調　查　報　告

壹、案　　由：銓敘部掌理全國公務人員之銓敘、任免、考績、退撫等相關事項，惟日前卻傳出約59萬筆公務人員個資外洩，疑遭國外網站揭露，引起公務人員憂慮。究個資外洩之原因、影響範圍及程度為何？有無人員涉有管理違失或不法竊取？相關檢討及後續因應措施為何？銓敘部資訊安全防護監管機制及事件通報與應變處理流程是否周妥？均有進一步調查釐清之必要案。

貳、調查意見：

一、銓敘部未能積極配合98年起推動之「政府機關（構）資訊安全責任等級分級作業施行計畫」，迄105年10月始將可存取全國公務人員銓審資料之「銓敘業務網路作業系統」及「公文管理及線上簽核系統」納入ISMS(資訊安全管理制度)驗證範圍，使含機敏機關在內之全國公務人員個資長期暴露於高風險環境，爰本案58萬餘筆個資洩漏，該部難辭其咎，顯有違失。

(一)本案通報處置及洩漏原因分析

1、通報處置：據行政院資安處院臺護字第1080185817號函復說明，108年6月22日該院接獲國家安全會議(下稱國安會)通報，有心人士於國外論壇(Raidforums)公開販售疑似銓敘部持有之公務人員個人資料約58萬筆，行政院資安處即責請國家資通安全會報技術服務中心(下稱技服中心) 隨即通知該部，銓敘部於6月22日因尚未能立即確認係屬該部資料，爰依資通安全管理法(以下簡稱資安法) 規定先行通報1級資安事件，經銓敘部確認論壇網站之個人資料確為該部所

有，於6月23日再次通報提升資安事件嚴重等級為3級。

（1）3級事件定義：依據「資通安全事件通報及應變辦法」，資通安全事件共分4級，本案應符合第3級「**未涉及關鍵基礎設施維運之核心業務資訊遭嚴重洩漏**，或一般公務機密、敏感資訊或涉及關鍵基礎設施維運之核心業務資訊遭輕微洩漏」之條件。

（2）為協助銓敘部資安事件應變處置，行政院依「資通安全事件通報及應變辦法」第17條規定，於6月25日召開資安防護會議，邀集國家安全局、調查局、刑事局及技服中心等，組成專案團隊，進行事件調查及危害分析。

（3）據銓敘部查復，該部108年7月1日至5日配合行政院資安處、調查局及刑事局進行該部全部資訊環境資訊安全檢測及相關採證、鑑識及調查作業。7月15日再配合行政院資安處進行該部ISMS管理制度之實地稽核。

2、據銓敘部108年6月25日新聞稿初步分析洩漏資料如下：疑似外洩資料為該部94年1月1日至101年6月30日間中央及地方機關公務人員送審人員歷史資料，經比對後實際影響人數為24萬餘人。該外洩資料**為舊公文管理系統之收文資料**，並非最新銓敘審定資料，且該系統已於104年3月即下架。

（1）據該部查復資料，案關資料庫於公文系統建置時同步設立，至104年12月31日停止使用者連線使用，惟系統下線後，資料庫因文書檔案實務作業比對舊有資料之需要，處於常態關閉。

（2）上開系統相關硬體係於108年5月14日奉准報

廢,相關個資旋於同年6月22日在國外論壇遭公開販售。

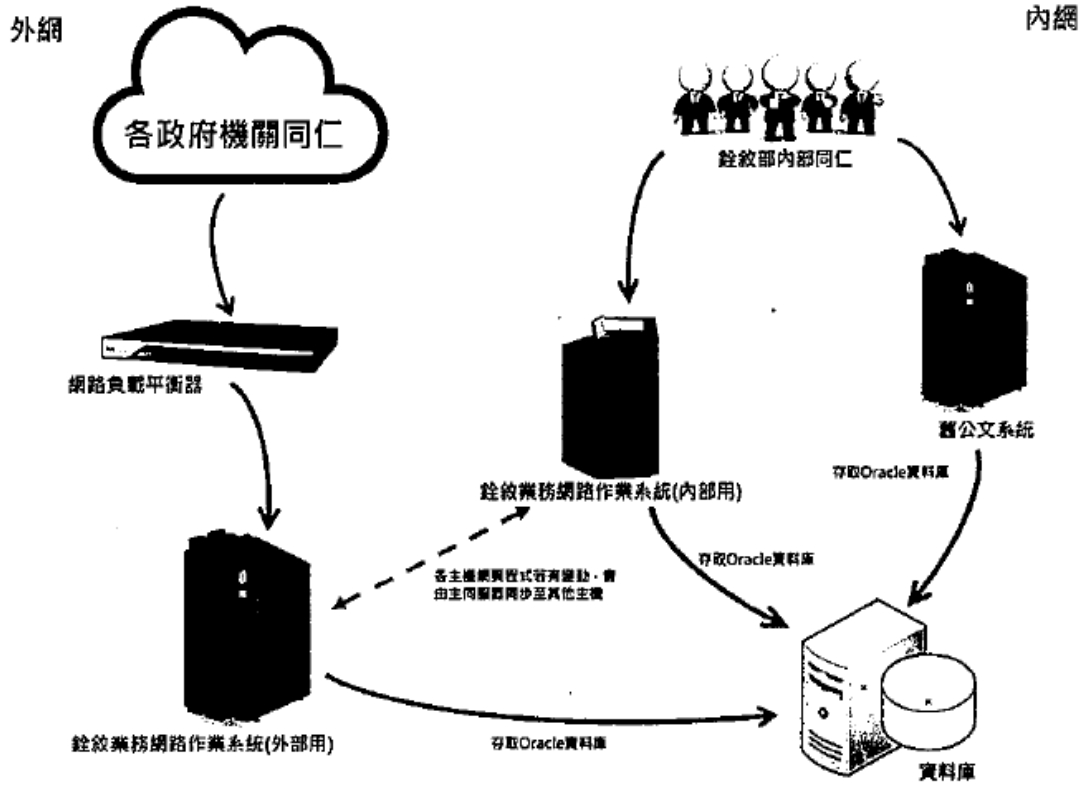
3、綜整調查局、刑事局及行政院資安處分析洩漏原因如下：

（1）調查局自外洩資料筆數及內容研判，外洩資料疑於101年6月1日下午遭竊,惟當年銓敘部資訊室相關主機均不存在，包括：舊公文系統主機報廢、銓審系統更新、資料庫系統更換（Oracle/MS SQL)，且資料庫主機未完整開啟稽核功能，已無從追查駭客竊取資料之手法與確切時間。

（2）刑事局則說明，透過鑑識惡意程式之建立時間分析，研判攻擊者以入侵銓敘業務網路作業系統方式取得資料庫權限後，匯出資料庫內容。

（3）行政院資安處則說明，銓敘部部分主機過去有陸續遭植入惡意程式情形，研判前揭期間之公務人員銓審資料仍有外洩之虞。

（4）綜上，舊公文系統與銓敘業務網路作業系統共用同一資料庫(如下圖)，**透過惡意程式建立時間及銓敘業務網路作業系統存在多項可利用之攻擊弱點，研判資料由銓敘業務網路作業系統外洩之可能性較高**。



4、洩漏範圍:經銓敘部清查後，確認屬該部104年3月下線之舊公文管理系統內，94年1月4日至101年6月1日之歷史收文基本資料589,991筆，實際影響人數為243,376人，欄位包含身分證字號、姓名、服務機關、職務編號、職稱。其機關屬性如下：

機關屬性	人數	比例
行政機關	184,214	75.68%
公營事業機構	12,989	5.34%
衛生醫療機構	22,165	9.11%
公立學校職員	24,044	9.88%
合計	243,412	100%

（1）依據銓敘統計年報，101年底全國公務人員[1]共

[1]係以行政機關、公營事業機構、衛生醫療機構及公立學校（職員）為統計範圍，不包括公立學校教師、軍職人員及各機關學校約聘僱人員、技工、工友、正式工員、駐衛警察與臨時、勞力派遣人員，

計34萬3,861人，其中行政機關228,913人、公營事業機構69,137人、衛生醫療機構19,676人、公立學校(職員)26,135人。**換言之，本次計有全國70.77%之公務人員個資遭到外洩，等於每3人中至少有2人資料遭到外洩達7年之久**。

（2）資料範圍包含中央及地方機關公務人員之銓敘送審歷史資料(送審資料期間約為民國94年1月至101年6月1日)，不含軍職人員及約聘雇人員共243,376筆，其中外洩範圍包含國安局、行政院海巡署、內政部警政署、內政部移民署及法務部調查局等機關文職人員之送審基本資料。

（3）承上，所謂文職人員之定義，該部說明略以「，依憲法第九章考試院為國家最高考試機關……，依公務人員任用法任用需送銓敘部銓敘審定之公務人員屬文職人員之範疇」等語；**惟業務內容機敏與否與文職或軍職無涉，以法務部調查局及所屬調查處為例，自首長至調查員及調查官等共洩漏約2000餘人，故本案對國家安全之傷害，自不得以所洩個資僅限文職人員而有所稍減，況國外論壇所揭露者未必與實際外洩數量相當，實際外洩情形難以估計**，銓敘部實應負起相關責任。

(二)綜整銓敘部資安管理沿革及本案大事記如下：

時間	事件
90年1月	行政院國家資通安全會報成立，並制定「資訊系統分類分級與鑑別機制參考手冊」(104年7月改為「資訊系統分級與資安防護基準作業規定」)
90年3月	國家資通安全會報技術服務中心(技服中

	心)成立。
92年6月	銓敘部「銓敘業務網路作業系統」上線運作
93年7月	銓敘部舊公文系統開發建置
98年	國家資通安全會報制定「政府機關（構）資訊安全責任等級分級作業施行計畫」(104年改為「政府機關(構)資通安全責任等級分級作業規定」) 銓敘部成立資安委員會，並導入ISMS，驗證範疇僅「退撫查驗系統」。
99年1月	銓敘部取得ISO27001驗證
101年6月1日下午3時	研判本案資料外洩時間(外洩範圍為94年1月4日~101年6月1日歷史收文資料)
104年3月	銓敘部舊公文系統下線(新系統上線)
104年7月	行政院「資訊系統分類分級與鑑別機制參考手冊」改為「資訊系統分級與資安防護基準作業規定」 行政院「政府機關（構）資訊安全責任等級分級作業施行計畫」改為「政府機關(構)資通安全責任等級分級作業規定」
105年10月	銓敘部ISMS驗證範圍由「退輔查驗系統」,擴大為資訊室所管理之系統，含本案「銓敘業務網路作業系統」及「公文管理及線上簽核系統」。
108年1~3月	資通安全管理法及六項子法施行，此前規定均停止適用。
108年5月14日	舊公文系統報廢
108年6月22日	行政院資安處接獲國家安全會議通報，有國外論壇(Raidforums)販售疑似銓敘部之公務人員個資約58萬筆。行政院技服中心隨即通報該部。
108年6月23	銓敘部確認58萬筆確為該部所有，隨即依資

日	安法向行政院通報為第三級事件。
108年6月25日	行政院資安處(含技服中心)會同調查局、刑事局組成專案團隊，進行事件調查及危害分析
108年7月1~5日	行政院資安處、調查局及刑事局進行該部全部資訊環境資訊安全檢測及相關採證、鑑識及調查作業
108年7月15日	行政院技服中心進行銓敘部資安稽核並提出報告。

(三)有關銓敘部導入ISMS過程及驗證範圍：

1、銓敘部說明，為配合行政院國家資通安全會報「建立我國資通訊基礎建設安全機制計畫」方案之推動，於98年先以該部「公務人員退休撫卹查驗作業系統」(下稱退撫查驗系統)為範圍，導入ISMS。

（1）查行政院國家資通安全會報網站公開資料[2]，行政院賡續推動「建立我國通資訊基礎設施安全機制計畫(94年至97年)」、「國家資通訊安全發展方案（98年至101年)」及「國家資通訊安全發展方案（102年至105年)」。

（2）次查，「**政府機關(構)資訊安全責任等級分級作業施行計畫」係依據「國家資通訊安全發展方案（98年至101年)」**第6、7項行動方案「推動資安治理」及「推動資訊與資訊系統分類分級」辦理。**其施行對象包括中央各政府機關(構)(含五院所屬機關(構))**，並敘明各政府機關（構）首長應負該管單位全盤資安成敗之責，以期落實執行成效。**並將上開政府機關(構)資安等級區分為A、B、C、D等四級，而銓**

[2] https://nicst.ey.gov.tw/Page/C008464A6C38F57C

敘部自前開計畫頒布迄今，均屬資安責任等級A級機關，爰應有相應之資安管理及防護水準。

（3）承上，茲將**資安責任等級**A級機關應執行之工作事項節錄如下表，其中ISMS推動作業備註即敘明：「**驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。**」

作業名稱	應執行工作事項
防護縱深	NSOC[3]直接防護/SOC[4]自建或委外、IDS[5]、防火牆、防毒、郵件過濾裝置
ISMS推動作業(註一)	通過第三者驗證
稽核方式	每年至少2次內稽
資安教育訓練(一般主管、資訊人員、資安人員、一般使用者	1.每年至少(3、6、18、3小時) 2.資訊人員、資安人員需通過資安職能鑑定
專業證照	維持至少2張資安專業證照
檢測機關網站安全弱點	每年2次
註一：驗證範圍應涵蓋機關（構）之核心業務資訊系統，並逐步擴大至全單位。	

2、銓敘部98~105年僅將「退撫查驗系統」納入ISMS驗證範疇，案涉系統「銓敘業務網路作業系統」及「公文管理及線上簽核系統」迄105年10月時才納入，101年外洩時尚未納入，前開系統既涉及全國公務人員(含國安機敏人員)個資，卻沒有納入驗證範圍。

（1）據復，該部「退撫查驗系統」係「銓敘業務網路作業系統」最重要之子系統，其中退撫查驗

[3] NSOC，National Security Operation Center，國家資通安全防護管理平臺。
[4] SOC，Security Operation Center，資訊安全監控中心。
[5] IDS，Intrusion Detection System，入侵偵測系統。

子系統係提供全國各人事機構辦理公務人員退撫發放作業時，進行領受人員資格查驗及發放業務使用，除與其他組編歸系、任用審查、考績及退休撫卹等各項子系統關係緊密外，並需由部外機關提供相關個人資料，因所涉及個資種類眾多及數量龐大，且使用者為全國各人事機構人事人員。換言之，該部認為於98年以「退撫查驗系統」為主體進行驗證，即可同時防護「銓敘業務網路作業系統」之其他子系統。

（2）惟查，縱然「退撫查驗系統」係為「銓敘業務網路作業系統」最重要之子系統，但核心子系統通過ISMS驗證，仍不能代表整體系統均能通過ISMS驗證。

（3）行政院資安處簡宏偉處長於本院詢問時亦說明：「……驗證廠商在驗證時，驗證範圍要能說得清楚才可以，資安法其中就有要求核心系統要全部納入，而且3年內要納入，這是法遵事項」等語。

3、再查，本案既屬「未涉及關鍵基礎設施維運之**核心業務資訊遭嚴重洩漏」之**第3級資通安全事件，該部「銓敘業務網路作業系統」及「公文管理及線上簽核系統」卻自98年迄105年，長期未納入ISMS驗證範圍，該部亦未將驗證範圍逐步擴大至全單位，顯然未能確實依照「政府機關（構）資訊安全責任等級分級作業施行計畫」辦理，使全國公務人員個資長期處於ISMS驗證不完整之狀態，而使有心人士有機可趁。

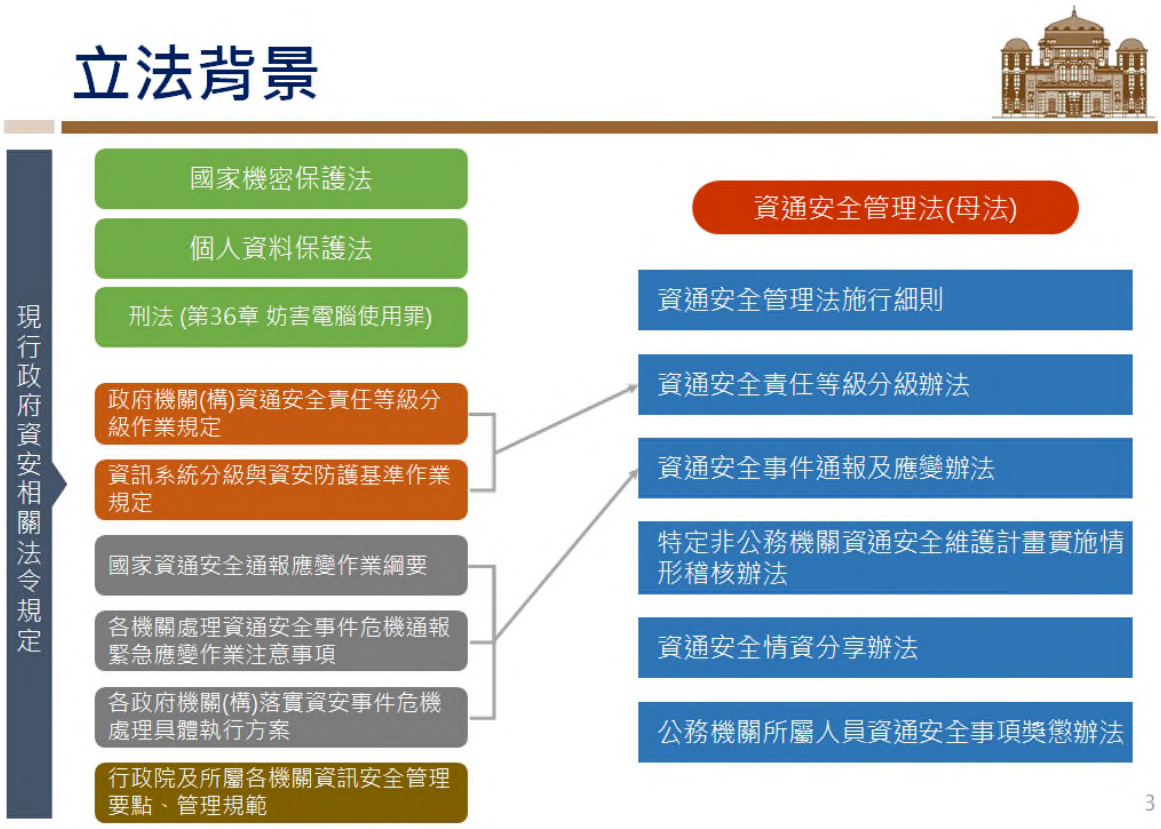
(四)綜上，銓敘部未能積極配合98年起推動之「政府機關（構）資訊安全責任等級分級作業施行計畫」，迄105年10月始將可存取全國公務人員銓審資料之

「銓敘業務網路作業系統」及「公文管理及線上簽核系統」納入ISMS(資訊安全管理制度)驗證範圍，使含機敏機關在內之全國公務人員個資長期暴露於高風險環境，爰本案58萬餘筆個資洩漏，該部難辭其咎，顯有違失。

二、銓敘部於108年發現資料外洩以前，長期將案涉「銓敘業務網路作業系統」及「公文管理及線上簽核系統」低估為安全等級中級，未能依照「資訊系統分級與資安防護基準作業規定」四大構面予以詳實評估，以致相關系統防護基準不足，益證該部長期漠視全國公務人員個資之洩漏風險，確有怠失。

(一)「資訊系統分級與資安防護基準作業規定」沿革及內容。

1、行政院國家資通安全會報於90年1月成立，隨即制定「資訊系統分類分級與鑑別機制參考手冊」，於104年7月改為「資訊系統分級與資安防護基準作業規定」，108年1月資通安全管理法通過後，相關規定即納入子法「資通安全責任等級分級辦法」中，茲將108年前後相關法令整併結果簡單整理如下圖：



2、按「資訊系統分級與資安防護基準作業規定」，安全等級分為【普】、【中】、【高】三級，由機關依機密性、完整性、可用性及法律遵循性四大影響構面，分別考量資訊系統於發生資安事件時可能造成之衝擊，即衡量資訊系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級，並有「**資訊系統之安全等級，取其四大影響構面安全等級最高者**」之規定，且須每年加以檢討，並奉機關資安長核定。

（1）資訊安全等級不同，其防護基準之控制措施要求標準及嚴謹程度自亦有別，包含存取控制、稽核與可歸責性、營運持續計畫、識別與鑑別、系統與服務獲得、系統與通訊保護、系統與資訊完整性等8大項目之內容，均有相當差異，其遭入侵竊取資料之難易度亦有所不同。

（2）舉例而言，按行政院國家資通安全會報於104年7月修正之「資訊系統分級與資安防護基準作業規定」，安全等級【普】、【中】、【高】之系統於存取控制之帳號管理即有下列強度不同之控制措施：

存取控制 (Access Control)	安全等級		
	普	中	高
帳號管理 (Account Management)	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序	1.執行等級「普」之所有控制措施。 2.資訊系統已逾期之臨時或緊急帳號應刪除或禁用。 3.應禁用資訊系統閒置帳號。 4.應定期審核資訊系統帳號之建立、修改、啟用、禁用及刪除動作。	1.執行等級「中」之所有控制措施。 2.當超過機關所規定之預期閒置時間或可使用期限時，系統應自動將使用者登出。 3.資訊系統應依照機關所規定之情況及條件(如上班時間或指定IP來源)，使用資訊系統。 4.監控資訊系統帳號以發現違常使用，並於發現帳號違常使用時回報管理者。

（3）此外，銓敘部係依資安法訂定及實施資通安全維護計畫、指派副首長兼任資通安全長。

(二)銓敘部相關資訊系統分級情形,該部查復說明如下:

1、該部107年資訊系統分類分級情形，納入評估之20個系統，屬「非系統開發機關」者計10個，安全等級「中」者計7個，安全等級「低」者計3個，而本案可能涉及外洩之系統「銓敘業務網路作業系統」及「公文管理及線上簽核系統」於安全等級均屬中級。

2、據復，該部係依資產評估與風險管理作業程序辦理評估資訊資產之風險後核列安全等級，並針對

個別資訊資產可能的風險情境，逐一評定風險發生機率與風險衝擊大小後，決定相關資訊資產安全等級。其中關鍵性評估因素之一為風險發生機率，主要依過往發生機率評量可能性等級，該部自105年起擴大驗證範圍為「銓敘部資訊室所管理之資訊系統」，又該部歷來並無重大資安事件發生(除108年6月22日事件外)，是以相關系統風險發生機率評值較低，爰歷年皆核列為中級。

(三)承上，該部案涉資料庫既存放含國安機敏單位在內達24萬餘人之全國公務人員個資，該部未考量機密性及法律遵循性，長年將可存取前開資料庫之「銓敘業務網路作業系統」及「公文管理及線上簽核系統」核列為安全等級中級。其怠失甚為明確。

1、該部林文燦次長於本院詢問時亦坦承：「我們同意(安全等級)應該要高級，而且現在(指詢問時)就已經是高級」。

2、行政院於實地稽核中，亦指出該部安全分級多以服務中斷為考量，建議將系統內存放資料之機敏性一併納入，並遵循「資通安全責任等級分級辦法」附表九「資通系統防護需求分級原則」，重新檢視系統分級，避免低估資通系統之重要性。

(四)此外，該部將國安機敏單位與一般機關人員個資置於相同保護機制下，並未針對機敏單位之銓審資料另行加密或隔離處理，亦有未妥；惟該部已於本案發生後規劃對於資料庫內一般人員之個人資料識別欄位進行去識別化處理，另對機敏人員則進行資料實體隔離作業。

(五)綜上，銓敘部於108年發現資料外洩以前，長期將案涉「銓敘業務網路作業系統」及「公文管理及線上簽核系統」低估為安全等級中級，未能依照「資訊

系統分級與資安防護基準作業規定」四大構面予以詳實評估，以致相關系統防護基準不足，益證該部長期漠視全國公務人員個資之洩漏風險，確有怠失。

三、銓敘部核列案涉系統為安全等級中級已屬低估，而行政院資安處於108年案發後協助稽核更指出，該部未能就中級防護基準之控制措施或ISMS四階文件內容妥予落實、驗證及追蹤改善情形，更肇致本案因缺乏資料庫稽核日誌，無從追查洩漏方式，顯示該部系統實際防護水準恐低於安全等級中級，均有改善必要。

(一)茲節錄行政院技服中心協助銓敘部進行資安稽核，與本案關係較為密切之建議如下，其中部分項目業於前開調查意見敘及，爰不贅述:

1、在策略面

(1)「資訊系統分級與資安防護基準作業規定」(均於資通安全管理法108年施行後廢止)之防護基準，分別訂有通行碼複雜度、最少變更字元數、最短及最長之字元數、資訊系統應遮蔽之資訊，以防止未經授權之使用者可能窺探與使用及資訊系統開發安全應以檢核表方式進行確認等規定，經抽查發現，銓敘部「銓敘業務網路作業系統」及「公文管理及線上簽核系統」未依規定辦理前述事項。

(2)若干內外部稽核所提出之建議改善事項，歷經多時仍未有效改善(如104年之使用者安裝軟體控管、107年之U槽存取安全控管等)。

(3)機關於106及107年資訊安全委員會管理審查會議所提報之資訊安全目標量測指標「資料庫遭未授權存取或異動事件」發生次數為0，惟因機關無啟動資料庫稽核日誌，前述指標如何量

測其可信度，宜進一步釐清。

2、管理面：

（1）針對人員離職時，帳號存取權限收回、停用或移除之處理，未有明確之作業流程。針對特權帳號之管理，亦欠缺明確規範。應依「資通安全責任等級分級辦法」附表十「資通安全防護基準」規定，加強人員之帳號權限管理機制。

（2）對於廠商使用維護帳號，未留存使用紀錄，如有出現異常登入，將無法查驗，應依「資通安全責任等級分級辦法」附表十「資通安全防護基準」規定，留存廠商使用帳號相關紀錄，以利稽核。

（3）廠商維護未留存紀錄，且維護時使用自行攜帶並可上網之筆電，建議後續廠商維護時，使用單位所準備且未上網的電腦，提供適當權限之帳號，以降低間接受駭之風險。

3、技術面

（1）依「資通安全責任等級分級辦法」附表十「資通安全防護基準」規定，資通系統之開發、測試及正式作業環境應為區隔，目前機關內網尚未完成存取控制,應儘速區隔資通系統之開發、測試及正式網段。

（2）依「資通安全責任等級分級辦法」附表十「資通安全防護基準」規定，中、高等級之資通系統需注意版本控制與變更管理，抽查發現銓敘業務網路作業系統目前並無源碼(source code)版本管理，機關應重新盤點並針對中、高以上資通系統建立一致性之版本控制機制。

（3）資通系統目前透過遠端登入進行程式上版，經抽查發現銓敘業務網路作業系統並未執行遠端

登入之權限審查，機關應針對所有的資通系統建立一致性之權限審查流程，並落實執行。

（4）目前資訊資產文件(如網路架構圖)較不完整，對於業務交接恐較困難，亦造成資安風險，建議強化文件完整度。

(二)次查，銓敘部與本院同為非屬行政院所轄之資安責任等級A級機關，但該部經行政院技服中心協助查核結果，與本院近年ISMS驗證結果相較，該部資通安全落實程度確有改善空間，茲舉下列數點為證：

1、該部電子郵件仍未採純文字讀取。

2、該部使用者電腦安全防護檢測結果，在29台受測電腦中，檢出2個惡意程式、13台未更新安全性、14台未更新java、22台未更新Adobe Reader、11台未更新Adobe Flash Player，其比率實屬偏高。

3、基於密碼之鑑別資通系統應強制最低密碼複雜度，但檢測結果顯示，該部同仁使用密碼字串過於簡單(使用5碼數字組合)。

(三)有關案涉資料庫未能開啟資料庫稽核日誌，以致無法追查洩漏原因一節:

1、查**該部自訂**之ISMS四階文件中之「銓敘部資訊安全管理制度資訊安全實施綱領」(第2.7版)，玖.執行資訊安全/九.系統稽核工具章節中載明略以：「.....**為保護相關稽核軌跡紀錄，應建置log集中伺服器，並安排專人管理，以保護稽核軌跡紀錄之安全與完整性**」，惟本案發生後，相關協助機關敘明如下：

（1）行政院說明，銓敘部之數位日誌(Log)保存不完整，可供研判之跡證有限，增加釐清資料外洩管道之難度。

（2）法部部調查局說明，該部資料庫主機未對所有

資料庫schema(資料庫結構)開啟稽核功能，已無從追查駭客竊取資料之手法與確切時間。

（3）刑事局針對銓敘部伺服器主機、個人電腦系統進行伺服器映像檔取證、數位日誌(Log)與惡意程式分析;但囿於該部相關Log資料保存未臻齊全，可供研判之跡證有限，難已確認具體資料外洩範圍。

2、銓敘部資訊室方映鈞主任則於本院辦理詢問時，針對資料庫稽核日誌一節說明略以：「過去是因為資料很大，不容易存，但現在都改善了」等語，足證該部過去並未澈底落實自訂之ISMS文件內容。

(四)綜上，銓敘部核列案涉系統為安全等級中級已屬低估，而行政院資安處於108年案發後協助稽核更指出，該部未能就中級防護基準之控制措施或ISMS四階文件內容妥予落實、驗證及追蹤改善情形，更肇致本案因缺乏資料庫稽核日誌，無從追查洩漏方式，顯示該部系統實際防護水準恐低於安全等級中級，均有改善必要。

四、銓敘部將ISMS輔導及驗證工作委由單一廠商辦理，未予適當切割，以致監督制衡效果不彰、驗證有欠獨立客觀，相關SOC、滲透測試、弱點掃描及資安健診等措施亦未發生效用，有欠周妥，而該部委外模式在各機關間並非個案，行政院既為資通安全法主管機關，宜針對相關風險研謀適當改善措施。

(一)ISMS導入及驗證相關規定沿革。

1、行政院國家資通安全會報於98年制定「政府機關（構）資訊安全責任等級分級作業施行計畫」，將資安等級區分為A、B、C、D四個等級，並區分為政府機關、學研機關（構）各事業分組及其他等

四組，其中核列安全責任等級B級以上機關，需通過ISMS第三方驗證。

2、104年1月，行政院資通安全會報將「政府機關（構）資通安全責任等級分級作業實施計畫」修正為「政府機關（構）資通安全責任等級分級作業規定」，其中A級機關應辦理之工作事項摘述如下表。

作業名稱 / 等級	資訊系統分類分級	ISMS 推動作業	資安專責人力	稽核方式	業務持續運作演練	防護縱深	監控管理	安全性檢測	資安教育訓練(一般主管、資訊人員/資安人員、一般使用者	專業證照
A 級	1.完成資訊系統分級(104 年底前) 2.完成資訊系統資安防護基準要求(105 年底前)	1.全部核心資訊系統完成 ISMS 導入(105 年底前) 2.全部核心資訊系統通過第三方驗證(106 年底前)	指派資安專責人力 2 人	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	1.防毒、防火牆、郵件過濾裝置 2.IDS/IPS、Web 應用程式防火牆 3.APT 攻擊防禦	SOC 監控(104 年底前)	1.每年至少辦理 2 次網站安全弱點檢測 2.每年至少辦理 1 次系統滲透測試 3.每年至少辦理 1 次資安健診	1.每年資安人員(資訊人員)至少 2 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練 2.每年一般使用者與主管至少須接受 3 小時資安宣導課程並通過課程評量	每年維持至少 2 張國際資安專業證照與 2 張資安職能訓練證書之有效性

3、108年1月1日，資通安全管理法之子法：「資通安全責任等級分級辦法」施行(108年3月5日「政府機關（構）資通安全責任等級分級作業規定」停止適用)，將適用對象訂為公務機關及特定非公務機關兩者，並將安全責任等級區分為A、B、C、D及E五級，自此ISMS推動相關作業已具備明確法律依據。

(二)銓敘部ISMS推動作業委外情形

1、查該部105至108年，將ISMS推動作業分別以「105年度ISO27001變更驗證範圍輔導暨資訊安全管理制度(ISMS)維護委外服務案」、「106年ISO27001驗證續評輔導暨資訊安全管理制度(ISMS)維護委外服務案」、「107年ISO27001重新評審輔導暨資訊安全管理制度(ISMS)維護委外

服務案」、「108年ISO27001驗證續評輔導暨資訊安全管理制度(ISMS)維護委外服務案」等委外辦理。

2、查該部ISO27001自100年迄今驗證稽核廠商如下：

年度	100	101	102	103	104	105	106	107	108
委外廠商	BSI[6]	BSI	BSI	BSI	BSI	SGS[7]	SGS	SGS	TCIC[8]

3、行政院於108年7月15日赴銓敘部提出之實地稽核報告指出銓敘部「目前資安健診、滲透測試、弱點掃描、SOC監看、ISMS輔導及驗證皆委由單一委外廠商辦理，建議對委外案進行適當切割，達到委外案間互相監督效果」等語。

4、次查，銓敘部雖有辦理SOC、滲透測試、弱點掃描及資安健診等措施，但技服中心108年7月檢測時，仍發現93年6月4日至108年6月25日有多部系統主機陸續遭植入50餘支惡意程式，相關措施未能發揮應有效果。對此，該部說明，歷年係委由專業資安廠商辦理SOC、滲透測試、弱點掃描及資安健診等措施，亦依檢測結果進行相關因應及修補作業，惟**囿於預算檢測範圍僅以提供外部服務之伺服主機為主，該部規劃相關資安檢測作業擴大至全部主機。**

(三)有關銓敘部將ISMS推動作業委外辦理，委外廠商未能協助機關澈底落實ISMS內容及發掘潛在威脅，該部亦未就上開情形加以掌握，相關佐證如下：

1、行政院於查復資料說明:「銓敘部每年委外辦理

[6] 香港商英國標準協會太平洋有限公司台灣分公司。
[7] 台灣檢驗科技股份有限公司。
[8] 環奧國際驗證有限公司。

資訊安全管理系統(ISMS)輔導及驗證、資安威脅預警監控(SOC)、資訊系統滲透測試、主機弱點掃描及資通安全健診等服務，未能有效協助機關發掘潛在威脅」等語。

2、換言之，機關將**ISMS委外輔導與第三方驗證案合併辦理，且驗收條件又為通過第三方驗證，恐有球員兼裁判**，驗證機構不易維持獨立性之虞。

3、承上，有關驗證機構獨立性之把關，行政院資安處協助進行銓敘部稽核時，發現驗證公司未能落實查核，故已向財團法人全國認證基金會(TAF)提出，**TAF即啟動專案調查，認定驗證機構未保持驗證之獨立性**，因此做出減列處分，益證前開合併委外模式確有相當風險。

4、行政院資安處簡宏偉處長於本院詢問時亦指出「從資訊業務委外後，**連核心職能都委外**了，委外管理上，21家廠商是輔導，驗證廠商部分是受TAF管理的，都有一個制度去檢視他們符不符合」等語。

(四)再查，該部於「資通安全作業管考系統」填報之防護基準控制事項「符合」比例甚高(以105年為例，「銓敘業務網路作業系統」共48個控制項目僅有3個不符合)，與108年行政院赴該部協助稽核，該系統僅抽查13項就有8項不符合，其符合防護基準之程度顯有相當差距，其中縱有因各年度防護基準有所增修，尚難以同一標準衡量，但仍顯示行政院以相較驗證機構更為客觀之立場進行稽核，更能協助機關發掘潛在威脅。

1、對此，行政院亦說明，各機關至管考系統所填報事項，為針對應辦事項之自評結果，其目的在了解各機關之應辦事項是否辦理，至於辦理情形及

是否落實，仍有待透過內部及外部資通安全稽核機制，始得確認機關各構面資通安全防護之完整性及有效性。

2、為改善上述情形，108年於資通安全管理法強化第二方驗證，要求各上級機關應稽核所屬機關之資通安全維護計畫實施情形，協助所屬機關落實資通安全維護工作，以落實分層監督管理機制。

(五)按108年8月26日最新修正之「資通安全責任等級分級辦法」(資通安全法子法)規定，無論等級為A、B、C級(D、E級除外)之公務機關或特定非公務機關，除驗證範圍及完成年限有所不同，推動ISMS導入及通過驗證均為法遵事項，而相關規定亦未明定不得合併辦理，爰行政院所指銓敘部合併辦理恐有球員兼裁判，不易互相監督制衡一節，恐非個案，主管機關宜針對相關風險研謀適當改善措施。

1、據行政院資安處查復，國內資安管理輔導廠商，該處所知悉之國內ISMS輔導廠商計有三甲科技、中華電信、台灣應用軟件、安侯企業、安碁資訊、昇達價值管理、美思科法、財團法人中華民國國家資訊基本建設產業發展協進會、偉立資訊、創逸科技、博創資訊、勤業眾信、資拓宏宇、資誠聯合會計事務所、漢昕科技、精誠科技、德欣環宇、德諾科技、數聯資安、璞方科技、聯準科技等21家。目前機關存在委託單一廠商統包SOC、ISMS驗證等情形，就現已瞭解資訊，尚難認定此一情形之普遍性。

2、行政院資安處簡宏偉處長亦於本院詢問時說明：「**我們發現政府機關為了採購方便，輔導和驗證是綁一起**，我們正在研擬驗證要透過共同供應契約」等語，顯見現行ISMS輔導驗證模式顯有改善

必要。

(六)綜上，銓敘部將ISMS輔導及驗證工作委由單一廠商辦理，未予適當切割，以致監督制衡效果不彰、驗證有欠獨立客觀，相關SOC、滲透測試、弱點掃描及資安健診等措施亦未發生效用，有欠周妥，而該部委外模式在各機關間並非個案，行政院既為資通安全法主管機關，宜針對相關風險研謀適當改善措施。

五、銓敘部長期缺乏資安人力資源，不僅有網管人員兼任資安工作、需投入大半人力自行開發或增修相關業務系統及人員流動率高等問題，更難以掌握ISMS輔導及驗證品質，均有改善必要；而資通安全相關法遵及技術知能要求與日俱增，其挑戰不獨為銓敘部所有，行政院對於現行資安相關職系核心職能及培訓方式已規劃改善措施，宜持續推動並澈底落實，始能厚植機關資安專業，俾達成「資安即國安」之目標。

(一)根據「政府機關（構）資通安全責任等級分級作業規定」，A級機關之資安人力及證照要求如下，而銓敘部填報於「資通安全作業管考系統」之資料，均符合相關規定，合先敘明。

1、資安人力：指派資安專責人力2人。

2、專業證照：每年維持至少2張國際資安專業證照與2張資安職能訓練證書之有效性。

3、該部說明，確依規定每年辦理資安教育訓練，相關資安證照之取得亦符合規定(取得資安專業證照[ISO27000l主導稽核員]證照2張及資安職能評量證書5張)

4、查該部登錄於「資通安全作業管考系統」之資料，該部107年具有以下證照。分別為國際資安專業證照(兩張ISO/IEC 27001:2013 Lead Auditor)

及資安職能訓練證書(含資安事故處理、資訊系統風險管理、電子資料暨個資保護管理、電子郵件安全等證書)。

(二)惟查，行政院卻於108年7月因本案復該部協助稽核時指出，在人力面，銓敘部資通環境業務不斷擴增及增加複雜度之同時，**資訊室同仁資安管理及技術知能未同步提升**，且高度仰賴委外廠商及同仁未建立資安風險意識之情形下，形成資安防護罅隙；該院資安處簡宏偉處長於本院約詢時亦有「連核心職能都委外」等語。對此，銓敘部說明，因該部業務屬性，需投入大半人力自行開發或增修相關業務系統，以致多由網管人員兼任資安人員，人力不足加上人員異動流動率高，易造成知識傳承及工作銜接不易。另資安技術職能培訓部分需長期投注資源及經驗培育，目前依規定辦理之短期訓練不易發揮功效。

1、承上，以銓敘部資通環境業務不斷擴增及增加複雜度之情形下，其資通安全人力顯然不能只符合「政府機關（構）資通安全責任等級分級作業規定」之要求；更嚴峻的問題在於，由於前開規定屬於最基本的人力要求，此種**符合規定卻不符合實需之情形，銓敘部恐非個案**，實不利於達成「資安即國安」之目標。

2、銓敘部則說明，該部目前已增加資安專職人員1名，並就現有資訊人力，將盡速移撥增加資安人力，持續投注訓練資源以強化資安技術人力素質，並定期辦理後續資安工作稽核，以確認控制措施能有效執行。

(三)次查，在資通安全法施行後，A級機關依法應配置4名資安專職人力，以銓敘部為例，含資訊室主任在

內僅編制14人為例，資安專職人力需佔到近三成，對業務執行實為艱鉅之挑戰，對其他機關而言亦復如是。對此，行政院說明及規劃如下：

1、依法配置資安專職人力並進行資通安全專業訓練：配合資安法之施行，資安責任等級A級機關應配置4名資安專職人力，此人力將賦予全職扮演機關內部資安管理及獨立檢視機關資通安全業務之角色，且資通安全專職人員應依法每年至少接受12小時以上之資通安全專業課程訓練或資通安全職能教育訓練；其他資訊人員、一般使用者及主管，亦應依法接受專業或通識訓練。

2、建立資安專職人員職能鑑別機制：為提升資安人力專業知能，本院資通安全處已依資安專職人力職能需要，建立職能發展地圖及獨立資安職能評量制度，評測資安人員知識與技能。

3、建立機關人員資通安全事項獎懲機制：資安法已訂有「公務機關所屬人員資通安全事項獎懲辦法」，各機關可就其所屬人員辦理業務涉及資通安全事項，自行訂定獎懲基準，以促進該等人員對於資通安全工作之重視與投入。

4、機關首長之重視仍為首要之務：因人員及經費配置均為機關首長之權責，資安法已賦予各機關編列預算與人力之法律依據，機關首長應依資安法規定，於機關總員額範圍內，優先調配資安專職人員，又機關經費之運用亦然，爰機關首長主動考量業務及資訊發展需要，合理調配必要之資源仍為首要之建議。

5、新增資通安全職系，以利培養專才:因資通安全雖屬資訊業務之一環，然其實質上分屬不同專業領域且資安業務日益繁重，本院資通安全處有感

於公務資安人力不足，建議考試院於公務人員晉用管道增列資通安全職系，俾利各機關專才專用。

6、協助機關補實資安專職人力：配合資安法之施行，資安責任等級A、B及C級機關應配置4人、2人及1人資安專職人員，該院資通安全處及該院人事行政總處刻正研擬協助各機關補實資安專職人力之措施。

7、協助機關爭取經費提升資安防護能量：近年政府財政有限，各機關預算難以大幅成長，另跨院經費相互協助之適法性仍待釐清，該院現已透過資安旗艦計畫及前瞻基礎建設計畫，投入資安預算改善資通安全環境，後續仍將持續在可得之資源下協助機關完善資安防護措施。

(四)綜上，銓敘部長期缺乏資安人力資源，不僅有網管人員兼任資安工作、需投入大半人力自行開發或增修相關業務系統及人員流動率高等問題，更難以掌握ISMS輔導及驗證品質，均有改善必要；而資通安全相關法遵及技術知能要求與日俱增，其挑戰不獨為銓敘部所有，行政院對於現行資安相關職系核心職能及培訓方式已規劃改善措施，宜持續推動並澈底落實，始能厚植機關資安專業，俾達成「資安即國安」之目標。

參、處理辦法：

一、調查意見一至五，函請銓敘部確實檢討改進見復。

二、調查意見四、五，函請行政院確實檢討改進見復。

調查委員：仉桂美

劉德勳

包宗和

中　　華　　民　　國　109　年　2　月　21　　日