調　查　報　告

壹、案　　由：包宗和委員、江明蒼委員、江綺雯委員調查：據悉，外交部領事事務局於資安檢查時發現外館有關民眾出國登錄資料系統遭入侵，究其狀況及原因為何？遭竊取帳密進行非法存取的手法為何？為何未能預防？是否有人為疏失？該局是否有建構完整的資安系統？政府資安預算用於外交工作的狀況為何？資安人力配置是否不足等情？均有深入瞭解之必要案。

貳、調查意見：

據悉，外交部領事事務局於資安檢查時發現外館有關民眾出國登錄資料系統遭入侵，究其狀況及原因為何？遭竊取帳密進行非法存取的手法為何？為何未能預防？是否有人為疏失？該局是否有建構完整的資安系統？政府資安預算用於外交工作的狀況為何？資安人力配置是否不足等情？均有深入瞭解之必要，爰申請自動調查。案經向行政院、國家發展委員會(下稱國發會)、國家通訊傳播委員會(下稱通傳會)、法務部、法務部廉政署(下稱廉政署)、法務部調查局(下稱調查局)、外交部、外交部領事事務局(下稱領務局)、外交部政風處調取相關卷證資料詳予審閱，並於民國(下同)106年3月7日實地履勘、訪查外交部領事事務局聽取簡報，並詢問外交部、外交部領務局等相關主管及承辦人員，業調查竣事，茲將相關調查意見臚陳如下：

一、領務局資訊安全維護不周，致出國登錄系統遭入侵，造成民眾出國資料10,050筆有外洩之虞，除戕害政府形象外，並影響民眾對電子化政府之信賴，核有違失：

(一)按個人資料保護法（下稱個資法）第18條規定：「公

務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。」上開所稱「安全維護事項」係指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取技術上及組織上之措施，該措施得包括下列事項，並以與所欲達成之個人資料保護目的間，具有適當比例為原則：一、配置管理之人員及相當資源。二、界定個人資料之範圍。三、個人資料之風險評估及管理機制。四、事故之預防、通報及應變機制。五、個人資料蒐集、處理及利用之內部管理程序。六、資料安全管理及人員管理。七、認知宣導及教育訓練。八、設備安全管理。九、資料安全稽核機制。十、使用紀錄、軌跡資料及證據保存。十一、個人資料安全維護之整體持續改善（個資法施行細則第12條規定參照）。政府機關其他資訊安全維護相關規定，如附表1。

(二)法務部[1]及國發會[2]對現行政府機關資安防護相關法令規定復稱：

1、法務部：為建構國家資訊安全環境，行政院定有「行政院及所屬各機關資訊安全管理要點」及「行政院及所屬各機關資訊安全管理規範」，……，協助各機關強化資安防護工作之完整性及有效性。

2、國發會：行政院已訂有「行政院及所屬各機關資訊安全管理規範」，規定各機關應依據個資法、國家機密保護辦法與行政院及所屬各機關資訊安全管理要點等有關法令，進行政府機關資安業務維護，……。

[1]法務部106年3月29日法律字第10603504580號函。
[2]國發會106年3月17日發資字第1060004599號函。

(三)領務局設立國人出國登錄系統之目的，係為即時掌握旅外國人之最新動態資料，期能於國人遭遇急難或於駐在國發生天災、重大事變時，可由駐外館處查詢旅外國人緊急聯絡方式即時提供援助，提昇服務國人績效。依該系統之設計，國人所登錄之資料係由領務局郵件伺服器主機判別國人登錄之出國地點，定時自動以電子郵件發送各相關駐外館處，並由駐外館處每日不定時收信歸檔，以備不時之需。

(四)行政院對本事件之查處情形[3]：

1、事件發生經過：

領務局於本(106)年1月25日接獲捷克駐外代表處反應，無法正常收取民眾出國登錄資料，除進行問題排除外，同時進行資通安全例行檢查，於1月26日發現外館領務人員公務信箱帳號密碼設定規則遭破解，導致有心人士成功登入系統並存取郵件，故於1月26日22時44分依「國家資通安全通報應變作業綱要」規定主動至國家資通安全通報應變網站通報2級一般資安事件。

外館領務人員電子郵件帳號主要以收取「出國登錄」系統轉發民眾出國登錄緊急聯繫資料及一般領務諮詢問題等資料，因民眾出國登錄緊急聯繫資料，包含姓名、生日、身分證字號、護照號碼、性別、電話等個人資料，爰於1月28日0時12分調升為3級重要資安事件。

經查，領務局官方網站「出國登錄」系統係供旅外國人出國前填寫緊急聯繫資料，倘前往地點發生重大災變或有緊急事故時，駐外館處將依

[3]行政院106年3月23日院臺護字第1060168324號函。

登錄資料，即時聯繫國人或其親友，提供必要協助。該局表示民眾於登錄緊急聯繫資料後，系統隨即將登錄資料以電子郵件方式轉發至該國之外館領務人員電子郵件帳號。

有關領務局本起個資外洩事件，肇因於電子郵件密碼規則遭破解，該局已立即停止以電子郵件傳送出國登錄資料至外館，改由外館於緊急狀況時直接向該局查詢資料，並以雙因子認證方式確保使用者身分；同時，該局亦主動通報，且依個資法規定通知相關當事人，針對後續可能發生狀況預擬應變機制，相關作為應屬妥適，行政院資通安全處(下稱行政院資安處)亦責請該局應加強清查內部其他系統有無類此情形，後續將依本次資安專案稽核結果，持續追蹤管考各項建議事項的改善情形。

2、行政院資安處派員實地瞭解：

（1）經郵件軟體開發/維護商檢視郵件登入紀錄，自105年10月10日至本年1月26日期間，遭外部不同來源IP，使用匿名網路Tor（The Onion Router),每天以間隔30分鐘輪流登入不同外館電子郵件帳號，初步寬估約有17,916筆民眾出國資料有外洩之虞【後經查明，實際為10,050筆，其內容不包括身分證字號】。

（2）另請該局資安廠商於106年1月26日至現場進行事件鑑識，項目包括防火牆紀錄、網域伺服器(AD)及郵件伺服器作業系統等，均未發現惡意程式與異常登入主機行為，雖郵件帳號密碼符合政府組態基準設定(GCB)及機關內部稽核作業規範(長度及複雜度)，惟具規則性，初步研判係規則遭破解，而造成此資安事件。

3、調查結果：

（1）有關領務局本起個資外洩事件，肇因於電子郵件密碼規則遭破解，致使民眾個資外洩，違反個資法第18條「公務機關保有個人資料檔案者，應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏」規定。

（2）針對近期政府機關發生重大資安事件，行政院資安處除邀集相關機關召開專案會議並進行內部檢討，強化資安防護作為，同時要求相關人員依權責進行檢討。

(五)外交部對本事件發生原因之說明[4]：

1、領務局配發駐外館處之領務電子信箱帳號密碼雖符合政府組態基準設定(GCB)及機關內部稽核作業規範(長度及複雜度)，惟具規則性，故遭破解；另領務局基於便民考量，為利旅外國人遇有急難時，駐外館處可於第一時間直接運用國人登錄之資訊聯繫協助，係由系統直接以電子郵件傳送出國登錄個資，且資料未加密。

2、大部分外館密碼（以館名代碼加數字及特殊符號命名）具規則性，故遭破解，現已改由程式隨機產生之複雜難度更高之12位密碼。

(六)詢據外交部及領務局相關主管對前開缺失均坦認不諱，並表示：「此次資安事件遭媒體披露後，造成民眾不安，本部深感抱歉，將全面檢討相關缺失」；「本事件……領務局的疏忽是未與時俱進，電子郵件以明碼傳送，經由此事件後，已改由外館於必要時以浮動密碼加配發密碼之雙層登錄方式向領務局查詢相關出國登錄資料，並對出國登錄主機之資

[4] 外交部106年3月20日外授領資字第1069000045號函。

料庫加密。」有本院詢問筆錄附卷可稽。

(七)綜上，領務局資訊安全維護不周，致出國登錄系統遭入侵，造成民眾出國資料10,050筆有外洩之虞，本事件經媒體批露，除戕害政府形象外，並影響民眾對電子化政府之信賴，與首揭各項規定有悖，核有違失，應予檢討改善。

二、領務局對本資安事件之通報未盡妥適，除未依限通報相關主管機關外，亦未即時通報檢、警、調等專責機關協助偵查，以適時有效追查入侵對象、動機及損害控管，進而妥適維護資安防護工作，洵有違失：

(一)按「各機關應建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向權責主管單位或人員通報，採取反應措施，並聯繫檢警調單位協助偵查。」次按「網路如發現有被入侵或有疑似被侵入情形，應依事前訂定的處理程序，採取必要的行動」、「網路入侵的處理步驟如下：……。立即向權責主管人員報告入侵情形。向機關內部或外部的電腦安全緊急處理小組反應，以獲取必要的外部協助」、「網路入侵之追查：入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。」復按「資安事件影響等級：資安事件影響等級分為4個級別，由重至輕分別為『4級』、『3級』、『2級』及『1級』」、「3級事件：密級或敏感資料遭洩漏」、「資安事件事中緊急應變：查詢通報應變網站、系統弱點(病毒)資料庫或聯絡技術支援單位(或廠商)等方式，以尋求解決方案；如無法解決，應迅速向主管機關或技術服務中心(下稱技服中心)反應，請求提供相關技術支援」、「資安事件如涉及刑責，應做好相關資料(含稽核紀錄)保全工

作，以聯繫檢警調單位協助偵查」、「各級政府機關(構)發現資安事件後除應循內部程序上報外，並須於1小時內，至通報應變網站通報登錄資安事件細節、影響等級及支援申請等資訊，……」末按領務局之資安責任等級屬於A級，應遵循行政院及所屬各機關資安管理規範辦理相關工作事項，查「行政院及所屬各機關資訊安全管理要點」第41點、「行政院及所屬各機關資訊安全管理規範」第伍章「網路安全管理」-二「電子郵件之安全管理」-(四)「網路入侵之處理」第2點「網路入侵之處理步驟」第(5)及(6)點、「國家資通安全通報應變作業綱要」第2章整體作業-2.3資安事件影響等級-(二)-1、第3章通報作業-3.1各級政府機關-(二)、第4章「應變作業」-4.1各級政府機關-(二)「事中緊急應變」第3及第6點及「政府機關(構)資通安全責任等級分級作業規定」第肆章「具體作法」等規定均定有明文。

(二)行政院國家資通安全會報(下稱資安會報)103年6月24日第26次委員會議決議，應強化網路犯罪防治機制，內容摘以：

1、討論案一、強化網路犯罪防治機制。

2、決議：鑒於網路犯罪問題往往涉及多個目的事業主管機關，且犯罪手法不斷翻新，各相關部會間溝通協調十分重要。請內政部定期(每季)召開會議作為溝通協調平臺，並由內政部次長擔任召集人，邀集法務部、通傳會、經濟部、金管會及科技部等相關部會共同研商網路犯罪偵防相關政策與重要業務之推動，期新型態網路犯罪事件發生時，政府機關能儘速提出突破性的作法及有效的管理措施。

(三)查「電腦犯罪防制、資安鑑識及資通安全處理事項」係法務部調查局法定職掌；次查「辦理資訊、通信及網路數位鑑識工作」「協助偵辦重大及特殊新興科技犯罪案件」「網路犯罪偵查技術之研究及運用」等事項，係內政部警政署刑事警察局法定職掌，法務部調查局組織法第2條第1項第8款及內政部警政署刑事警察局辦事細則第15條及第16條均有明文規定。

(四)本事件通報及檢討情形[5]：

1、領務局於本（106）年1月25日進行資通安全檢查時偵測發現領務作業電子郵件系統有異常活動情形，經調閱相關紀錄於1月26日發現有心人士似已識破部分駐外館處領務信箱使用之密碼，截取該局發送駐外館處之郵件；該局於發現問題當日（1月26日）成立「資通安全緊急應變小組」；當日22時44分，至「國家資通安全通報應變網站」通報登錄資安事件細節、影響等級等資訊[6]。

2、外交部對本事件之檢討及策進作為，已於106年3月9日召開「強化本部資訊安全專案會議」，就資安事件通報、資安稽核、資訊人力管考、資訊軟硬體管理等機制及資訊預算編列與執行進行檢討改進。

(五)行政院表示，領務局於106年1月26日22時44分至國家資通安全通報應變網站通報2級一般資安事件。因民眾出國登錄緊急聯繫資料，包含姓名、生日、身分證字號、護照號碼、性別、電話等個人資料，爰於1月28日0時12分調升為3級重要資安事件。

---

[5] 同註4。

[6] 外交部領事事務局出國登錄個資遭截取資安事件總檢討報告，106年2月24日，前註之附件六。

(六)詢據外交部及領務局相關主管表示：「領務局原以2級通報，報到行政院資安處後，才改為3級通報。因為行政院資安處認為有個資，故改為3級。」「事件發生是差不多下午3點多」「(委員問：這種級別的判斷，是否應該由貴局內部先行確定，而非由上級機關來決定？)領務局自事件發生後，已經先口頭報告外交部資電處，之後再查詢相關被駭之範圍。本局當日下午5點多確認，到晚上10點多通報」「通報機制是到國家資通安全通報應變網站填報，通報網站有相當多的資料必須要填，填好送出去會到我們的主管機關外交部資電處做第2層複審」「(委員問：領務局資安責任等級屬於A級，本應立即通報。但本事件卻花費相當長的時間。請問貴局是否知道屬於A級？是否知道如何執行通報作業？)是，謝謝委員指教，本部及所屬以後會再檢討，依規定執行」「(委員問：等級數及通報的窗口夠不夠縝密？)非常感謝委員點出這個問題的核心，本部會立刻請資電處開會檢討」「(委員問：本事件有無移請檢、警、調偵查？)本局已將相關日誌移給行政院資安處，由該處移請相關機關調查。」「(委員問：依據管理要點規定，各機關發生資安事件，均須聯繫檢警調單位協助偵查，並非透過第三者間接來執行)調查局日前至本局調閱資料，稱係接獲貴院之函」「委員問：次長，……，依行政院及所屬各機關資訊安全管理要點第41點明示，要立即向權責主管單位或人員通報，且要採取反應措施，並聯繫檢警調單位協助偵查。我不曉得，為何沒有做，這個要查吧。其實今天關心到的都是通報機制，包委員曾主持某一反恐調查，是屬預防性，我們才知道反恐其實最重要的是敏感度、反應機制

及彼此間的橫向及縱向聯繫，本案可否加以了解？)謝謝委員指教」「在此要特別代表外交部感謝幾位委員的指教，對本事件幾位委員都看得非常精準，對於本部那些缺失應予改善，將會立即開會檢討，再做一些精進作為，再次感謝幾位委員的指教」。

(七)本事件發生後之通報過程[7]：

1、106年1月26日下午4時：本事件發生時間。

2、106年1月26日下午10時44分：領務局至國家資通安全通報應變網站填報本事件時間。

3、106年1月26日下午11時3分：外交部至國家資通安全通報應變網站審核事件時間。

4、106年1月27日上午0時37分：資安會報技服中心至國家資通安全通報應變網站審核事件時間。

(八)經核，為建構國家資訊安全環境，行政院定有「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」、「國家資通安全通報應變作業綱要」及「政府機關(構)資通安全責任等級分級作業規定」，旨在協助各機關強化資安防護工作之完整性及有效性；另政府於內政部及法務部均設有協助各政府機關資安鑑識及網路犯罪偵查之專責單位。惟查，領務局對本資安事件之通報未盡妥適，除未依限通報相關主管機關外，亦未即時通報檢、警、調等專責機關協助偵查，以適時有效追查入侵對象、動機及損害控管，進而妥適維護資安防護工作，洵有失當；前開通報缺失，外交部相關主管於接受本院詢問時均坦承不諱，並表示該部及所屬以後會再檢討，依規定執行，有本院詢問

[7] 外交部約詢後補充說明資料，106年4月6日領資字第1069000054號函。

筆錄附卷足憑。

(九)綜上，領務局對本資安事件之通報未盡妥適，洵有違失，允應確實檢討改進。

三、領務局對本資安事件通知當事人之內容顯欠具體明確，失之空泛，對個別回應之民眾方予以較明確說明，難謂無差別待遇。本事件處置過程，未盡周延，有悖個資法及行政程序法相關規定意旨，容有未當：

(一)個資法第12條規定:「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」所稱「適當方式通知」，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之；但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之。又通知內容，應包括個人資料被侵害之事實及已採取之因應措施（本法施行細則第22條規定參照）；同法第28條規定：「公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。……」行政程序法第5條規定：「行政行為之內容應明確。」同法第6條亦規定：「行政行為，非有正當理由，不得為差別待遇。」

(二)領務局通知當事人及後續處置情形：

1、領務局依據個資法規定於106年2月6日上午以電子郵件通知105年10月10日至106年1月26日完成出國登錄之17,916位當事人(本院註：如圖1所示)，籲請提高警覺，視情況採取適當防範措施，避免使用出生年月日及英文姓名等個資設定個人電郵信箱密碼，並建議在出國期間定期主動向家人報平安，倘在海外遇有急難狀況發生，請即

與駐外館處聯繫洽助。同時提供該局聯絡資訊，如當事人想瞭解個案情況或因此造成損害，可透過電郵或電話與該局聯繫，將依法律規定處理。經統計自2月6日上午9時電郵通知近3個月內所有出國登錄民眾，共接獲相關民眾16封電郵及14通電話(詳如表2、3)，並均由專人回應。

> info@boca.gov.tw 於 2017年2月6日 上午9:12 寫道：
>
> 親愛的參與「出國登錄」的朋友：
>
> 您好！
>
> 感謝您支持外交部領事事務局提供旅外國人的安全保護機制，在領務局網頁登錄您出國期間之緊急聯絡資訊。
>
> 領務局為維護電腦資訊安全，近於資通安全檢查時偵測發現領務作業電子郵件系統有異常活動，初步研判領務局發送予駐外館處之部分國人出國登錄資料有可能遭不明人士攔截。
>
> 領務局已立即排除相關異常情形並加強資安管控。為恐有心人士不當運用相關聯絡資訊，建議您提高警覺，視情況採取適當防範作為；您在出國期間請定期主動向家人報平安，遇有急難狀況發生，請即與駐外館處聯繫洽助。
>
> 造成您的困擾或不便，外交部領事事務局謹申致歉意。

圖1　領務局通知當事人之電子郵件

資料來源：外交部

2、2月8日上午9時經蘋果日報即時新聞披露後，外交部公眾外交協調會(下稱公眾會)及領務局不斷接獲各媒體電話詢問，公眾會爰發布新聞採訪通知，由領務局發言人副局長鍾文正於當日上午10時30分在外交部新聞中心統一向媒體說明本案發生經過、緊急處理措施及後續因應作為；2月9日上午10時30分再由公眾會執行長王珮玲及該局副局長鍾文正利用外交部「單位主管新聞說明會」針對外界質疑續作補充說明。

(三)詢據外交部相關主管表示：「(委員問：受影響之民

眾是否有反應相關事件後續發展，貴局是否有從這些反應來歸納問題，以研判此事件之可能影響？）從民眾的反應均僅擔心是否有影響，但尚無確實之事件發生。本局後續將遵照委員指示，未來如有相關民眾反應，將盡一切力量幫助民眾協助解決問題。」

(四)經核，領務局於本資安事件發生後，雖以電子郵件通知相關當事人在案，惟查均採制式簡要方式處理，一概以「……領務局發送予駐外館處之部分國人出國登錄資料有可能遭不明人士攔截。……建議您提高警覺，視情況採取防範作為」通知當事人，卻未包括損害求償法律規定之告知，通知內容難謂具體、明確，失之空泛，一般民眾礙難理解並具備「視情況採取防範作為」之職能，洵有未洽；嗣對30位回覆之民眾，方於電子郵件中採較為明確通知：「視情況採取防範作為：例如避免使用出生日期或英文姓名等設為個人電郵信箱密碼」，並較明確解釋未來處理機制，難謂無差別待遇；領務局對個別回應之民眾雖均經處理有案，惟就上開民眾回覆內容以觀，業損及民眾對電子化政府之信賴及處置周全性之期待，處置伊始過程未臻明確、周全，未盡符合首揭相關規定旨趣，容有未當。領務局允應貼近民意，並開誠布公加強宣導溝通，盡一切力量幫助民眾協助解決問題，以化解民眾疑慮並獲民眾支持，俾挽回民眾對政府之信賴。

四、外交部未本於權責發揮監督機制，對領務局本事件資安通報未按規定先予審核，歷次資安稽核未盡落實，流於形式，資訊安全管理監督不周，亦有疏失：

(一)按「各機關首長及各級業務主管，應負責督導所屬員工之資訊作業安全，防範不法及不當行為。」次

按「應由機關之副首長兼任資安長(無副首長者由首長指派)，並設置『資通安全處理小組』，由資安長擔任召集人，負責訂定資安事件通報應變作業計畫，執行資通安全預防、危機通報及緊急應變處理相關措施，並納入機關(構)業務永續運作計畫之一部分；同時亦須協助所屬機關(構)之資安事件通報及應變處理作業，……。」查行政院及所屬各機關資訊安全管理要點第17點及「國家資通安全通報應變作業綱要」第2章「整體作業」-2.2「主管機關」等規定均定有明文。

(二)另「外交部長綜理部務，並指揮、監督所屬機關(構)及人員」、「本部設資訊及電務處」、「資訊及電務處掌理本部、本部所屬機關（構）與駐外機構資通安全之規劃、推動及督導等事項」，查外交部處務規程第2條第5條及第21條亦有明文規定。

(三)外交部及領務局資安防護體系及機制[8]：

1、組織：該部編制於資訊及電務處之資通安全科負責該部暨駐外館處資安相關規定、資安政策之訂定，另編制資訊及電務處之資訊中心負責資訊系統軟硬體維管等。領務局以任務編組方式設置「資訊小組」，由該組資訊人員兼辦資安防護系統軟硬體維管及業務運作。

2、資安維護計畫：

（1）外交部：為確保該部及駐外館處資通安全，該部從使用者端、系統與網路及人員資安教育3層面執行資安防護。

（2）領務局人員資安教育：定期辦理電子郵件社交工程演練，提升同仁資安意識；定期辦理資安

[8] 同註4。

通識教育課程，加強領務局同仁資安觀念；每年不定期赴駐外館處執行領務資訊系統技術協助，並針對領務組同仁進行教育訓練暨資訊安全宣導。

3、外交部為符合行政院規定之資安等級A級機關應辦事項，配合辦理定期資安健診、評估系統暨網頁弱點、寄發電子郵件社交工程演練信件、滲透測試等。領務局為符合行政院規定之資安等級A級機關應辦事項，亦配合辦理定期資安健診、網站安全弱點檢測、滲透測試、配合外交部辦理上述電子郵件社交工程演練及自行辦理電子郵件社交工程演練。

4、有關外交部稽核辦理情形，依據資安等級A級機關應辦事項規定，5項核心業務系統(公文系統、電子表單系統、數位檔管系統、外交服務網及電子郵件系統)已於105年12月通過ISO27001之驗證，並依ISO27001規定每年辦理內部稽核及外部稽核。領務局稽核辦理情形，依據資安等級A級機關應辦事項規定，3項核心業務系統(護照系統、簽證系統、文件證明系統)將於106年底通過ISO27001之驗證，並依ISO27001規定每年辦理內部稽核。

(四)詢據外交部「對領務局資安維護之相關措施或監督」表示：

1、依據行政院「政府機關（構）資通安全責任等級分級作業規定」，外交部及領務局均屬資安責任等級A級機關，均依據前揭分級作業規定辦理各項資安防護措施，相關年度資安稽核、健診作業檢測之報告等，外交部及領務局均各自函送辦理結果予行政院資安處備查。

2、領務局雖係外交部三級機關，惟由於領務工作及所延伸之領務資訊系統及業務有其特殊性及機敏性，各項資訊預算之編列、資訊人力、赴駐外館處執行資訊安全之督考、維管及教育訓練等，領務局資安工作事項均自行辦理，且直接向行政院資安處呈報，完全獨立於外交部資訊及電務處統籌管考範圍之外。

3、外交部於106年3月9日召開「強化本部資訊安全專案會議」，由章主任秘書主持，會中已就資安事件通報應變機制作全盤檢視。會議決議領務局及外交部各單位之資安事件，仍需依據「國家資通安全通報應變作業綱要」第2章第2.2項規定辦理，於行政院國家資通安全通報應變作業網站進行通報作業，經外交部資電處審核通過後（倘緊急，可立即電洽外交部資電處資安科科長），再通報行政院資安處，另外交部資電處並需同時副知「國家安全會議資通安全辦公室」。

(五)查領務局之資安責任等級屬於A級，允應遵循行政院及所屬各機關資安管理規範，落實辦理相關工作事項，包括每年至少2次內稽、每年至少辦理1次核心資訊系統持續運作演練、每年至少辦理2次網站安全弱點檢測、每年至少辦理1次系統滲透測試、每年至少辦理1次資安健診等事項(「政府機關(構)資通安全責任等級分級作業規定」參照)。惟就前揭外交部坦承對領務局相關資安措施失之監督(領務局本事件資安通報未按規定先經外交部資電處審核通過)，及本資安事件相關缺失以觀，外交部對領務局歷次之資安稽核、檢查未盡落實，流於形式，未本於權責發揮監督機制，機先發現相關缺失並適時督導改正，難辭督導不周之咎失，與首揭相

關規定有悖，亟應併予檢討改善。

五、法務部調查局對領務局民眾出國登錄系統遭入侵事件，允應本於權責賡續積極深入清查，以維護公務機關及國家整體安全：

(一)依監察法第30條規定:「監察院於必要時，得就指定案件或事項，委託其他機關調查。各機關接受前項委託後，應即進行調查，並以書面答復。」按電腦犯罪防制、資安鑑識及資通安全處理事項係法務部調查局法定職掌；調查局設資通安全處，掌理妨害電腦使用犯罪之防制及偵查、數位證物檢驗及鑑定……等事項。法務部調查局組織法第2條第1項第8款及該局處務規程第4條及第10條均定有明文。

(二)本院為深入追查本案有無人謀不臧(盜賣個資……等)，甚或危害國家安全等不法情事，爰依監察法第30條規定，委託調查局調查。案經該局查復[9]到院要以：

1、調查局資通安全處於106年3月31日以調資肆字第10614508790號書函發交調查局臺北市調查處調查，該處於4月12日函領務局調取資安檢測報告及郵件主機日誌，嗣於4月21日取得「紀錄檔光碟」及「外交部領事事務局事件調查報告書_1060127」各1份，並函送調查局資通安全處研析。

2、經檢視該紀錄檔光碟共67個紀錄檔，以各外館英文縮寫為檔名，其內容僅包含時間(格式：年-月-日 時:分:秒)與IP位置，並無提供其他相關資訊說明該IP位置使用者進行何種行為，調查局遂洽請領務局提供詳細資料或同意進行調研，6月

[9] 法務部調查局106年7月6日調資肆字第10614519790號函。

22日該局資訊小組陳進益組長覆以：「願意配合調查，但該等資料均已是最原始、最完整資料，無法再提供其他資料」等語。

3、復檢視領務局提供「外交部領事事務局事件調查報告書_1060127」，對郵件主機系統Zimbra可能存放紀錄日誌檔位置進行研析。依據Zimbra系統官方文件顯示，相關日誌檔(log)皆存放於路徑(/opt/zimbra/log)資料夾中，另參該報告第18頁(報告分項四、程序分析)第22行與第24行確有程式（rotatelogs）對 httpd_access.log 與 httpd_error.log以每日為單位切割日誌紀錄並儲存成不同檔案，足資證明該等檔案皆可能記錄相關日誌資料，需再請領務局提供俾利調查駭侵方式及系統遭入侵手法、時間等。

4、綜上，僅憑目前領務局提供之「紀錄檔光碟」記載時間與IP位置實難以判定駭侵行為、方式及時間；惟領務局判定帳號遭入侵並轉寄之依據為何亟待釐清。

(三)綜上，按電腦犯罪防制、資安鑑識及資通安全處理事項係法務部調查局法定職掌，為維護機關資通安全，防制不法分子利用電腦犯罪牟取不法利益，甚或危害國家安全，法務部調查局允應本於權責賡續積極深入清查，以維護公務機關及國家整體安全。

六、行政院對領務局民眾出國資料遭駭事件之稽核與後續處置，尚稱妥適，惟仍應加強督促各政府機關(構)全面落實檢討網路安全措施並採行相關具體策進作為，以防止類似入侵或攻擊情事再度發生，以落實政府資安作業，進而提供安全便利之電子化政府服務措施：

(一)行政院為國家最高行政機關；行使憲法所賦予之職

權；行政院院長，綜理院務，並監督所屬機關，憲法第53條及行政院組織法第2條、第10條分別定有明文。

(二)按「行政院為積極推動國家資通安全政策，加速建構國家資通安全環境，提升國家競爭力，特設國家資通安全會報」；次按有關「跨部會資通安全事務之協調及督導」等事項，為該會報法定任務之一；復按「該會報置召集人一人，由該院副院長兼任」；復按「該會報之幕僚作業，由該院資通安全處辦理」；末按「本會報下設網際防護體系，由本院資通安全處主辦，負責整合資安防護資源，推動資安相關政策，並設下列各組：『關鍵資訊基礎設施安全管理組』：本院資通安全處主辦，負責規劃推動關鍵資訊基礎設施安全管理機制，並督導各領域落實安全防護及辦理稽核、演練等作業。『資通安全防護組』：本院資通安全處主辦，負責規劃、推動政府各項資通訊應用服務之安全機制，提供資安技術服務，督導政府機關落實資安防護及通報應變，辦理資安稽核及網路攻防演練，協助各機關強化資安防護工作之完整性及有效性。」資安會報設置要點第1至第5點，均有明文規定。

(三)資安會報組織架構：詳見圖2

105年8月1日生效

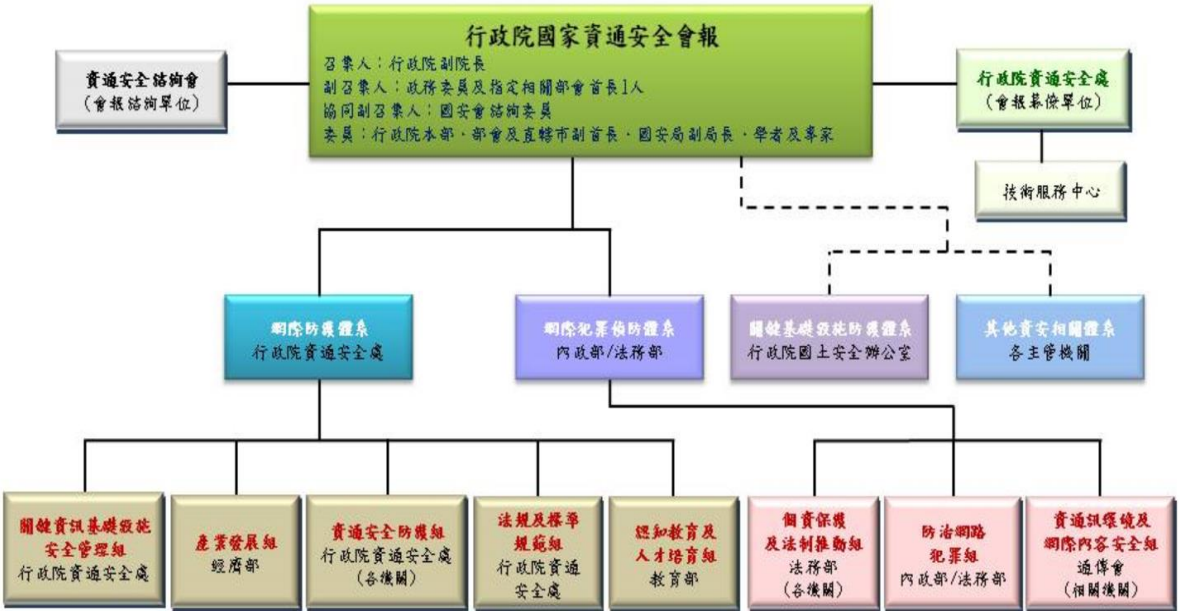

圖2　資安會報組織架構圖

資料來源：資安會報網站

(四)近期公務機關發生資安事件案例，如下表：

編號	報導日期	案例概述	報導來源
1	98.6.1	臺灣多所學校師生個資外洩百度查得到 在大陸搜尋網站「百度」，可搜尋到臺中縣數百名國中、小教師的身分證字號等個人資料，以及更多台灣學校學生個資。	資安人科技網
2	103.9.23	學校漏洞 洩260新生個資 逾260名彰化縣彰德國中學生的新生個資在網路上外洩，包括學生姓名、身分證字號、出生年月日、住家地址等都被看光光。	《蘋果》資料室
3	105.7.21	第一銀行ATM盜領事件 第一銀行ATM提款機遭到歹徒盜領金額共約8,327餘萬元。全臺20家一銀分行，共41台提款機，2名歹徒在完全無操作ATM的情形下，直接讓ATM吐鈔後大量提領，並立即將現金裝入背包離開，作案過程約5~10分鐘就在每台ATM輕鬆盜領數百萬元。調查局資通安全處確認國際駭客植入的兩支惡意程式分別為Cngdisp.exe與Cngdisp-new.exe，漏夜到一銀測試發現，2款惡意程式一次會讓ATM吐出現鈔6萬元，因此讓嫌犯在短短60小時內，以遠端操控模式讓全臺20家分行及機關內41台自動櫃員機自動「開口吐鈔」，領走8千多萬元新臺	聯合新聞網

編號	報導日期	案例概述	報導來源
		幣逃逸。	
4	105.10.26	勞動部被駭　3萬個資外流 勞動部勞動力發展署「台灣就業通」網站，傳出新北市一間國際資產管理公司涉嫌7月時入侵該網站，並竊取3萬多筆民眾個資。	聯合報
5	106.1.11	北市府洩個資　員工薪資看光光 管理北市府超過7萬多名公職人員的「薪資發放管理系統」，員工姓名、職稱、各項津貼，甚至銀行帳號，都外洩到網路搜尋平台。包括北市工務局、北市北投清潔隊，甚至人民保母北市內湖分局的警員個資，都被看光光！	華視
6	106.2.8	領務局遭駭　國人出國個資外洩 外交部領事事務局日前發現外館電子郵件有異常活動，研判部分民眾出國登錄資料恐遭駭外洩，副局長鍾文正證實，出現異常活動大約是最近3個月，估計約有1萬多筆資料，領務局已成立專案工作小組調查，並向民眾致歉。	聯合晚報
7	106.2.23	又是「比特幣勒索」　桃園6學校遭駭客恐嚇 桃園6所學校，在春節期間陸續收到駭客透過印表機傳送恐嚇信件，要求支付3個比特幣，大約新臺幣10萬元，不然就會癱瘓校園網路。其實不只桃園，包括臺北、高雄、臺中，都有學校遭到勒索，全臺共有46所學校受害。	TVBS新聞

資料來源：監察院製表

(五)行政院函送立法院第9屆第2會期第4次會議所提臨時提案之研處情形：

1、提案內容：立法院委員鑑於日前第一銀行盜領案，駭客利用使用者瀏覽器上的記憶體弱點，利用木馬方程式進行中間人攻擊來竊取用戶帳號、密碼導致個資外洩形成資訊破口，進而造成機密資料被竊取或滅失，經查幾乎所有政府單位之資訊系統均無相關防護措施。行政院應立即要求各機關單位，儘速檢討其網頁應用服務系統，對於網頁服務安全進行更進階的防禦措施，如釣魚網站攻擊、使用者密碼加密保護等，並確實建

立防禦措施與應變機制，以防止類似事件再度發生，若有任何機關單位仍然漠視資訊安全，導致再度發生資安事件，相關權責人員且必須予以嚴懲，是否有當？請公決案。

2、行政院研處情形[10]：

為健全中央與地方各級政府機關之資通安全防護能量，及落實各項資安防護工作，行政院積極推動我國資安相關工作，已建立完整的政府資安防護體系及機制，各項重要措施說明如下：

（1）各級政府機關防護能量之建構：

〈1〉明定資訊系統防護作業規定：為確保各政府機關（構）對所轄資訊系統設置有效之資訊安全防護措施，已訂定「資訊系統分級與資安防護基準作業規定」，要求各政府機關(構)依機密性、完整性、可用性及法律遵循性四大構面，分別評估資訊系統之安全等級，並依高、中、普等級明定資訊系統資安防護基準（分7大類型，計29項控制措施），以確保各政府機關（構）掌握重點保護標的，採行適當安全控制措施，完成應有防護基準，確保資訊系統之安全防護作為。

〈2〉明定資安責任等級分級作業規定：為明確規範各政府機關（構）之資通安全責任等級，並透過資通安全管理，以防範潛在資安威脅，進而提升國家資安防護水準，已訂定「政府機關（構）資通安全責任等級分級作業規定」，要求各政府機關（構）依其資安責任等級，落實政策、管理、技術、認證與訓練四

[10] 行政院105年10月27日院臺護字第1050041162號函。

大面向、10項作業之資安防護應辦事項，包含網站安全弱點檢測及滲透測試等防禦措施，以強化政府機關（構）網站之資安防護能力。

〈3〉落實資安縱深防禦：各政府機關（構）資訊系統之資安防禦措施，除依上述規定建立自我防護能量外，資安會報技服中心亦建置二線資安監控機制，加強資安縱深防禦。

（2）政府機關緊急應變能量之驗證與落實：

〈1〉定期執行資安事件通報與演練作業：為有效掌握政府機關（構）之資安事件，並迅速緊急應變處置，已訂定「國家資通安全通報應變作業綱要」,律定資安事件通報應變作業程序，並要求政府機關（構）應定期辦理緊急應變演練作業，以檢視其資安防護及應變管控能力。

〈2〉定期執行資安外部稽核：資安會報為強化各政府機關（構）資安能量，每年至少選定20個重要機關（構）辦理資安外部稽核，事前對資訊系統及網路環境執行技術檢測，再依策略、管理及技術等三面向，進行資安實地稽核，並邀請產官學研之資安專家共同參與，以期協助各受稽機關（構）強化資安防護工作之完整性及有效性。

〈3〉定期執行網路攻防演練：資安會報自102年起每年辦理網路攻防演練，並採電子郵件社交工程演練、實兵演練及情境演練方式進行，促使各政府機關更熟悉處理資安事件之標準作業程序外，並協助及改善多項網站系統弱點。

〈4〉後續精進作為：為建立安全及可信賴之電子化政府，確保資訊系統安全，將責成國家發展委員會研議政府機關網站全面使用安全傳輸通訊協定（HTTPS）之可行性，以提升資訊系統於網路傳輸資料之安全性及信賴度。

(六)國發會復稱[11]：

1、有關外交部領事事務局之民眾出國登錄資料系統資安事件應屬個別機關資訊安全防護作業疏失，該會就法規面、技術面及管理面三方面提供建議及後續策進作為如下：

（1）法規面：行政院已訂有「行政院及所屬各機關資訊安全管理規範」，規定各機關應依據個資法、國家機密保護辦法與行政院及所屬各機關資訊安全管理要點等有關法令，進行政府機關資安業務維護，建議外交部領事局確實落實上開國內資安法規及「政府機關（構）資通安全責任等級分級作業規定」，並遵循ISO 27001資訊安全管理、ISO 20000服務管理等國際標準要求，以確保內部資訊安全。

（2）技術面：短期內應進行全面性資安檢測，調整系統服務方式，避免以電子郵件方式寄送民眾資料至外館，調整由外館以安全連線方式連回該系統，並透過多重身分認證取得資料，依據等級制定對應之登入身分辨識安全機制，涉及個人資料之傳輸應採加密後進行。長期可建立資安之預警分析與管理監控服務，透過事前蒐集監控、事中偵測應變及事後鑑識分析等作為，以強化整體資訊安全成熟度。

[11] 同註2。

（3）管理面：員工資安教育是推動資安的首務，建議領事局應加強宣導公務同仁資安觀念，強化資安共識與危機意識，俾使同仁瞭解和遵行機關的資安政策，落實各項標準作業流程及資安規範，並重新盤點機關各項服務及持續更新資安風險地圖，了解各項服務所面臨的資安風險並採取對應之防禦機制，輔以定期稽核制度，檢視使用者操作行為，提高安全責任層級，透過正確的資訊安全觀念及落實執行，以有效減少資訊安全事件的發生頻率。

2、結論與建議：

行政院資安處主責國家資通安全基本方針、政策及重大計畫等資安相關業務，……，面對政府所提供之服務所衍生之資訊安全議題，該會甚為重視且持續掌握國內外發展趨勢，後續將配合行政院資安處政策協調權責部會分工辦理，以提供安全便利之電子化政府服務。

3、有關研議政府機關網站全面使用安全傳輸通訊協定(HTTPS)[12]之現況及可行性說明如下：

（1）為確保資料傳輸過程之安全性及隱密性，經查政府機關網站如有蒐集個人資料或需於網路傳

[12] 超文字傳輸安全協定（Hypertext Transfer Protocol Secure，縮寫：HTTPS，常稱為HTTP over TLS，HTTP over SSL或HTTP Secure）是一種網路安全傳輸協議。在計算機網路上，HTTPS經由超文字傳輸協定進行通訊，但利用SSL/TLS來加密封包。HTTPS開發的主要目的，是提供對網路伺服器的身分認證，保護交換資料的隱私與完整性。這個協議由網景公司（Netscape）在1994年首次提出，隨後擴展到網際網路上。資料來源：維基百科，https://zh.wikipedia.org/wiki/%E8%B6%85%E6%96%87%E6%9C%AC%E4%BC%A0%E8%BE%93%E5%AE%89%E5%85%A8%E5%8D%8F%E8%AE%AE

【註】：SSL/TLS：透過HTTPS傳送的資料非常安全，因為HTTPS會透過「傳輸層安全性」通訊協定(TLS)提供以下三道重要的資安防護網：

(1)加密：對交換的資料進行加密，防止資料遭到竊取。也就是說，當使用者在瀏覽網站時，任何人都無法「竊聽」其對話、追蹤他們在多個網頁之間轉換的活動，或竊取其資訊。

(2)資料完整性：系統會偵測出資料在傳輸過程中是否遭到有意或無意的修改或破壞。

(3)驗證：驗證您的使用者是否與預期的網站進行通訊。這能預防攔截式攻擊並建立使用者的信任感，進而促進其他商業利益。

送敏感資料者，多已採用HTTPS協定，該會於105年9月辦理行政院所屬二級機關(34個)、部分三級機關(122個)網站檢核，檢核結果二級機關網站採用HTTPS傳輸安全計12個，占35%，行政院所屬三級機關網站採用HTTPS傳輸安全計25個，占20%，詳如下表：

機關性質	已導入HTTPS之機關
二級機關	教育部、經濟部、交通部、衛生福利部、科技部、行政院海岸巡防署、行政院公共工程委員會、行政院主計總處、行政院人事行政總處、中央銀行、國立故宮博物院、公平交易委員會
三級機關	警政署、役政署、戶政司、地政司、領務局、國庫署、臺北國稅局、高雄國稅局、北區國稅局、中區國稅局、南區國稅局、臺灣金融控股(股)公司、臺灣土地銀行(股)公司、調查局、廉政署、智慧財產局、工業局、國際貿易局、水利署、航港局、公路總局、中華郵政(股)公司、勞動力發展署、海洋巡防總局、高雄榮民總醫院

資料來源：國發會

(2)觀諸先進國家如美國、日本、韓國及新加坡等政府網站仍未全面採用HTTPS協定，現行多採漸進導入方式，至國際瀏覽器大廠(如Google、Apple等)亦優先使用HTTPS，並逐步限制網站未來須使用HTTPS協定。

(3)綜上，網站使用安全傳輸通訊協定(HTTPS)已是強化網站安全之發展趨勢，相關技術亦已成熟，經該會評估，政府機關網站使用HTTPS協定係屬可行，考量各機關人力及資源限制，爰規劃採分階段方式推動行政院所屬機關重要對外服務網站使用HTTPS機制。鑑於政府政策一致性，該會後續將依據行政院資安處政策要求，藉由計畫審議或正式會議時機，要求權責部會配合辦理，以落實政府資安作業。

(七)通傳會表示[13]：

[13] 通傳會106年3月21日通傳基礎字第10600097080號函。

1、機關應依行政院資安規範積極配合辦理，強化跨機關聯防能力：資安會報為掌握我國政府機關及公民營事業機構資安事件，迅速雙向通報及緊急應變處置，98年2月5日已頒布「國家資通安全通報應變作業綱要」(105年8月1日修正)，以因應內外部環境情勢變化，強化政府機關通報應變能力。並考量我國政經情勢特殊，面對全球複雜多變的資通訊環境，以及日益嚴重的資安威脅，為持續精進各項資安防護工作，於104年配合「政府機關(構)資通安全責任等級分級作業規定」之研修及分行實施，參考資通訊科技發展與網路攻防演練、政府機關(構)資安健診、系統滲透測試、稽核等結果，進行參考手冊研修，並將名稱調整為「資訊系統分級與資安防護基準作業規定」。鑒於上揭政府資安規範確已布達，為提升機關資安聯防能力、降低資安攻擊威脅，行政院所屬機關應依上揭規範積極辦理。

2、機關應提升組織資安素質，強化資安防禦：依上揭國家資通安全通報應變作業綱要規定，行政院所屬各機關應自行負責規劃、推動其各項資通訊應用服務之安全機制，辦理資安防護、應變及通報等作業，為記取本次資安事件提升機關網路資安防禦，各機關應確實依上揭資訊系統分級與資安防護基準作業規定，落實網路攻防演練、資安健診、系統滲透測試、稽核等作為，以有效提升組織資安素質。

3、鑒於國際近年對於資通安全保護，已逐漸以訂立專法之方式加以規範，而我國雖有適用於私部門之資通安全相關法制，如刑法電腦犯罪專章、電信法、個資法及政府資訊公開法等，但尚欠缺以

風險管理為出發點，針對整體資通環境之法律位階規定；行政院雖已訂定行政院及所屬機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等規範，惟尚無賦予各機關資通安全維護義務之法律基礎。為更能有效提升我國公務機關之資通安全能量，並將關鍵基礎設施及部分其他非公務機關所提供，涉及國土安全維護與民眾生活安全之產品或服務，以法律明確規範其資通安全，行政院資安處刻正推動資通安全管理法草案之立法，以建立對公務及非公務部門之完整資安規範。

(八)調查局表示[14]：

政府資安事件發生時，建議副知調查局派人協助調查，並保全資安事件軌跡以利公務機關資安事件之掌握及配合後續司法訴追。

(九)行政院表示：

1、資安人力、預算之相關規定：

（1）依「政府機關(構)資通安全責任等級分級作業規定」，要求各機關依不同資安責任等級，應指派適當資安專責人力(A級機關指派資安專責人力2名，B級機關指派資安專責人力1名，C級機關則依各主管機關規定)，目前多由各機關現有資訊人力兼辦。

（2）資安預算則暫無相關規定。

2、資安人力配置、預算訂定之現況：

（1）鑒於資安演變趨勢及業務新增，原有兼職資安人員不足因應，亟需專職資安人員(全時辦理資安業務)，依行政院資安處本年所辦理之資安人

[14] 調查局106年7月6日調資肆字第10614519790號函。

力調查結果，現有A級機關平均有1.6名專職資安人力，B級機關平均有0.5名專職資安人力，C+級機關平均有0.1名專職資安人力，C級機關平均有0.2名專職資安人力。

（2）行政院資安處為協助相關部會推動各項資安重要政策，並協助各關鍵基礎設施領域主管機關建立各該領域ISAC、CERT及二線SOC機制，以落實關鍵資訊基礎設施防護(CIIP)，由該處負責推動106年跨部會資通安全科技計畫包括「加速政府資安防護建設計畫」(國發會、金融監督管理委員會、法務部、國防部)及「資安旗艦計畫」(經濟部、科技部、衛生福利部、內政部、通傳會、教育部、交通部)。

3、相關檢討、策進作為：

（1）配合後續資安管理法施行，各機關將新增多項資安業務，為妥適因應，目前行政院資安處刻正研擬相關策進作為，期望建立政府資安快速應變小組，目前規劃針對關鍵基礎設施主管機關及資安等級A級機關分階段配置專職資安人員，平時派駐機關督導資安業務，發生資安事件時組成跨機關小組，藉以培育資安人才，充實公務體系資安專職人力；本案目前刻由行政院資安處與行政院人事行政總處研商調整方案內容，嗣於近期調整完畢後將邀集相關機關召開會議研議，後續依規劃期程逐步推動。

（2）針對近期政府機關發生重大資安事件，行政院資安處除邀集相關機關召開專案會議並進行內部檢討，強化資安防護作為，同時要求相關人員依權責進行檢討；另行政院資安處刻正研擬資通安全管理法(草案)，業於第14條中規範公

務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵，未遵守本法相關資通安全義務時，應追究行為人、其服務機關資通安全長及相關人員之行政責任。將在子法中之資通安全事件通報及應變辦法中律定明確獎懲標準。

（3）行政院為建立安全及可信賴之電子化政府，確保資訊系統安全，將責成國發會研議政府機關網站全面使用安全傳輸通訊協定（HTTPS）之可行性，以提升資訊系統於網路傳輸資料之安全性及信賴度。目前辦況：

國發會已擬定106年3月28日至30日，於北中南地區辦理4場次「政府機關DNS主機安全設定及網站導入HTTPS說明會」，未來規劃行政院所屬二、三級機關全球資訊網原則於106年12月底前完成使用HTTPS傳輸協定;政府機關重要對外服務網站至遲於107年12月底完成使用HTTPS傳輸協定。

（4）本事件之問題癥結、法令疏漏或窒礙之處、興革補救及檢討改進措施：

〈1〉近年來，對於公務機關或關鍵基礎設施等進行網路攻擊之情形時有所聞，在我國公部門部分，目前已設有資通安全推動單位與相關遵行規則，而在私部門部分，目前雖有可適用之相關法令，但仍缺乏一套以風險管理為基礎，規範整體資通環境之專法。行政院資安處已參酌美、日、德等先進國家立法原則，並考量我國社經環境與法規制度，研議行政院版之資安管理法草案。另為求法律之周延性，已完成公務機關、民間團體及學者專家

之意見徵詢，並據以調修相關條文內容。

〈2〉目前適用對象原則以公務機關、關鍵基礎設施提供者、公營事業及政府捐助達一定比例之財團法人為主。考量各界對於本草案內容已具共識，將俟完成資訊及資安人力盤點後即召會審查。此外，為利法案後續推動，已賡續研訂施行細則及相關子法，並規劃完整配套措施。

(十)行政院於106年4月27日院會通過「資通安全管理法草案」，明定包括行政院各部會、地方政府等公務機關應做好資通安全維護，訂定資安事件的通報及應變機制，以加強資安的防護能量，若違反上述情節，公務員將依其情節輕重受懲戒或懲處；中央目的事業主管機關或直轄市、縣（市）政府應指定關鍵基礎設施提供者，關鍵基礎設施提供者應訂定、修正、實施資通安全維護計畫；關鍵基礎設施提供者以外的非公務機關，應訂定、修正、實施資通安全維護計畫；非公務機關應訂定資通安全事件之通報及應變機制……等。

(十一)外交部相關主管接受本院詢問時表示：「(委員問：經查外交部駐外館處未有專業資訊人員，資訊業務是由外館同仁兼辦，因本人最近前往法蘭克福及西班牙，他們告訴我剛赴任時，須花許多心力瞭解資訊業務，在小小的資訊室裡，每天處理大量資訊工作，難道外館沒有配置資安人員，有甚麼解決辦法？)其實這是本部長久以來的問題，我們也在想辦法解決」「因派駐外館工作多數為外領人員，外館普遍缺乏資訊人員，……。誠如次長所言，這是我們所面臨的問題，……」「本部都非常重視資安問題，本部與國安會、國安局及行政院資安辦公

室，每年均有幾次前往駐外館處做資安健診，剛才委員關切我們專業資訊人員為什麼那麼少，這部分我們察覺到，實際上我們有一個很理想的計畫，就是分區能夠於每個區配屬一個專業資訊人員，全球分6個區，但因預算及人才的問題，故至目前為止，僅北美區有1個專屬資訊人員配置在華府」「資安預算很難增加，因為預算都是固定的，現正編列107年概算，通常不會超過106年的額度，還可能逐年要減少10%」「(委員問：看來外館資安人員是不足的，可能是經費不夠或無專業人才，但又非常重要，遑論外交部這麼重要的機構，甚至於一般文教機構，都有至少一個懂得資安的人可以詢問或於緊急狀況時能即時處理，理論上，外館也應當如此。但那麼多外館，倘每館都配置一個資安人員，事實上力有未逮，不過，這倒是一個很重要的問題，尤其現在我們將外交視同作戰，許多駭客想駭進來，這是蠻重要的課題。……，能請說明一下)領務局已建置資安監控中心(SOC)……」「(另剛談到外館資安人員不足，那只有退而求其次，就由現派駐外交人員，或由當地約聘的方式來做，所以我們如何來作教育訓練，增加他們的資安知識，也就是說，遇到資安問題不太嚴重時，大概可以由同仁自己來應付，此方面的教育訓練，外交部或領務局有無規劃加強資安訓練。)有關加強資安職能訓練方面，除了剛才領務局提到資安監控中心(Security Operation Center,SOC)，那是一個做法。另外人員資安教育訓練方面，外交部有3個做法：(1) 定期辦理電子郵件社交工程演練；(2)定期辦理資安通識教育課程；(3)不定期赴外館做資安技協。」

(十二)綜上論述，近期政府機關資安事件頻傳，相關違

規情節突顯機構資安意識薄弱、教育宣導有待強化及資通安全機制尚待提昇等缺失。行政院對領務局民眾出國資料遭駭事件之稽核與後續處置，尚稱妥適，惟仍應秉持針對本事件之稽核與後續策進處置之精神與品質，加速「資通安全管理法」立法期程，統籌資安會報等相關防護、偵防體系，加強督飭所屬就法規面、技術面及管理面三方面全面落實檢討網路安全措施並採行相關具體策進作為，以防止類似入侵或攻擊情事再度發生，以落實政府資安作業，進而提供安全便利之電子化政府服務措施。

附表1、政府機關其他資訊安全維護相關規定一覽表

名稱	相關內容
行政院及所屬各機關資訊安全管理要點(88年9月15日函頒)	壹、目的 一、行政院為推動各機關強化資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全、保障民眾權益，特訂定本要點。 柒、網路安全管理 二十二、各機關利用公眾網路傳送資訊或進行交易處理，應評估可能之安全風險，確定資料傳輸具完整性、機密性、身分鑑別及不可否認性等安全需求，並針對資料傳輸、撥接線路、網路線路與設備、接外連接介面及路由器等事項，研擬妥適安全控管措施。 二十三、各機關開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。 二十六、……。 機關網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭不當或不法之竊取使用。 二十七、……。 機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關應視需要以適當之加密或電子簽章等安全技術處理。 機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管機關認可之加密或電子簽章等安全技術處理。 捌、系統存取控制 三十五、各機關之重要資料委外建檔者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。
行政院及所屬各機關資訊安全管理規範(88年11月16日發布)	肆、電腦系統安全管理 五、個人資料之保護 1、應依據電腦處理個人資料保護法等相關規定，審慎處理及保護個人資訊。 2、應建立個人資料控制及管理機制，……。 伍、網路安全管理 一、網路安全規劃與管理 (一)網路安全規劃作業 1、應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系

	統存取。 2、對於跨組織之電腦網路系統，應特別加強網路安全管理。 3、利用公眾網路傳送敏感性資訊，應採取特別的安全保護措施，以保護資料在公共網路傳輸的完整性及機密性，並保護連線作業系統之安全性。 (四)主機安全防護 1、存放機密性及敏感性資料之大型主機或伺服器主機(如 Domain Name Server 等)，除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身份辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取(如一般網路服務 HTTP、Telnet、FTP等的登入密碼)，及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。 (七)網路資訊之管理 6、對外開放的資訊系統，如存放民眾申請或註冊的私人資料檔案，應研究以加密方式處理，並妥善保管，以防止被竊取或移作他途之用，侵犯民眾隱私。
國家資通安全通報應變作業綱要(105年8月1日修正)	1、第1章前言：本綱要務請各級政府機關(構)落實執行，俾配合推動提升通報應變時效、健全資安防護能力、……，以全面強化政府資安防護機制，確認政府擁有安全、可信賴的資通訊環境。 2、第4章應變作業： 4.1 各級政府機關(構) 各級政府機關(構)應建立資安事件之事前安全防護、……之具體機制，至少須包括下列各項： 2.……，對於機敏文件、資料及檔案等應採取加密或實體隔離等防護措施。 7.應針對上述建立之資通安全防護環境及相關措施，列入年度定期稽核項目，定期實施內部稽核，以儘早發現系統安全弱點並完成修復補強。

監察院製表

附表2、民眾郵件洽詢及回復統計表

編號	姓名	洽詢日期	回復日期	洽詢內容	回復摘要	回復人
1	林小姐	2月6日	2月6日	您的意思是我的個資外漏嗎？ 請問什麼是視情況採取適當防範作為？ 我對於您這封信深感惶恐。 請解釋遭不明人士攔截的資訊傷到哪裡？全部個資外洩？還是說哪個部分？可否解釋？ 而不是只是一封深感抱歉的信，請我們自行注意安全不了了之。	已e-mail回復。	郭○○
2	洪小姐	2月6日	2月17日	資料外洩？ 所以出國登錄等於給自己找麻煩？ 保護國人資訊安全不是職務上的責任義務嗎？竟然輕忽到讓不明人士攔截？這麼基本的職責都做不好，難怪邦交國一個個減少，……。 做不好，就換能做得好的專業人士來做，別抱著泡茶聊是非的心態耗在那兒等領退休金，真是令人太生氣了。	已電話回復，解釋未來處理機制並取得諒解。	黃○○
3	周小姐	2月6日	2月6日	您是指我們在政府單位登錄的資料可能已被有心人士擷取嗎？ 這樣我們怎麼會放心將資料登錄在上面！ 其所謂不明人士是誰，被截取的資料也沒有辦法有個配套措施嗎？我們在國外的安全會不會因此受到影響呢？	民眾未登錄護照號碼，所以身分證字號及護照號碼均未傳送外館，已e-mail回復。	黃○○
4	蔡小姐	2月6日	2月8日	如何刪除過去曾登錄的資料呢？	協助刪除出國登錄資料。	黃○○
5	康小姐	2月6日	2月17日	何時能確認是否確實遭駭客攔截資料？ 確認後會再發信件通知嗎？ 資料被攔截者，貴單位會另行通知	已e-mail回復。	李○○

編號	姓名	洽詢日期	回復日期	洽詢內容	回復摘要	回復人
				嗎？麻煩請一定要通知當事人。		
6	徐先生	2月6日	2月6日	這是否說明我的護照資料被陌生人知道而胡亂使用？之前出國，我沒有申請出國登錄，請問做出國登錄的目的是什麼？	已電話回復，因未完成登錄程序，故無個資傳送外館遭截取之虞。	黃○○
7	蕭小姐	2月8日	2月18日	請問什麼叫「建議您提高警覺，視情況採取適當防範作為」？這句話有說跟沒說一樣。 什麼是「適當防範作為」，告你們嗎？不是吧？ 在同一封信裡講清楚有這麼困難嗎？ 請交代清楚好嗎？ 請回復什麼是視情況採取適當防範作為，例如甚麼？	已撥6次無接聽，改以e-mail回復。	黃○○
8	李小姐	2月8日	2月17日	1.所以我登錄的個資到底有沒有遭竊？我該如何得知？ 2.對於個資遭竊民眾，貴局後續作為是什麼？就是請民眾提高警覺嗎？這樣好像就是在對民眾說：「你們的重要個資被竊囉~我也沒辦法啊~你們自己小心吧(攤手)」對於貴局目前為止的處理非常失望！貴局有沒有要說明清楚？	已電話回復，解釋未來處理機制並取得諒解。	李○○
9	陳小姐	2月8日	2月8日	之前出國登錄之資料是否可全數刪除？	協助刪除出國登錄資料。	黃○○
10	林先生	2月8日	2月17日	這是件完全不能接受的錯誤！ 這就是支持貴部活動的後果嗎？ 我現在很擔心我的個人資料外洩所可能會發生的權益損失，請提出解決方式！ 請研議讓個資外洩的受害人可以修改身分證字號和護照號碼的方案！！	確認其登錄期間並非資料遭截取時間內，已電話回復獲同意免另文函復。	黃○○
11	李小姐	2月9日	2月17日	請問針對我的個資被駭的問題，貴局會採取什麼措施因應？	以電話回復，解釋	黃○○

編號	姓名	洽詢日期	回復日期	洽詢內容	回復摘要	回復人
				萬一我們因此利益受損或者家人因而受騙上當而有所損失時，貴局應當賠償我們所有的損失及精神上的賠償。此事非同小可，請貴局提供解決方案及申訴管道。	未來處理機制並取得諒解。	
12	李先生	2月9日	2月17日	所以意思是道歉就沒事了嗎？	已電洽解釋未來處理機制並取得諒解。	黃○○
13	謝小姐	2月10日	2月14日	請速將本人出國登錄資料刪除，謝謝。 以後再也不登錄了，非常失望。	協助刪除出國登錄資料。	黃○○
14	余小姐	2月12日	2月16日	有收到你們的通知告知資訊安全出了問題，那請問我的資料是否外洩？是外洩了什麼資料？你們如何做後續處理？ 我們需要做什麼來保障自己資料不外洩？	已電話回復，因未完成登錄程序，故無個資遭截取之虞，解釋未來處理機制。	李○○
15	趙小姐	2月14日	2月21日	本人已多次致電聯繫要請更換一本新的護照。我在埃及回國後，收到2位當地不明人士APP聯絡，對方知道我出入境的國家及相關個資。此事件讓我相當困擾。	因查伊未填寫護照號碼，爰協助當事人自費申辦新護照。	郭○○
16	江先生	2月17日	2月21日	你們真是讓人失望，這是我第一次出國向你們登記，竟然是資料可能外洩，怎麼會發生這樣如此離譜的事，你們外交部人員到底在作什麼？你們有沒有在檢討？你們的失職人員有沒有應該下台負責？ (對你們做事失望的人的心聲)	確認其個資並未遭到攔截，已e-mail回復：對於你提出的寶貴意見，本局將虛心受教，並檢討改進。	黃○○

資料來源：外交部，監察院彙整製表

附表3、民眾電話洽詢及回復統計表

編號	姓名	電話	洽詢日期	時間	簡要內容	民眾態度	接聽人
1	X小姐	0930-******	2月7日	10:25	出國登錄個資是否安全？解釋後OK。	語氣平和	黃○○
2	李小姐	0911-******	2月8日	08:45	有出國登錄，洽詢可否換新護照。解釋後不換護照。	–	李○○
3	陳小姐	0935-******	2月8日	12:30	僅抱怨。	語氣怒轉平和	黃○○
4	X小姐	0989-******	2月8日	13:15	伊未登錄，因看新聞標題聳動，僅洽詢個資是否會洩漏。	語氣平和	黃○○
5	楊先生	內線轉來	2月8日	14:58	105年6月登錄及詢問郵箱變更，已解釋不影響。	語氣平和	黃○○
6	陳小姐	0987-******	2月8日	15:40	出國登錄個資是否安全？解釋後OK。	語氣平和	黃○○
7	X小姐	03-*******	2月8日	19:28	詢問私人郵箱變更，已解釋。	–	蘇○○
8	周先生	–	2月9日	09:45	出國登錄個資是否安全？解釋後OK。	語氣平和	黃○○
9	陳小姐	770*****	2月9日	10:05	伊未登錄，因看新聞標題聳動，僅洽詢其個資是否會仍洩漏。	語氣平和	黃○○
10	賴小姐	0921-******	2月9日	10:50	抱怨居多，例如銀行回復郵件有加密，基本資料未來可能會被偽造之擔憂，可否查復其個資有否洩漏，或倘須更改各類身分資料，如何協助。另未來倘有因個資損害其權益，如何證明是本局造成？解釋後OK。	語氣怒轉平和	黃○○
11	莊先生	0928-******	2月9日	13:39	洽詢渠出國期間家裏遭竊賊破壞門鎖未成，可否求償？已查復告未遭截取，不受本事件影響。	語氣平和	黃○○
12	曾先生	0919-******	2月9日	14:35	洽詢12月出國登錄資料是否外洩？已查復並經解釋後OK。	語氣平和	黃○○
13	趙小姐	0939-******	2月9日	15:24	有出國登錄，並稱疑似遭駭客知悉出入境，係本局疏失，堅持換新護照，因查其護照號碼未填寫，已協助伊自費申辦新護照。	語氣強硬	黃○○
14	X小姐	226*****	2月10日	15:08	僅洽詢該公司同仁出國，其個資是否仍會洩漏？已解釋無登錄沒有資料外洩之虞。	語氣平和	黃○○

資料來源：外交部，監察院彙整製表