行政院所屬各機關因公出國人員出國報告書
（出國類別：考察）

駐外科技組資訊安全體系輔導建置計畫（第二期）結案報告（第二組：駐美東與加拿大科技組）

服務機關：行政院國科會資訊小組
姓名職稱：孫國庭設計師
派赴國家：美國、加拿大
出國期間：96/3/28~96/4/9
報告日期：96/5/1

目　　錄

壹、緣起

資訊社會中，政府機關、民間企業及個人等普遍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，因此外交部對事涉國家外交最前線之各駐外單位提出實體隔離等資安要求。但本會目前分布於美加地區之六個駐外單位，受限於有限之人力、經費，再加專業知識之不足，雖然當地資訊科技進步，各種資訊專業人才眾多，若有任何資安問題發生，容易就近找到專業技術人力支援協助，但是，基於實際業務之機密性質考量，本會仍需定期派員檢核其資訊安全實施成效，並針對最新資訊安全技術和本會應用系統辦理教育訓練，以協助其建立完備之資訊安全作業環境。

貳、目標

一、積極防衛資通設施，維護業務正常運作。

二、主動偵測安全威脅，降低實質危害因素。

三、建構安全通報體系，強化事前預警機制。

四、保障個人隱私權益，促進網路多元發展。

參、實施方式

96年將對於美國與加拿大六個科技組辦理資訊安全稽核計畫：

第一組 駐美西地區科技組

包括駐洛杉磯、舊金山、休士頓等三個科技組。

第二組 駐美東地區與加拿大科技組

包括駐華盛頓、芝加哥、渥太華等三個科技組。

駐美加地區之科技組，由於當地資訊科技進步，各種資訊專業人才眾多，若有任何資安問題發生，較易就近找到專業技術人力支援協助，故本會只需定期派員檢核其資訊安全實施成效，並針對最新資訊安全技術和本會應用系統辦理教育訓練。

肆、工作行程

日　期	說　　明
96/3/28(星期三)	搭機離台赴美國芝加哥。
96/3/29(星期四)	於芝加哥科技組工作。
96/3/30(星期五)	於芝加哥科技組工作。
96/3/31(星期六)	自由活動。
96/4/01(星期日)	搭機離美轉赴加拿大渥太華。
96/4/02(星期一)	於渥太華科技組工作。
96/4/03(星期二)	於渥太華科技組工作。
96/4/04(星期三)	搭機離加轉赴美國華盛頓 D.C.。
96/4/05(星期四)	於華盛頓科技組工作。
96/4/06(星期五)	於華盛頓科技組工作。
96/4/07(星期六)	自美國華盛頓 D.C.返台
96/4/09(星期一)	抵達桃園國際機場。

伍、參加人員

姓名	職稱	公司
孫國庭	設計師	行政院國家科學委員會資訊小組
連志強	技術部副理	三蔚企業有限公司

陸、計畫執行

主要工作順序區分如下：

一、蒐集相關資訊

爲蒐集各駐外科技組資訊安全執行狀況與資訊設備的數量，以及各單位目前所面臨的問題，特於行前透過 E-mail 寄送資訊設備與環境現況調查問卷（如附件一），請各駐外單位填寫。調查結果如下:

(一).硬體設備：各單位資訊相關設備數量如下表

設備現況 （科技組）	桌上型電腦(台)	筆記型電腦(台)	印表機(台)	掃描器(台)	無線網路
芝加哥	7	1	5	1	0
華盛頓	8	2	7	3	1
渥太華	3	2	5	2	1

(二).網路環境

各單位經由內部網路相互連線，以達資源共享，對外係以 ADSL 撥接上網，網路頻寬約爲（1MB~2MB），與本會或其他機關進行資訊互通交流。

(三).辦公室套裝軟體

- ✧ MS Windows 2000、MS Windows XP
- ✧ MS Office 2000、MS Office XP、MS Office 2003
- ✧ MS IE
- ✧ 其他：防毒軟體、壓縮軟體、PDF writer

(四).應用系統使用現況（統計時間：2006/01~2006/12）

駐 外 單 位	電子收文 (資料筆數)	電子發文 (資料筆數)	國合簡訊網 (被審核通過且上線的文章數量)	海外學人資料庫（資料筆數）	工作月報(資料筆數)
駐加拿大科技組	72	12	139	17	324
駐芝加哥科技組	38	4	192	0	324
駐華盛頓科技組	97	29	51	0	324
合計	207	45	382	17	972
註：新聞剪影資料共 245 筆資料（統計期間：2006/01~2006/12）					

(五).資訊安全維護現況

爲了解各科技組對資訊安全基本維護項目之執行狀況，資訊小組於行前透過 E-MAIL 寄送資訊安全自評表（如附件一）請其填寫。

經各單位自評後得知，各單位之電腦均裝有防毒軟體並定期更新病毒碼；另外微軟作業系統部份科技組有定期安裝修補程式；且普遍未安裝木馬掃描軟體，及弱點掃描軟體，有漏洞存在也完全不知。

(六).目前所面臨的問題

硬體 - 由於部分科技組電子信箱缺乏資訊安全軟體保護，作業系統中毒、或遭到木馬程式植入，另外部分使用無線網路的科技組，相關安全設定與使用者控管不足(如傳輸加密協定)。

軟體 - 部分駐外科技組之微軟系統相關軟體授權數不足、缺少安裝光碟片。

資安 – 部分駐外科技組之訊安全措施均有遺漏不足之處，又因單位內資訊缺乏資通安全技術及網路人力，在問題的處理上往往困難費時。

二、現場稽核建置

(一).資訊安全稽核

由本計畫人員親至各駐外科技組，依據資訊小組設計之資訊安全稽核表(如附件二)，針對每壹台電腦逐項檢查其執行狀況，以實際了解各駐外科技組資安狀況。

(二).建置資訊安全架構

依下列資訊安全工作逐項完成建置(或補足建置)，並透過說明確保同仁日後能自行完成以下工作。

1. 弱點掃描(確認網路及電腦待修補的漏洞)
   - ✧ 使用微軟基本安全性分析軟體掃描 (MBSA)掃描網路，了解科技組現有網路的弱點與漏洞。
2. 建立防護機制 (安裝修補程式)
   - ✧ 針對各項弱點與漏洞進行修補程式安裝。
   - ✧ 修補程式更新 (Hot Fix、Service pack)
   - ✧ 安裝、啓動並設定軟體防火牆
3. 掃描與刪除
   - ✧ 病毒掃描與手動清除。
   - ✧ 重新設定防毒軟體與排程更新病毒碼與掃描。
   - ✧ 惡意程式掃描(後門程式、間諜程式) (Microsoft Defender)
   - ✧ 透過 3~4 種掃描軟體交錯掃描。
   - ✧ 登錄檔檢查

✧ 可疑檔案檢查

✧ 蒐集可疑檔案與 log 送回資訊小組進行分析。

4. 重新掃描(確認網路及電腦的漏洞已修補完畢)

(三).教育訓練

課程大綱如下(詳如附件三)：並依照資訊安全稽核結果較弱之處，加強訓練。

1. 基礎資訊安全工作（搭配資訊安全維護與操作手冊）

✧更新微軟軟體修補程式(OS、Office…)。

✧掃毒軟體定期更新、定期掃描。

✧木馬程式掃瞄（Microsoft Defender）。

✧啓動防火牆。

✧檢查資訊安全相關設定 Microsoft MBSA

2. 機密資料傳輸

✧ 實體隔離

✧ Winzip

3. 資訊安全注意事項

(四).其他問題處理

- 資訊業務相關應用系統安裝與故障排除，作業系統效能調整。
- 協助安裝常用基本之應用軟體(各單位提供有版權之光碟片)

(五).支援協助外交部其他各組處理資訊相關問題

三、設備採購

由於國內資訊設備價格低廉、品牌多、品質好，故部分駐外科技組請資訊小組代為採購以下設備，並隨行攜至各科技組。

(一).加拿大：HP 筆記型電腦一台，Microsoft Select License 之Windows XP、Office 2003 一套。

四、回國後後續工作

(一).不定期接受電話、E-mail 諮詢資訊相關問題

(二).每月資訊安全更新通知

(三).提供重大資訊安全事件即時警訊(E-mail)

另外科技組對部份應用系統之相關問題與建議，資訊小組於回國後會依其需求修改更新。

柒、問題與建議

(一).駐芝加哥科技組

✍ 問題：

- 實體隔離電腦防毒軟體過期、病毒碼未更新。
- 連網電腦帳號、密碼的設定過於簡單或與帳號相同，安全性不佳。
- 連網電腦 MS Office hotfix 未更新。
- 未安裝木馬掃描軟體，及弱點掃描軟體。

✍ 建議：

- 已協助更新完成實體隔離電腦防毒軟體，建議日後應有專人負責是項工作。
- 對帳號、密碼的設定應考量長度及複雜性(如密碼 8 碼、字元包含大小寫與特殊符號)確保密碼強度，以增加系統使用安全性。
- 已協助安裝木馬掃描軟體，及弱點掃描軟體，現場掃瞄無發現木馬軟體。

(二).駐渥太華科技組

✍ 問題：

- 部分電腦操作使用時，反應非常緩慢。
- 無線網路僅使用 802.11b，提供平常五部聯網電腦使用，頻寬經常吃緊不敷使用。而且附近均爲無線網路環境，若有 802.11g 者，則更易受到干擾而效能大打折扣。
- 無線網路使用 WEP 加密，安全性不佳。
- 連網電腦帳號、密碼的設定過於簡單或與帳號相同，安全性不佳。
- 連網電腦並未更新到 Windows XP sp2 與其他相關 hotfix，MS Office hotfix 亦未更新。
- 電腦作業系統仍有部分爲多國語言版之 Windows XP Media Center Edition 版本，此爲家用多媒體版本而非辦公室版本。
- 未安裝木馬掃描軟體，及弱點掃描軟體。
- 實體隔離電腦防毒軟體過期、病毒碼未更新。

✍ 建議：

- 經過實地勘查的結果，發現大部分電腦病毒碼雖有更新但修補程式未更新，且遺漏了 Office 更新。
- 針對效能緩慢的電腦，除增加記憶體外，建議移除不必要的常駐程式，並重新安裝電腦 OS。
- 針對無線網路頻寬不敷使用，除建議更換 802.11g 和 WPA 加密規格的設備外，考量辦公室環境分佈在相同樓層，建議架設實體線路以確保安全。
- 對帳號、密碼的設定應考量長度及複雜性(如密碼 8 碼、字元包含大小寫與特殊符號)確保密碼強度，以增加系統使用安全性。

- 經協助安裝 Windows 與 Office 之更新程式，但仍有部份電腦安裝過程失敗無法順利完成更新，形成防護漏洞，針對這些電腦，建議重新安裝，以確保整體資安環境正常。

- 爲了方便管理與提升作業系統功能和安全等級，建議將部份仍使用 Windows XP Media Center Edition 的家用多媒體版本作業系統重新安裝爲 Windows XP Professional with sp2 版本。

- 已協助安裝木馬掃描軟體，及弱點掃描軟體，現場掃瞄發現木馬軟體，部份電腦可以移除木馬，無法移除木馬者，重新安裝作業系統。但是仍有 2 部電腦無法順利安裝木馬掃描軟體，可能形成資安漏洞，建議重新安裝該部電腦之作業系統。

- 已協助更新完成實體隔離電腦防毒軟體，建議日後應有專人負責是項工作。

(三).駐華盛頓科技組

✍ 問題：

- 帳號、密碼的設定過於簡單，安全性不佳

- 未安裝木馬掃描軟體，及弱點掃描軟體。

✍ 建議：

- 對帳號、密碼的設定應考量長度及複雜性，以增加系統使用安全性。

- 已協助安裝木馬掃描軟體，及弱點掃描軟體，現場掃瞄無發現木馬軟體。

捌、結論

一直以來本會各駐外科技組均無資訊專業人員編制，設備損壞時無法自行維護，送外修護又恐資訊外洩；當遇到各種資訊病毒與駭客攻擊時，也無法辨識處理。

因此本會此次特別安排資訊小組人員赴各科技組，現場輔導協助其建置資訊安全環境，同時解決各項資訊相關問題，並對其人員進行教育訓練，以期許未來各科技組能自行持續執行資訊安全工作。

然而駭客手法日新月異日，新變種病毒層出不窮。經由此次之輔導與訓練，各科技組短期內應可維持正常運作；但長期來看，即使有資訊小組透過電話 E-mail 之方式提供各種諮詢服務，但因溝通上之距離與專業認知之差距，一定仍會有無法解決之問題。因此建議本會未來仍須定期派員赴各科技組到場協助資訊安全相關工作，以確保各科技組之資訊業務順利運作。

玖、附件

附件一　駐外科技組資訊設備與環境現況調查表、資訊安全自評表

附件二　資訊安全稽核表

附件三　教育訓練文件