駐舊金山科技組
資安教育訓練

主講人：薛大勇

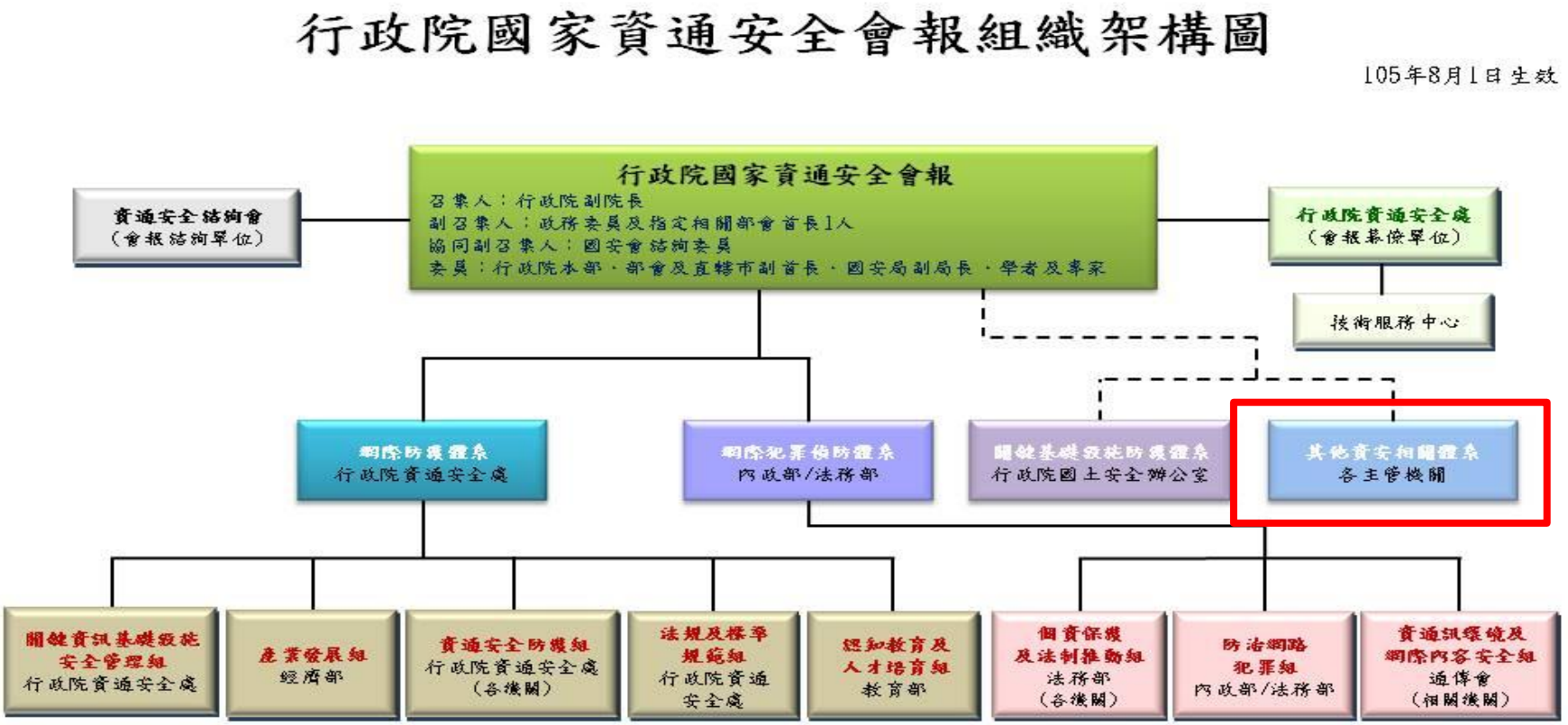
107年5月

大綱

資安教育

- 政府資安防護機制
- 駐外機構資安作業規則說明
- 資安事件應變標準作業程序說明
- 常易忽略之駐外資安規範提醒
- 非合署辦公之駐外單位資安強化措施
- HiKey使用說明
- 問題與討論

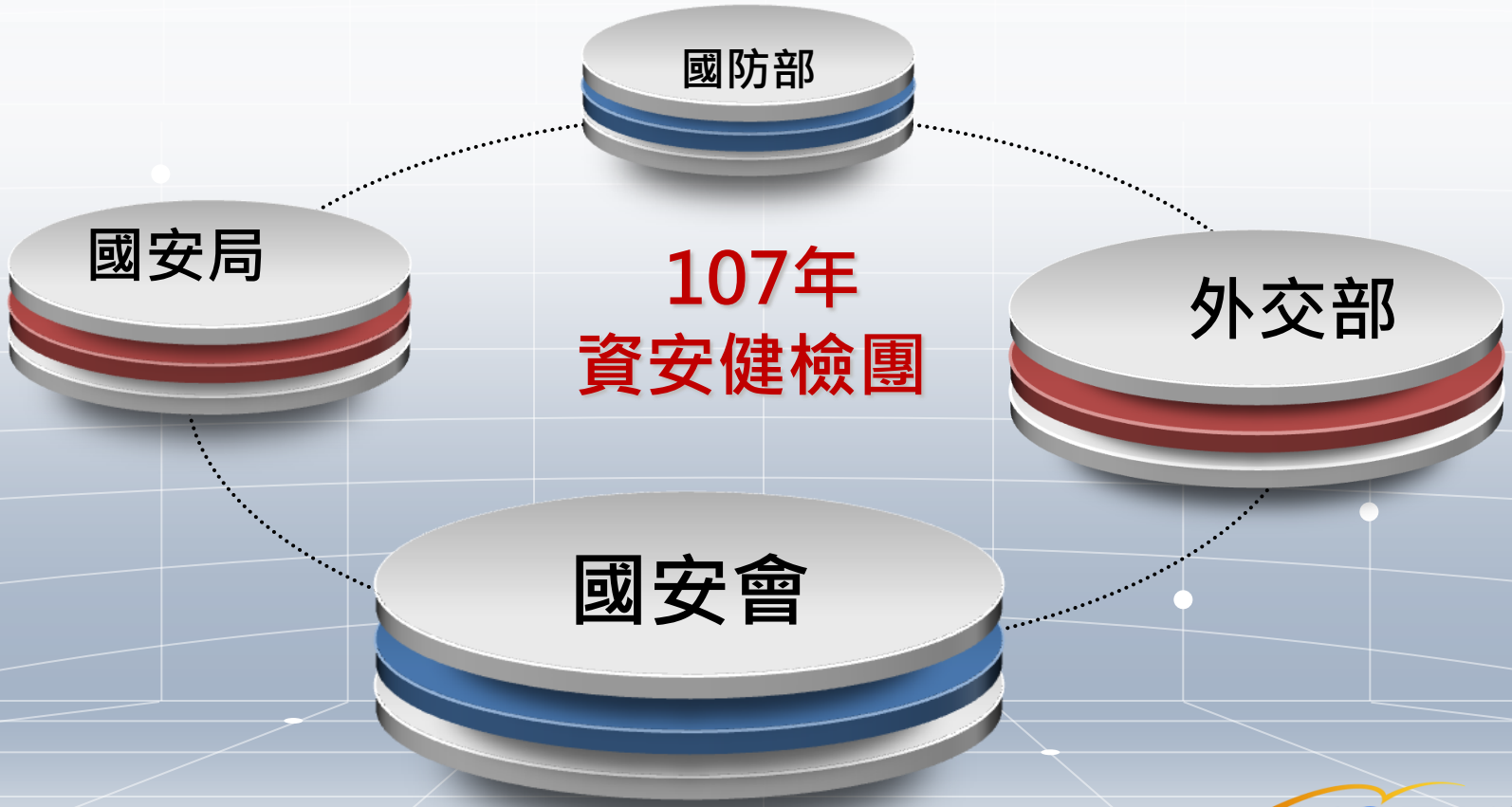
政府資安防護機制(1/2)



＊ 外交部–外館網際防護體系會報，訂定〔駐外機構資安作業規則〕

政府資安防護機制(2/2)

行政院國家資通安會報針對國家外交最前線之駐外單位，要求強化資安管控，並由國安局定期派員稽核。



駐外機構資安作業規則說明(1/15)

一、目的

為健全各機關駐外機構資通安全環境，**強化駐外人員資通安全程度及認知，防止人為疏失、蓄意破壞 或機密資料外洩等情事發生，確保駐外機構電腦設備、資料、系統及網路安全，** 特訂定本規則。

二、適用範圍

本規則主要規範駐外機構公務作業相關資通安全責任，**各駐外人員（含雇員）應落實執行**。如有違反者，請各派遣機關依相關法規懲處。**各駐外館處所有公務電腦，除專機專用之領務及電務電腦外，均有本規則之適用。**

駐外機構資安作業規則說明(2/15)

三、密碼管理規定

(一)系統之**登入帳號必須設定密碼**，並**應啟用螢幕保護程式密碼**保護之。

(二)密碼長度、密碼更換及螢幕保護程式啟用時間等規則，依據**「政府組態基準」(Government Configuration Baseline ,GCB)**設定辦理。

(三)**不得啟用自動記憶帳號及密碼之功能。**

駐外機構資安作業規則說明(3/15)

四、實體隔離規定(1/2)

(一)**實體隔離電腦專用於公務作業**，禁止私接上網，**上網電腦專用於上網瀏覽資訊或電子郵件。**

(二)實體隔離電腦製妥之文件如需利用網際網路傳輸或上網電腦下載之文件需複製至實體隔離電腦使用時，須先將 文件複製到「**上網電腦專用隨身碟**」，再移至目的電腦。此等媒體僅當作兩部電腦間檔案傳送之「載具」，**使用前、後應以格式化方式刪除所有檔案。**

駐外機構資安作業規則說明(4/15)

四、實體隔離規定(2/2)

(三)**實體隔離電腦不可移作他用**，上網電腦變更用途為實體隔離電腦時，須先將電腦硬碟格式化並重新安裝作業系統。

(四)**資料之加解密須在實體隔離電腦進行**。

(五)實體隔離電腦與上網電腦**不得共用印表機**。

(六)實體隔離電腦與上網電腦**可視情況使用簡易型KVM切換器**(僅具鍵盤、螢幕及滑鼠切換功能，不含連網或影音端子等功能)以共用螢幕、鍵盤、滑鼠。

駐外機構資安作業規則說明(5/15)

五、網際網路管理規定(1/4)

(一)上網電腦**禁止瀏覽非法或機關所限制之網站**。

(二)**機密性或敏感性資料須以主管機關認可之加密機制於實體隔離電腦加密後方可在網際網路上傳送**。

(三)**個人私用之e-mail不得傳送公文或公務連絡**，收發公務電子郵件時，**瀏覽器須關閉郵件預覽之功能**。公務電子郵件信箱使用應遵循**「駐外機構公務電子郵件信箱使用原則」**。

駐外機構資安作業規則說明(6/15)

五、網際網路管理規定(2/4)

(四)電腦應避免24小時開機，不使用時即關機或離線。

(五)**辦公室內禁止架設、使用無線網路。**但已建置「跨國骨幹網路」專網之駐外機構，須先經館長核可，並由資安官填妥申請表通報外交部資訊及電務處登錄後，以手持行動裝置經由鎖網卡唯一序號(MAC Address)註冊方式連網者，不在此限。

駐外機構資安作業規則說明(7/15)

五、網際網路管理規定(3/4)

(六)機敏場所如非業務需要，禁止安裝網路攝影機等視訊會議設備。

(七)**出差使用有線或無線網路時，應遵守第四點關於「實體隔離」及第七點「資料保護」等相關規定。**

(八)**用於列印之相關設備**，如多功能事務機、印表機及影印機等如具無線功能，購置安裝時，**須即關閉（deactivate）無線功能。**

駐外機構資安作業規則說明(8/15)

五、網際網路管理規定(4/4)

(九)供同仁借用之筆記型電腦或行動裝置須有專人管理，並區分上網使用及處理公務用（實體隔離)，上網使用之設備須避免處理公務，設備歸還後須進行系統重灌或還原。

(十一)**禁止開啟連網資訊設備(包括上網電腦、多功能事務機、印表機及影印機等)之遠端連線功能**。但經外交部或派遣機關核准，以安全連線方式連至駐外機構上網電腦進行遠端維修或系統設定，並在使用完畢即關閉連線者，不在此限。

駐外機構資安作業規則說明(9/15)

六、軟體使用規定

(一)**禁止下載、安裝或使用未經授權來路不明之軟體。**

(二)禁止私自安裝非法或來路不明軟體。**因業務需求申請安裝之軟體，須經組長核准辦理。**

(三)上網電腦應隨時線上**更新修補Windows、Office、Adobe Reader、Adobe Flash Player及Java等相關應用軟體漏洞及防毒程式病毒碼；實體隔離電腦應至少每週以人工更新防毒程式病毒碼。**

(四)禁止安裝及使用P2P分享軟體。

(五)各駐外機構**應架設「公共掃毒平台專用電腦」**，安裝配發之防毒軟體，**並定期更新防毒程式病毒碼。**

駐外機構資安作業規則說明(10/15)

七、資料保護規定(1/2)

(一)機密性或敏感性資料**須以主管機關認可之加密機制加密後儲存於光碟、磁片、外接式硬碟等可攜性媒體或實體隔離電腦硬碟中，並妥善保存。**

(二)移交電腦時，**應先將電腦硬碟格式化**、重新安裝作業系統。

(三)禁止使用上網電腦處理機密性或敏感性公務。

(四)禁止使用網路芳鄰共享資料夾。

(五)各項重要資料，**均應做妥善之備份，並定期檢測**，以確保備份資料之可用性。

駐外機構資安作業規則說明(11/15)

七、資料保護規定(2/2)

(六)各種具備**發送信號之行動裝置**(含穿戴裝置、智慧型手機、平板電腦等)**一律禁止私接公務電腦**。

(七)**公務用資訊設備**(含桌上型電腦、筆記型電腦、平板電腦、印表機、掃描器、外接硬碟、隨身碟等)**及網路架構相關設備**(含防火牆、VPN、網路交換器等)除專案、維修或出差外，**一律禁止攜出辦公場所**。資訊設備維修須遵照本規定第九點辦理。

(八)**禁止將私人資訊設備連接館處公務網路。**

駐外機構資安作業規則說明(12/15)

八、儲存媒體使用規定

(一)公務用可攜式儲存媒體之使用應遵守**「駐外機構公務用可攜式儲存媒體使用規定」**。

(二)報廢時，承辦人須會同資安官及兼辦政風業務人員辦理，**運用消磁設備或人力破壞方式進行報廢儲存媒體作業**，人力破壞方式如使用鐵鎚敲擊法破壞，拆開硬碟透過鐵鎚敲擊硬碟碟片（碟片應適當包覆確保操作人員安全），**須造成碟片破碎或嚴重刮傷變形，以保證資料無法被讀取**。為求銷毀程序周延確實，**執行銷毀作業時應以當天日期駐地報紙或列印當日電子報墊底拍照(或錄影)並具函報部**。

駐外機構資安作業規則說明(13/15)

九、資訊設備委外維護（修）規定

(一)各駐外機構**應洽請廠商查核維修人員背景**並提供相關資料。

(二)廠商在駐外機構內執行資訊設備委外維修護任務期間，**該資訊設備之使用者須全程陪同監督。**

(三)電腦資訊設備因維修必須攜出駐外機構時，**應先拔除該電腦硬碟，並由使用者負保管之責。**

(四)專用電腦部分（如領務專用電腦、電務專用電腦）請依所屬機關(單位)規定處理。

駐外機構資安作業規則說明(14/15)

十、資安課程規定

(一)依據行政院「政府機關(構)資通安全責任等級分級作業規定」，**駐外人員每年應接受至少3小時資安課程**，並於課後參加測驗，上課時數與分數列入考績參考。

駐外機構資安作業規則說明(15/15)

十一、駐外機構雇員不論國籍，均不得辦理機構內電務工作及eClient電子公文收發相關業務，或電腦系統及電子郵件帳號密碼管理、網路及防火牆管理等涉及機構網路架構及公文傳輸之資訊設備業務。

十二、駐外機構應成立「資通安全會報」，由館長（或副館長）擔任召集人，定期集會，向同仁宣達資安相關規定及近期通電、通函或案例，由館長指派主事級以上同仁為資安官協助辦理。**遇有資通安全事件，應依「駐外機構資安事件應變標準作業程序」辦理。**

常易忽視之駐外資安規範提醒

外交部

駐外機構資通安全作業規則

資料保護規定

7-3禁止使用上網電腦處理機密性或敏感性公務。

資料保護規定

7-1機密性或敏感性資料須以主管機關認可之加密機制加密後儲存於光碟、磁片、外接式硬碟等可攜性媒體或實體隔離電腦硬碟中，並妥善保存。

軟體使用規定

6-1禁止下載、安裝或使用未經授權來路不明之軟體。

網際網路管理規定

5-2機密性或敏感性資料須以主管機關認可之加密機制於實體隔離電腦加密後方可在網際網路上傳送。

5-9供同仁借用之筆記型電腦或行動裝置須有專人管理，並區分上網使用及處理公務用（實體隔離），上網使用之設備須避免處理公務，設備歸還後須進行系統重灌或還原。

非合署辦公之駐外單位資安強化措施(1/3)

非合署辦公

駐舊金山科技組

駐德科技組

落實駐外機構資通安全作業規則

加強數位線上課程及課後評量

駐外業務單位加強業務巡檢複評

定期指派本部或行政院資安處認可之資安人員稽核

非合署辦公之駐外單位資安強化措施(2/3)

技術面資安強化措施

調(派)任前及回國述職教育訓練

- 駐英科技組
- 駐法科技組
- 駐以色列科技組
- 駐印度科技組
- 駐休士頓科技組

- 外交部MPLS VPN管控
- Hi-key資安權限控管
- 停用軟體式SSL VPN
- 網路連線紀錄稽核

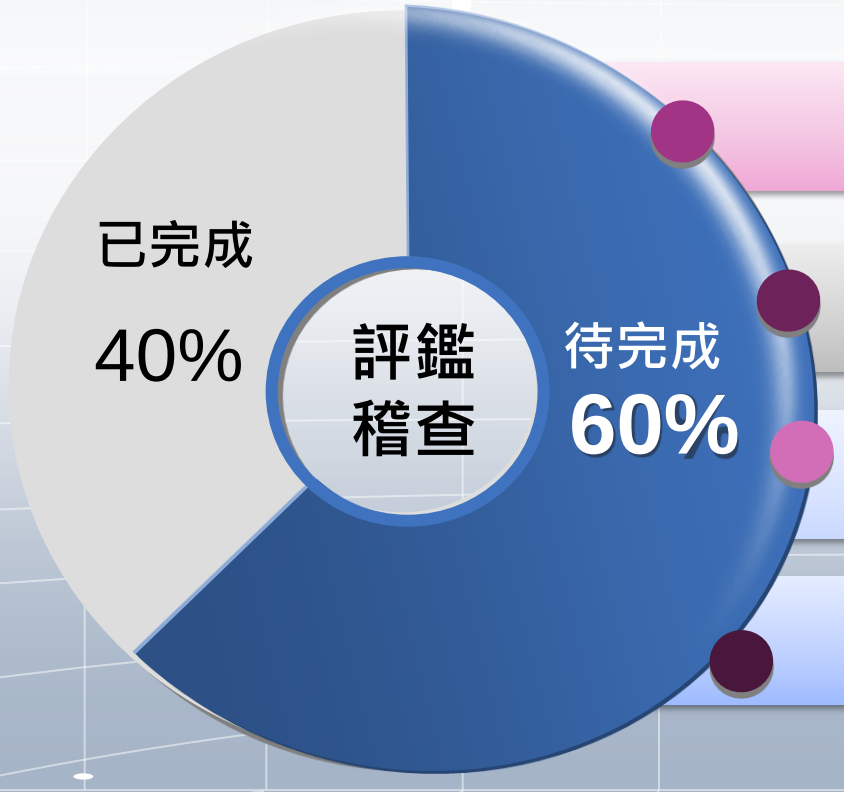
非合署辦公駐外科技組資安查核

- 駐舊金山科技組-5月
- 駐德科技組-6月
- 查核業務
  - 電腦/網路資安健診
  - 人員資安教育訓練

未來評估鎖定駐外科技組連線設備(限MAC 位址)

非合署辦公之駐外單位資安強化措施(3/3)

技術面　管理面　評鑑稽查



- 駐外科技組自評
- 主管機關評鑑
- 數位課程線上評量
- 電腦軟硬體設備 ---> 外交部權責區分

資安事件應變標準作業程序說明(1/2)

當駐外館處發現資安事件時，請依「駐外機構資安事件應變標準作業程序」進行通報，說明如下：

通報
(駐外或資電處執行)

- 自行發現：通知外交部資電處及本部資訊處
- 他機關發現：將通報受駭駐外館處

處理
(駐外執行)

找出受駭電腦→拔除該受駭電腦網路線→確認有無違反資安規定事項→3天內將受駭硬碟及「駐外機構資安事件損害管制調查表」寄回，並電陳外交部資電處及本部資訊處

資安事件應變標準作業程序說明(2/2)

後續處理
(資電處及資訊處執行)

(一)外交部接獲通報後，須於1小時內至通報應變網站通報登錄資安事件。

(二)受駭硬碟進行判讀或鑑識處理。

(三)將電腦遭駭之處理情形陳報。

(四)通電駐外機構周知及重申應遵守之相關資安規定事項，並請駐外機構自行全面資安稽核，加強資安防護。

懲處

確認責任歸屬、洩密等級及違規情節等，於奉核後移送政風處簽辦懲處。

HiKey使用說明

- ✓ HiKey 提供網路加密連線，權限仍依使用者角色區分
- ✓ HiKey 配發由主管人員依業務實需授權使用
- ✓ 本部依ISMS資安規定，每季進行權限審查

01

全球資訊網後台

- 科技組網站維護

02

EIP 內網群組

- 駐外科技組表單
- 駐外科技組公文
- 科技組群組角色

03

EIP 內網個人

- 個人差假 / 表單
- 個人待辦公文
- 部內公告訊息
- 部內個人角色

資訊(安)諮詢窗口

如有資訊(安)相關問題，

請聯繫資訊處李科長美玲

(cherry@most.gov.tw)，謝謝。

問題與討論