→ 洛杉磯
100/11/05(星期六)	假日
100/11/06(星期日)	洛杉磯 → 台北
100/11/07(星期一)	抵達台北

肆. 人員

姓 名	職　　稱
李筱瑜	國科會資訊小組主任

※另有隨行專案經理與系統管理師各一名，為「本會駐外科技組資訊服務重整及資安檢測計畫」專案之得標廠商派出

伍. 需求說明

行前經 E-mail 與電話訪談，彙整駐美國代表處科技組之需求如下：

網路需求

1、目前科技組上網是與代表處共用當地電信業者線路，而自行租用的 AT&T 網路線路則只提供代表處與科技組郵件伺服器使用。由於代表處租用之線路上網速度頻寬不夠，科技組希望能轉由 AT&T 的線路上網，連接至會內 intranet 系統、國合系統、國合簡訊網等以增加效率。

郵件需求

2、將駐美代表處科技組使用之 E-mail XXX@tecrosd.org，轉換至外館的 XXX@tecro.us 郵件系統。

3、關閉科技組過去自行申請的 tecrosd.org 網域名稱。

個人電腦需求

4、離線公務用電腦速度太慢需要協助升級。

5、Office 2003 版本升級

應用系統需求

6、因應五都改制，目前秘書使用之公文系統國科會版受文者內容須更新

7、提供駐美代表處科技組網站後台更新方式(現由國科會統一管理)。

資訊安全需求

8、為加強同仁資訊安全知識，提供駐美代表處全體同仁有關資訊安全之教育訓練課程。

陸. 工作內容

一、 資訊設備盤點與環境檢測

1. 盤點辦公室資訊設備

辦公室設備

個人電腦 共13台、NoteBook共5台、印表機共11台、作業系統 XP共14套、 Windows 7共2套、linux共 2套、Office 2003 共11套 、Office 2010共 2套

機房設備（4F科技組倉庫與2F機房）

網路頻寬：下載： 1.5MKbit/Sec.上傳： 1Mbit/Sec，防火牆伺服器1台、網頁過濾伺服器1台。網站伺服器2台、郵件伺服器2台、骨幹網路交換機1台、路由器3台

盤點設備後製作資訊資產表(詳附件一)。

2. 個人電腦檢測及版本更新

- 解決應用系統問題及重整補強作業系統
- 協助更新微軟作業系統修補程式
- 協助更新 Office 修補程式
- 協助更新套裝軟體修補程式

3. 依外交部資訊安全稽核表，協助檢查資安相關設定。

4. 網路伺服器弱點掃描

- 掃描網路，確認科技組現有網路的弱點與漏洞。

5. 建立防護機制

- 針對各項弱點與漏洞進行修補程式安裝。

6. 個人電腦惡意程式掃描

- 手動掃除病毒。
- 重新設定防毒軟體的定時排程工作，如：每日更新病毒碼與每週三中午完整掃描。
- 掃描並刪除惡意程式(後門程式、間諜程式)。
- 重新掃描，確認網路及電腦的漏洞已修補完畢。

二、 問題處理

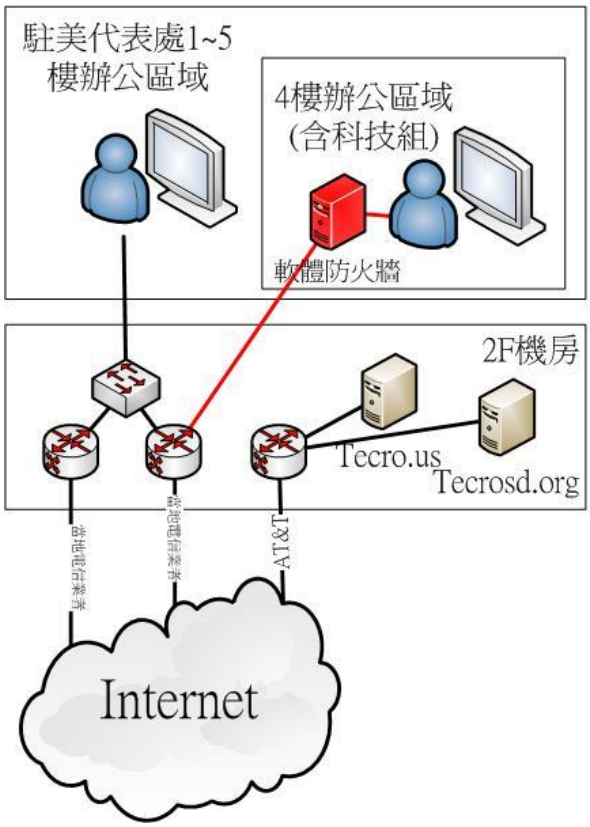
網路需求

1. 協助科技組轉由 AT&T 線路上網。

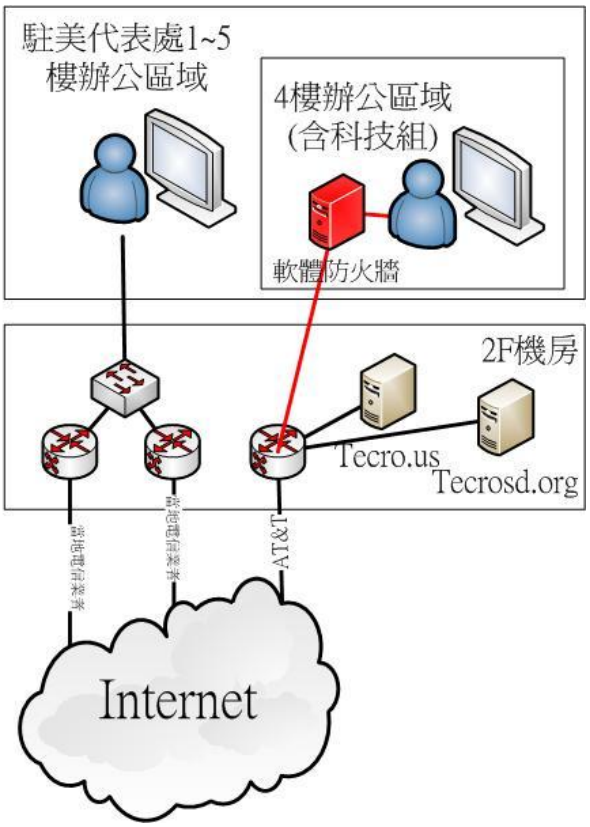
為避免影響同仁正常上班。遂於星期六由代表處 MIS 人

員陪同檢查 4 樓辦公區域與 2F 機房之間的網路線路連線，並將 4 樓辦公室網路切換至 AT&T 線路。

移轉前



移轉後



郵件需求

2. 協助組長上網電腦與隔離電腦對換，協助資料移轉、周邊設備設定、設定 E-mail 可同時收發 Tecrosd.org，Tecro.us。另外備份 Tecrosd.org 過去的全部郵件並燒錄於光碟片內。

個人電腦需求

3. 筆記型電腦、個人電腦共 8 部未更新病毒碼。

主要因實體隔離，筆記型電腦平時未連上網路，所以無法更新病毒碼，現場已透過手動的方式下載病毒碼，並

執行完整掃描。

4. 筆記型電腦、個人電腦共 18 部未更新作業系統修補程式

因為作業系統預設自動安裝的時間設定為凌晨 3:00，但該時段並非辦公時間電腦沒有開機，所以無法自動下載安裝修補程式。已手動安裝全部的修補程式 hotfix 後，設定自動更新時間於每週四中午 12 點。

5. 個人電腦設定的密碼過於簡單。

已於資訊安全座談會中，說明密碼的使用規則、如何建立密碼、密碼的更換週期，以及妥善保存個人密碼的方式。

6. 個人電腦 7 部運作效能緩慢，影響正常業務。

趙博士的公務電腦記憶體不足，已經更新為 1GB。秘書電腦記憶體不足，已向當地網管人員借調記憶體 1GB 暫時先裝上。其他效能不足的主機均已標示，待採購後安裝。

7. 完成 3 部電腦故障排除。

(1). 趙博士電腦無法開機，先備份電腦內重要檔案後再重新啟動。

(2). 組長公務電腦異常當機，記憶體更換後，狀況已改善。

(3). 副組長公務電腦不穩定容易當機，更換電源供應器後已改善。

8. 完成 2 台辦公室 Office2003 升級至 2010。

提供 Office 2010 版本安裝光碟與安裝步驟說明書給秘書，並現場將組長與雇員上網 NB 更新至 Office 2010 版本。

應用系統需求

9. 完成 2 部電腦國科會版公文文書製作軟體安裝。

   (1). 更新林秘書公務電腦公文文書製作的機關代碼，解決無法顯示部分收文機關的代碼的問題。

   (2). 副組長公務電腦重新安裝公文文書製作軟體。

10. 蒐集駐美代表處科技組網站需求。

三、 其他協助事項

1. 代表處 4F AT&T 網路線路防火牆記憶體升級。發現防火牆記憶體使用滿載，提供記憶體由 512MB 升級至 1GB。

2. 100 年 10 月 31 日星期一代表處與其他各組反應無法收發信件。經現場檢測結過發現，tecro.us 網域名稱已逾期，通知代表處 MIS 部門與當地業者聯繫。

3. 完成 2 部電腦的公文系統安裝(外交部版本)。利用閒置的舊電腦一台，重新安裝作業系統及外交部版本的公文系統，放置於副組長辦公室內，另於趙博士的公務電腦內，安裝外交部版本的公文系統。

4. 提供會內補助學者專家及研究生出席國際會議及補助出國進修人員等系統之各項資料，已於出發前與國內應用系統彙整後提供，未來將與系統承辦人討論是否建立介面供科技組同仁自行下載。

5. 與駐美代表處行政組開會，討論其目前資訊設備維運與資訊架構等所遇到的問題，並提供建議(詳附件二)。

四、 應用系統教育訓練與資訊安全座談會

1. 資訊安全座談會。

講　　員　：李主任筱瑜、陳信翰管理師

參與人員：駐美代表處共 37 位同仁參加

時　　間：100/11/03（星期四)15:00-16:30

簡報內容詳如附件三

2. 應用系統教育訓練

講　　員：陳信翰

參與人員：林秘書寶玉

時　　間：100/10/28（星期五）10:00-11:30

執行方式　：採一對一方式於秘書電腦上實地操作，並針對問題進行操作教學與解答。

柒. 建議

1. 筆記型電腦不常開機，以及實體隔離電腦未連網，以致未能定期更新修補程式，易造成資安漏洞。未來應於筆記型電腦開機時，先上網更新電腦病毒碼；實體隔離電腦則可每周上網下載病毒碼更新。(更新步驟詳見教育訓練光碟內，離線病毒碼下載步驟)

2. 目前科技組部分 PC 過於老舊效能較差，造成日常工作困擾，建議電腦記憶體均升級至 2G，包含趙博士的公務電腦、秘書的上網電腦、副組長的三台電腦、顧問及其他同仁的上網電腦。公用區電腦因目前沒有使用，建議報廢。

3. 關閉 tecrosd.org 網域名稱服務

   由於 tecrosd.org 網域名稱下提供 tecro.us 網域服務以及 mail.tecrosd.org 郵件服務，所以在關閉 tecrosd.org 網域名稱之前，必須先完成下列二項工作。

   (1). 建置 tecro.us 網域服務

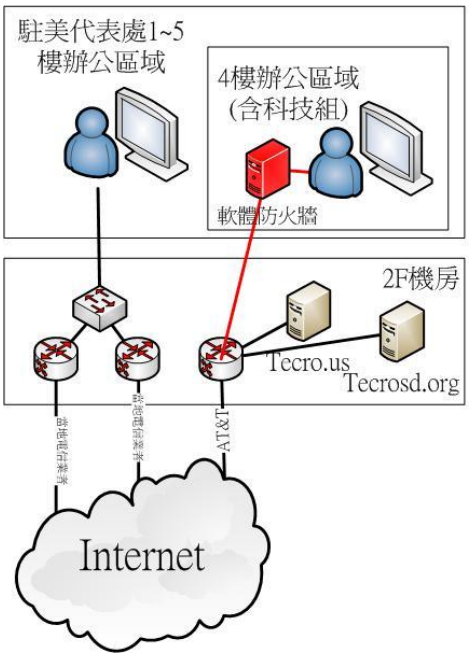
   於駐美代表處二樓機房利用一台伺服器或由虛擬化伺服器另行建置 tecro.us 網域服務，並到原申請 tecro.us 網域的單位更改路徑設定。

   (2). 關閉郵件服務：mail.tecrosd.org

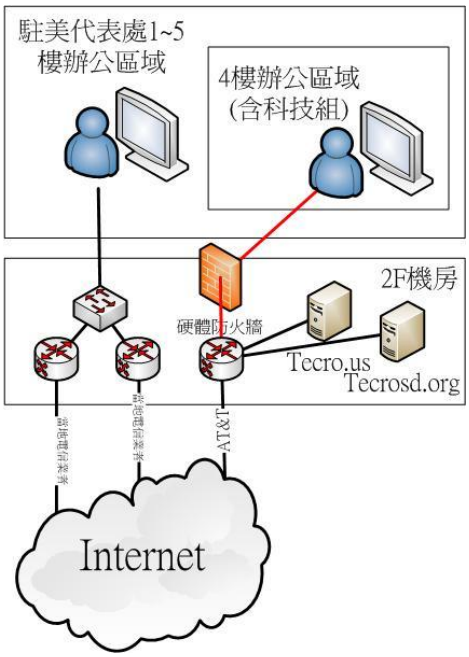
   目前科技組同仁均設有 tecrosd.org 及 tecro.us 兩個郵件信箱，建議自即日起對外通知一律使用 tecro.us 作為收發信箱，而不再使用 tecrosd.org。至於 tecrosd.org 信箱則持續觀察約 3-6 個月後，確定該信箱沒有新的信件即可關閉。

4. 目前 4 樓辦公區域之個人電腦均透過一軟體防火牆連到 Internet，此防火牆為一早期自網路上取得之免費開放軟體 ipcop，安裝於科技組一台老舊 PC 之 linux 作業系統上。因免費開放軟體沒有任何公司可提供保障與維護更新，而同仁亦無能力維護，目前實際防護效果有限，建議採購硬體式防火牆取代現有設備，並調整線路將其放置於 2 樓機房集中維運管理，以利後續維運。

防火牆現況



未來建議



捌. 總結

此次本小組已協助完成將駐美代表處科技組之郵件服務改與駐美代表處為同一套系統，同時未來四樓軟體防火牆如能改採用坊間現成之防火牆設備放置於二樓機房，則科技組未來即不再需投入專職人力維護而回歸由代表處統一維護管理，如此可解決困擾科技組多年來維護資訊設備之問

題，而原有的維護人力即可釋出專責於科技組之工作。

至於個人在工作上則應具有一定之資訊安全素養，不僅要注重電腦設備的資安防護、定期更新，更重要的在於資訊安全措施的落實執行。

駭客入侵與攻擊手法不斷創新，現有的各種防護並無法即時處理，因此惟有同仁遵守外交部資訊安全要求與規定，落實公務業務使用實體隔離電腦，妥善存放機敏公務資料等，才能減少資安事件的發生，並在資安事件發生時，降低業務上的衝擊。

目前資訊小組定期在本會Intranet內的「資訊安全政策」網站提供有最新之資安訊息，建議駐外科技組同仁可隨時上網瀏覽，而資訊小組未來也會不定期發出資訊安全相關信件，以提升同仁的資安防護能力。

玖. 附件

附件一　資訊資產表

附件二　行政組資訊架構建議

附件三　教育訓練文件