糾　正　案　文

壹、被糾正機關：外交部、外交部領事事務局。

貳、案　　由：外交部領事事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；另該局除對本資安事件之通報未盡妥適外，通知事件當事人之內容亦欠具體明確，失之空泛；外交部復未本於權責發揮監督機制，資訊安全管理監督不周，均核有違失，爰依法提案糾正。

參、事實與理由：

本案緣於外交部領事事務局(下稱領務局)於民國(下同)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，發現領務作業電子郵件系統有異常活動情形，初步研判係領務局發送予駐外館處之電郵，包括部分國人出國登錄資料可能遭不明人士攔截；於同年月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自105年10月10日至106年1月26日領務局發送駐外館處含有個資、已加密或未加密之郵件。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、領務局、外交部政風處調取相關卷證資料詳予審閱，並於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、領務局等相關主管及承辦人員發現，本案領務局資訊安全維護不周，致出國登錄系統遭入侵、對本資安事件之通報未

盡妥適、通知事件當事人之內容顯欠具體明確，失之空泛、外交部亦未本於權責發揮監督機制，資訊安全管理監督不周，確有怠失，應予糾正促其注意改善。茲臚列事實與理由如下：

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。

(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

[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。

「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，……。

(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

[3]行政院106年3月23日院臺護字第1060168324號函。

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

[4] 外交部106年3月20日外授領資字第1069000045號函。

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

[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。

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。

(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

[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。

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，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

[8] 同註4。

「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。

綜上所述，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；又該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；另該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；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，均核有違失，爰依監察法第24條規定提案糾正，移送外交部轉飭所屬確實檢討改善見復。

提案委員：包宗和

江明蒼

江綺雯

中　　華　　民　　國　　106　　年　　8　　月　　日

附表、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