公務人員對行政中立應有之認識

公務人員本於依法行政之原則，應熟悉中立法之內容並嚴守其規定。

◎李志強

壹、前言

公務人員行政中立法（以下簡稱中立法）草案於今（98）年 5 月 19 日經立法院第 7 屆第 3 會期第 13 次會議完成三讀程序，並於同年 6 月 10 日公布實施。其實早在 80 年間，銓敘部即提出建立文官行政中立法制構想，隨後從蒐集各國法案、徵詢各機關意見、邀集學者專家座談、向考試及立法委員提出簡報、綜整各界意見研擬草案，到送交立法院審議通過，期間歷經十餘年終於定案。

依據先進民主國家之經驗，政黨政治與文官中立兩者相輔相成，不可偏廢。申言之，既要有成熟的政黨政治，使政黨透過選舉程序取得執政地位，經由其選任之政務官及民意代表，制定政策及法律；另方面，也須有健全的文官體系，使常任事務官嚴守中立與公正之立場，忠實執行政令，以維持國家政務之安定成長，此乃我國制定中立法之宗旨。

國內每逢選舉，公務人員被動員情形及官員動用行政資源等議題，往往成為各政黨及候選人相互攻訐之目標，也是社會輿論關切之焦點。現今中立法既已實施，公務人員之行為分際在明確依據可資遵循下，不僅可避免無謂之困擾，同時也可維護自身相關權益，進而落實建立廉能國家之施政目標。為使公務人員及社會各界了解中立法之內涵，以下歸納說明之。

貳、規範重點

中立法共計 20 條條文，其內容包括明確規定公務人員參與政治活動之權利、限制及保障；各機關首長或主管人員於公職人員選舉期間之相關限制；長官不得要求所屬公務人員從事本法禁止之行為，以及公務人員如因拒絕從事禁止行為而遭受不公平對待或不利處分之救濟管道等事項。

一、立法目的

中立法第 1 條開宗明義揭示其立意是為確保公務人員依法行政、執行公正、政治中立，並適度規範公務人員參與政治活動。

二、適用對象

中立法所稱公務人員，指法定機關依法任用、派用之有給專任人員及公立學校依法任用之職員（第 2 條）。另於同法第 17、18 條定有準用對象，範圍如下：

1. 公立學校校長及公立學校兼任行政職務之教師。
2. 教育人員任用條例公布施行前已進用未納入銓敘之公立學校職員及私立學校改制為公立學校未具任用資格之留用職員。
3. 公立社會教育機構專業人員及公立學術研究機構研究人員。
4. 各級行政機關具軍職身分之人員及各級教育行政主管機關軍訓單位或各級學校之軍訓教官。
5. 各機關及公立學校依法聘用、僱用人員。
6. 公營事業機構人員。
7. 經正式任用為公務人員前，實施學習或訓練人員。
8. 行政法人有給專任人員。（註：包括行政法人有給專任之董《理》事長、首長、董《理》事、監事、繼續任用人員及契約進用人員）
9. 代表政府或公股出任私法人之董事及監察人。（上述屬第 17 條之規定）
10. 憲法或法律規定須超出黨派以外，依法獨立行使職權之政務人員（第 18 條）。其他非本條文之政務人員雖排除適用，惟為維護政黨間或選舉時之公平競爭，則另於政務人員法草案中予以規範。

此需說明者，軍人、教師及法官雖非中立法適用對象，然依立法說明，軍人行政中立之標準理應高於公務人員，且基於文武分治原則，自應依法及職務特性，於相關軍事法令中另予規範。教師由於從事教學、研究工作，並享有憲法保障之言論、講學等自由，且教師法公布施行後，教師與公務人員已分途管理，而教師之權利義務亦於教師法中加以規範，故如要求其行政中立，宜因其職務特性而於教師法中明定。法官依據憲法第 80 條，從事審判之行為須超出黨派以外，依據法律獨立審判，原即不受本法之規範；然法官審判外之行為仍適用中立法，惟如其他法律有更嚴格規定者，依中立法第 1 條第 2 項，自當從其較嚴之規定。由於法官法草案對於法官行政中立之標準高於中立法，故從其規定不將法官列為適用對象。

三、行政中立之原則

1. 依法行政原則：公務人員應嚴守行政中立，依據法令執行職務，忠實推行政府政策，服務人民。（第 3 條）
2. 公平對待原則：公務人員應依法公正執行職務，不得對任何團體或個人予以差別待遇（第 4 條），並以誠信公正原則處理事務。
3. 國家利益優先原則：依據主管機關銓敘部說明，行政中立之原則另包含國家社會之公共利益應超越黨派利益。

四、參與政治活動之權利

中立法除保障公務人員得加入政黨或其他政治團體之權利外（第 5 條前段）；另規定公務人員登記為公職候選人者，自候選人名單公告之日起至投票日止，應依規定請事假或休假，而長官對上述請假不得拒絕（第 11 條）。

五、參與政治活動之限制

綜觀中立法，其重點在於適度規範公務人員參與政治活動，可分為消極性的行為規範及積極性參與政治活動的限制規範兩種。前者除依法行政、公平對待等原則外，中立法第 12 條還明定「公務人員於職務上掌管之行政資源，受理或不受理政黨、其他政治團體或公職候選人依法申請之事項，其裁量應秉持公正、公平之立場處理，不得有差別待遇。」後者有關參與政治活動的限制部分，從中立法第 5 條至 14 條（第 11 條及第 12 條除外），篇幅幾占半數條文，重點如下：

1. 公務人員不得兼任政黨或其他政治團體之職務，不得介入黨政派系紛爭，亦不得兼任公職候選人競選辦事處之職務。（第 5 條）

2. 公務人員不得利用職務上之權力、機會或方法，使他人加入或不加入政黨或其他政治團體；亦不得要求他人參加或不參加政黨或其他政治團體有關之選舉活動。（第 6 條）

3. 公務人員不得於上班或勤務時間，從事政黨或其他政治團體之活動，但依其業務性質，執行職務之必要行為，不在此限。所稱上班或勤務時間，係指：1、法定上班時間。2、因業務狀況彈性調整上班時間。3、值班或加班時間。4、因公奉派訓練、出差或參加與其職務有關活動之時間。（第 7 條）

4. 公務人員不得利用職務上之權力、機會或方法，為政黨、其他政治團體或擬參選人要求、期約或收受金錢、物品或其他利益之捐助；亦不得阻止或妨礙他人為特定政黨、其他政治團體或擬參選人依法募款之活動。（第 8 條）

5. 公務人員不得為支持或反對特定之政黨、其他政治團體或公職候選人，從事下列政治活動或行為：
    a. 動用行政資源編印製、散發、張貼文書、圖畫、其他宣傳品或辦理相關活動。
    b. 在辦公場所懸掛、張貼、穿戴或標示特定政黨、其他政治團體或公職候選人之旗幟、徽章或服飾。
    c. 主持集會、發起遊行或領導連署活動。
    d. 在大眾傳播媒體具銜或具名廣告。
    e. 對職務相關人員或其職務對象表達指示。
    f. 公開為公職候選人站台、遊行或拜票。
    g. 其他經考試院會同行政院以命令禁止之行為。（第 9 條）

6. 公務人員對於公職人員之選舉、罷免或公民投票，不得利用職務上之權力、機會或方法，要求他人不行使投票權或為一定之行使。（第 10 條）

7. 各機關首長或主管人員於選舉委員會發布選舉公告日起至投票日止之選舉期間，應禁止政黨、公職候選人或其支持者之造訪活動；並應於辦公、活動場所之各出入口明顯處所張貼禁止競選活動之告示。（第 13 條）

8. 長官不得要求公務人員從事中立法禁止之行為。（第 14 條第 1 項）

六、罰則

中立法第 16 條規定，對違反本法之公務人員，應按情節輕重，依公務員懲戒法、公務人員考績法或其他相關法規予以懲戒或懲處；其涉及其他法律責任者，依有關法律處理。

七、救濟管道

公務人員若因行政中立有關事項，遭受不公平對待或不利處分時，依據中立法第 15 條第 2 項，得依公務人員保障法等相關法令之規定，請求救濟，以維護其權益。此外，中立法第 14 條亦明定，長官不得要求公務人員從事本法禁止之行為，對於違反者，公務人員得檢具相關事證向該長官之上級長官提出報告，並由上級長官依法處理；未依法處理者，以失職論，公務人員並得向監察院檢舉，此亦屬救濟途徑。

參、結論

猶記得中立法施行未久，即因本法第 17 條第 3 款將公立學術研究機構研究人員納為準用對象，而引發部分學術界強烈質疑，指有限制學術自由及剝奪言論自由等疑慮。在此姑且不論社會輿論及評價為何，但身為公務人員，本於依法行政之原則，確應熟悉中立法之內容並嚴守其規定，此應不容置疑。

（作者現任國立故宮博物院編審）

（本篇摘錄自法務部調查局清流月刊 98 年 10 月號）

政府機關為何要導入 ISMS

導入 ISMS 是為了保護政府機關的資訊安全，資訊安全的目標是設定機關內如何持續運作的資安管理目標與相關機制。

◎ 黃小玲

壹、前言

很久以前有一段相機底片的廣告詞曾提到：「我說…人活得好好的，他為什麼要拍照？」廣告詞的結尾則說：「我的天啊！什麼軟片這麼好啊？…一次 OK」。

許多資安負責人員的疑問是，如果我的現行運作機制維運良好，為什麼要導入資訊安全管理系統(Information Security ManagementSystem, ISMS)？而且導入 ISMS 後，機關是否等同服用萬靈丹，就可以藥到病除，一次 OK？

底片很神奇， ISMS 是否也一樣神奇？

貳、導入前的評估作業

政府機關若導入ＩＳＭＳ，涉及的範圍與衝擊對內部影響甚為重大，應審慎評估需求。導入 ISMS 包括的預算編列，必需考量項目，如輔導費用、控制措施調整或建置費用及後續驗證費用等，更遑論所投入之人力與時間成本。導入 ISMS 可以是一項非常耗費資源的工作，因此如何確保所投入成本之效益回收，需經由下述評估作業後，建議各政府機關依照所定義之策略目標與評量準則，進行是否需要導入 ISMS 之作業分析。

一、法律或規範的要求

1. 行政規範：政府機關導入ＩＳＭＳ有不同的需求來源，大部分的原因為自願性導入，認定機關確實存在著資安管理制度之需求，才決定導入 ISMS；至於部分非自願性的考量則為行政規範的要求。從 89 年開始每期 4 年的資通安全機制計畫，主要針對重要的政府機關建立一套完整的資通安全整體防護體系，包括資安專業人員的訓練、應變機制等防護；而該機制計畫亦包括重要政府機關(構)逐年通過資訊安全管理系統的驗證。政府若能從各機關先落實，再推向民間產業，共同建立完備的資安防護體系，並列入政府機關持續推動資安業務的範疇，則資安管理效益不言可喻。行政規範的符合通常是導入 ISMS 的主要考量，又因配合著機制計畫或是資通訊安全發展方案，施行計畫期程的設定，所以導入需求的急迫性與必要性反而容易被忽略。
2. 法律或合約要求：從法律的觀點來看，組織要考量的保護範圍是從個人資料至機關隱私，不論是內部管理或外部法律規範的要求，組織都應呈現積極的態度保護所擁有的資訊並建置完善管理的流程及相關的技術防護，以因應法律或合約的要求。資訊安全管理

系統在其條文中亦提及與法律規範條文的符合性；對所有政府機關來說，如何避免違反任何法律、法令、法規或契約義務，皆可列入導入 ISMS 的評量要點。

二、業務持續重要性與安全目標

導入 ISMS 是為了保護政府機關的資訊安全，而資訊安全的目標是設定機關內如何持續運作的資安管理目標與相關機制。

資訊安全的定義是考量維持資訊的機密性、完整性及可用性；同時還可以包括資訊的鑑別性、可歸責性、不可否認性及可靠性等方向。

資訊安全是讓組織在有限的資源(包括時間、人力及預算)內，確保政府機關可以維持服務不中斷，達成業務服務水準的協議，並取得下列三項基本安全要素的平衡點。

1. 機密性：確保只有被授權的人可以存取資訊。政府機關內部列入機敏性資訊分級者，皆應列入保護。
2. 完整性：確保資訊從產生開始、處置、存放及廢止時，處理方式的正確性與完整性。例如，如何確保網站資訊不被篡改與誤用。
3. 可用性：確保資訊在被授權人有需要時可以存取。例如：使用者在預先定義的時間或權限上是否可以存取。

圖 1：資訊安全目標示意圖

政府機關可以考量其所執掌的業務若是突然停頓或中斷，對國家、社會或民眾的衝擊分析或是所設定之安全目標後，再決定是否需要導入 ISMS。

三、組織風險考量

政府機關應考量所可能面臨之風險，面對這些風險來源時，是否已設定可接受之風險等級(Risk Acceptance Level)；如果風險為不可接受時，可考量 ISMS 所建議的最佳實作規範與控制措施是否為最佳的解決方案。

政府機關的風險來源可概分為以下幾種：

1. 資料外洩：因為業務流程相關資訊安全部分控管不佳，造成非授權人士可以存取。例如，某醫院曾傳出名人病歷外傳的事故，造成病人隱私受損並間接影響醫院名聲。
2. 內部員工的疏失或惡意行為：印出的業務報表任意擺放或是使用懶人密碼等等。例如，公務人員利用職務之便，任意出賣民眾資料以牟利。
3. 駭客威脅：系統上的弱點，可能吸引來自全球的駭客攻擊；包括針對一般使用者的社交工程手法，與鎖定特定機關的目標式攻擊手法。例如，電子郵件社交工程的受害者，可能造成使用者成為無意的加害者。
4. 資訊交換風險：政府機關若與法人組織或民間團體進行資訊交換時，亦應考量資訊交換上可能產生的風險。例如，醫療單位與健保相關單位進行資料傳輸或交換時的安全防護。
5. 公務家辦的風險：隨著一些儲存媒體的方便使用，公務家辦的趨勢與隨之而來的風險也逐漸增加。

政府機關需要考量不同的風險來源，分析現行的控制措施是否具備資訊安全管理的架構。當現行控制措施不足以降低風險等級時，或因現行控制措施缺乏一套管理機制時，亦可以列為導入 ISMS 的要素。

四、導入預期效益分析

政府機關雖然不像民營機構需要自負盈虧，但導入 ISMS 前的評估作業，應包括預期的效益分析；到底導入此管理系統，對機關的效益在那裏，而且是否值得這大量資源的投入。

下表為建議之預期效益分析：

表 1：ＩＳＭＳ導入前後預期效益分析

比較項目	ISMS導入前	ISMS導入後
清楚設定安全目標	未明確設定	可衡量指標
了解風險來源	被動回應	積極回應
業務所承擔之風險	風險高	風險降至可接受之等級
使用者操作信心	信心不足	信心高
使用者資安滿意度	滿意度低	滿意度高
資訊安全管理難度	分散式的資安管理	系統式的資安管理
資安事件回應速度	事件處理人力未有效管理	建立事件回應機制
資訊作業效率	人員經驗分享，效率低	定義標準作業程序書，效率高
內部稽核能力	缺乏專業人力	具規劃與實務能力

資訊安全管理系統的導入，如果事先未充分溝通清楚，容易產生管理階層或使用者對 ISMS 有過高的期待，以為資訊安全管理系統可以解決所有的資安事件，同時消弭所有可能之風險。導入前之效益評估與溝通，可以讓所有人對 ISMS 的效益有一致性的認知，如此方不會產生預期性之落差。

參、結論

當政府機關考量所有上述的情況後，可以在進行導入ＩＳＭＳ之前，列出評估項目與檢視表，以確認真正的需求是否已被清楚辨識。ISO(International Organization for Standardization, 國際標準化組織)相關的管理系統在國內組織環境內，若未進行實質的效益評估與內部資安需求的確認，則容易流於形式。如果政府機關只是為了導入而導入，為了驗證而驗證，逐漸地，資訊安全管理系統將淪為只是少數人負責維護的錯誤認知；縱使累積許多的資安政策與管理程序，卻未必能見到實質效益。因此 ISMS 導入前之評估，實在應謹慎為之。

參考文獻

- [1] ISO 27001：2005
- [2] ISO 27002：2005
- [3] 國家資通安全會報 94 至 97 年「建立我國通資訊基礎建設安全機制計畫」
- [4] 國家資通訊安全發展方案(98 年至 101 年)

（本篇摘錄自法務部調查局清流月刊 98 年 10 月號）

是誰破解了我的電腦

對資訊安全來說，沒有最安全，只有更安全。

◎魯明德

壹、案情摘要

這兩個月陸續發生了兩件看似影響不大的事，但是，見微知著，這些資訊安全的小疏失，往往會造成單位意想不到的損失，資訊管理者不可不察。

第一個案例發生在總統府，總統府為了拉近與民眾的距離，於今(98)年 7 月 18 日起推出馬總統的治國週記，不料馬上被網友發現總統府已預錄未來兩週的治國週記，而且把預錄的治國週記放到著名的影音網站 YouTube 上供人瀏覽。這讓總統府相當尷尬，很多媒體競相報導總統府的網站被「破解」了！

第二個案例則是 8 月間，新竹某明星高中的學生惡作劇，幫他同學上大學入學分發委員會的網站填寫分發志願，因為只填了一個臺大醫學系，而造成他的同學高分落榜。警方查出後以「妨害電腦使用罪」移送地檢署偵辦。

這兩件事乍看之下，風馬牛不相及，但是，究其根源，均為系統對於資訊安全的防範不夠所肇生的事端。本文將透過這兩個案例的解析，讓讀者了解資安事件發生的原因及資訊安全簡單的防範之道。

貳、案例解析

在第一個案例中，媒體的報導大都是馬總統治國週記網站被網友破解，究竟網友是怎麼「破解」總統府的網站？難道總統府的網站是不設防的嗎？其實不然，從媒體的報導中，可以發現：治國週報的影音檔，它的檔名是以發行時間做為檔名，而我們在瀏覽網頁時，在 IE 的網址列上，會把網址及檔案的路徑都顯示出來，所以，網友只要在網址上，依日期自行修改檔名，再按下 Enter 鍵，如果該檔名的檔案存在，就可以瀏覽了。所以，這種行為既沒有入侵網站，更談不上破解。

第二個案例就更奇特了，大學入學分發委員會進行選填志願的網站，考生只要輸入：身分證字號、准考證號碼、繳款號碼和通行碼，驗證通過就可以進入該網站填志願。根據《聯合報》的報導顯示：學校會把應屆畢業生的身分證字號、准考證號碼印成一整本，同學彼此都查得到，而繳款號碼及通行碼，可以從「大學考試入學分發相關資訊」本子上查到。

我們平常到提款機去領錢，一定要輸入帳號、密碼，讓系統確認提款人的身分，這是確保存款戶錢財安全的必要手段。我們在許多場合都可以看到這樣的提示警語：密碼不要寫在提款卡上，也不要用生日或容易讓人猜到的數字當密碼；這些都是在確保密碼的安全性。

上網填寫志願攸關考生權益，為了確認身分，考生必須輸入帳號、密碼，以驗證其身分，大學入學分發委員會採用身分證字號、准考證號碼、繳款號碼和通行碼同時輸入，做為驗證的工具，看似非常安全，不料，這些都可以讓有心人看到，這跟把密碼寫在提款卡上有什麼不同？

參、資訊安全防範之道

由於資訊科技的普及與快速發展，電子化企業已是目前的趨勢；對資訊的依賴愈深，資訊無法運作時，對企業的傷害也就愈大，所以資訊安全可說是每個企業的命脈。資訊安全的攻防就像矛與盾一樣，雙方都在不斷精進自己的武器。但是，隨著資訊產品的價格愈來愈便宜、功能愈來愈強，沒有什麼安全機制是不能被破解的，只是時間的長短而已；所以，對資訊安全來說，沒有「最安全」，只有「更安全」。

目前的網頁大多採用 3-tier 的架構，網頁所顯示的資訊，都來自後端的資料庫(Database)；在資料庫的運用上，通常是透過結構化查詢語言(Structured Query Language, SQL)進行。而最常發生在應用程式之資料庫層的安全漏洞就是 SQL Injection。

SQL Injection 是在輸入的資料字串之中夾帶 SQL 指令，設計不良的程式會忽略做 SQL Injection 的檢查，這些夾帶進去的指令就會被資料庫伺服器(Database Server)誤認為是正常的 SQL 指令而執行，因而招致破壞；只要是支援批次處理(Batch)SQL 指令的資料庫伺服器，都有可能受到此種手法的攻擊。因此，在設計系統時，一定要事先防範 SQL Injection。

密碼是進入系統的鑰匙，就像家裏大門的鑰匙一樣，一旦落到有心人士手上，家裏就門戶大開，即使有數道鐵門，都是沒有用的。入侵者最常用來竊取使用者密碼的方式就是暴力攻擊法(Brute Force Attack)，藉由程式來測試所有可能的密碼組合，進而找到使用者的密碼。

為了避免自己的密碼遭到暴力攻擊法的攻擊，必須要有足夠的複雜度，像以生日或與自己有關的數字、文字做為密碼，就很容易被破解。但是，複雜的密碼又不容易記，現在很多企業的系統，除了要求定期更換密碼外，還要有足夠的複雜度。在此，筆者提供兩個方法供讀者建立複雜度足夠又不易忘記的密碼。

第一個方式是截頭去尾，先設計一個句子，再把句中的母音去掉，如「I love Mjib」，去掉母音後剩下 lvmjib，再加上大小寫就可以組合出很多個密碼。第二個方式是使用拼音，同樣先設計一個句子，再用它的中文輸入法做為密碼，如「我愛清流」，用倉頡輸入就是 hqibbpeeqmbeyiu，也可以加上大小寫或結合截頭去尾法，就可以產生很多組密碼。

肆、結論

對資訊的依賴愈深，資訊安全就愈重要，而世界上沒有一個系統是不會被破解的；維護資訊安全，除了在系統設計時就要加以規劃外，我們使用者也要有基本的認知，才能共創雙贏。

（作者任職於華創車電技術中心股份有限公司電動車研發部）

（本篇摘錄自法務部調查局清流月刊 98 年 9 月號）

商業間諜竊密之初探

民間企業主在面對全球化競爭與兩岸擴大交流下，勢必需要建立自身的保防制度，並加強與政府保防部門之聯繫合作。

◎ 趙明旭

一、商業間諜之崛起

冷戰結束後，經濟、科技、商業性競爭壓力愈趨激烈，已然取代冷戰期間「高政治」的軍事安全議題，成為當前國家安全的重要範疇。各國情報機構基於維持組織生存或增進國家經濟力考量，而進行工業、科技、商業等之諜報行動亦時有所聞，使得國家反情報工作的需求更為迫切。臺灣工商業由於長期殫精竭慮、努力經營，在經濟上早見其成效；惟值此經貿繁榮之際，產業競爭轉趨激烈，如何保護企業所特有之營業秘密，實為商場致勝之鑰。

商業間諜之活動較之國防情報之蒐集，實有過之而無不及。其方式不勝枚舉，例如：企業界派員至他企業長期臥底，刺探重要情資；透過留學生在當地打探，甚至利用幫教授做實驗或相關研究之機會，竊取重要資料；收買在他企業任職之各階層相關人員或政府有關官員；監聽電話、侵入電腦網路，瞬間截取國際通訊；直接購併國外高科技公司，以獲取該國科技機密；藉政府力量，利用國家情報機構，以協助產業界蒐集產業情資。其中在網路竊密部分，根據國際知名通訊及 IT（Information Technology，資訊科技）方案供應商 Verizon Business 公布的「2009 資料外洩調查報告」(2009 Data Branch Investigations Report)顯示，12008 年的電子檔案外洩事故比過去 4 年的總數更多，主要針對金融服務業，並明顯涉及有組織罪行；報告顯示，2008 年期間一些嚴重網路罪行之受害者多為大企業，其中 93%的外洩紀錄為金融業，當中更有 90%涉及被執法機構認定曾參與有組織犯罪活動的不法分子。

面對全球化經濟戰略佈局，並從近年來兩岸之間經濟交流的緊密程度來看，無論政策如何變動或攔阻，皆難以迴避在商業機密上所形成的關漏；吾人雖不必以鎖國心態聚力防堵，但是必要的防制手段卻是絕對必需的。如馬英九總統即就大陸採購 20 億美元的臺灣面板乙案表示：「採購是好事，但若涉及投資，政府會特別注意，不會讓高科技技術外流」，顯見總統亦重視關鍵技術保密對我保持經濟競爭力之重要性。

二、各國對商業竊密之立法

在激烈的商業競爭中，國際間對營業秘密之保障與產業倫理及競爭秩序之維護，多已制定相關專法予以規範，如美國統一營業秘密法、加拿大統一營業秘密法、德國不正競爭防止法、日本不正競爭防止法、韓國不正競爭防止法等。而美國在 1996 年 10 月柯林頓總統簽署通過經濟間諜法案 (The Economic Espionage Act, EEA)後，竊取商業機密者將以聯邦罪犯處置，犯案者不只被科以罰金更要入監服刑，最高可判罰金 500 萬美元及 10 年有期徒刑。當時聯邦調查局長路易

士(Louis J. Freeh)在兩次的國會聽證會上強調該法之必要性，首先指出後冷戰時期，美國國內經濟發展的重要性和國家安全的重要性是一樣的；接續聲稱許多國家為了自己國內的經濟利益，不擇手段地積極介入偷取美國的商業機密；最後表示美國既有的現行法案無法有效起訴經濟間諜。EEA（經濟間諜法案）為美國國會為保障美國企業之經濟利益所立的非常之法。美國企業可以依據 EEA 要求美國政府動用司法權(FBI 和聯邦檢察官)以保障其私人之經濟利益，加強了美國工商業機密之保護，也確實將「保密防諜」提升到另一個境界。

我國在經濟、產業反間諜法制方面仍尚乏專門法規，除民國 85 年通過的「營業秘密法」，明確規範了營業秘密之構成要件、保密義務、訴訟程序中營業秘密之保護、營業秘密之侵害類型及營業祕密之救濟外，相關法律則散見於：民法的「侵權行為」、「契約規定」及「不當得利」(184-187 條、71-72 條、179 條)；刑法的「洩漏業務上知悉之他人秘密」、「洩漏業務上知悉工商秘密罪」、「洩漏公務上知悉之工商秘密」、「竊盜罪」、「侵占罪」、「詐欺得利罪」、「背信罪」及「侵入住宅罪」(316-318 條、320-321 條、323 條、335-336 條、339 條、342、306 條) ；公平交易法的「營業秘密之盜取」(19 條、30-41 條) ；著作權法及專利法、商標法等。

目前我國在面臨商業間諜威脅部分，多以「腦力密集度」高的電子業為主，電子業龍頭級大廠都曾面臨類似事件。如民國 92 年臺○電前專案經理劉某在前往大陸晶圓代工廠商中○任職前，以電子郵件大量洩密，而遭臺○電控告；友○公司及威○公司亦於同年爆發商業間諜案，原威○市場部經理張某到友○任職，並竊取友○研發的「晶片模擬測試程式」，爾後張員又回威○任職，友○公司懷疑他將程式公布在威○網站。而國內兩大房屋仲介業龍頭「信○」與「永○」房屋，亦於 97 年肇生商業間諜案件，「臥底人員」大量偷竊對手公司的推案企畫、客戶名單等重要營運資料。

三、我們應有之強化作為

馬政府上任後，為了和平發展兩岸關係，也讓臺灣休養生息並邁向全球化，馬總統的戰略思維已將我國三大目標「政治尊嚴」、「經濟發展」及「軍事安全」作一排序調整。而當前的國家總體戰略是以經濟發展及經濟安全為優先，為確保國家及民間企業關鍵、機密產業技術安全無虞，保防工作有關安全維護、機密保護之思維，相形之下則顯得相當重要。

在現今世界各國情報機關已將「經濟情報」列為首要目標之情形下，如何保護、管制我國商業機密及關鍵商業技術安全，仍待我保防體系統合協助並規劃執行，期能主動輔導、協助轄區民間私營企業建立機密安全維護等相關保防制度，進而主動協助且提供人民預警情資(如駭客攻擊等)、專業技術或法律諮詢，以保護其專門知識，建立政府、民間良性互動，強化「社會保防」功效。

面對世界經濟間諜橫行及高科技電子產業快速發展，我國似乎欠缺一套反制商業間諜的專門法律，或可在現有的「營業秘密法」之基礎上，增訂或另訂「經濟間諜法案」，俾利嚴格掌控可能對財產和民眾信心產生嚴重影響的「關鍵資產(包括有形和無形資產)」及受外國政府控制之企業的任何交易，透過嚴厲的罰則，嚇阻外國政府或國內商業間諜活動，維護整體國家利益。

四、小結

美國情報體系在 2005 年版的反情報戰略中提及要「協助護衛國家安全機密、關鍵資產與科技，免於竊密、外力秘密轉移或利用」；在 2007 年版則提到「保護美國經濟優勢、商業機密」。在全球化的經濟市場下，商業競爭、資訊普及、人才流通等對商業機密竊取更為便利。除了情報人員外，負有特殊任務的訪客、商人、記者、科學家、技術員、留學生等，在安全管控機制鬆散下，都有可能輕易竊取或得知關鍵技術的祕密。敏感的商業機密和業主的訊息外流，將會腐蝕我們的相對經濟優勢，甚至危害國家安全。非法獲得機密技術的外國組織或公司，也會在免於負擔重大研發與革新技術的成本下，不公平地與其他公司競爭，並有較大的機會獲取利益。民間企業主在面對全球化之競爭與兩岸擴大交流下，勢必需要建立起自身的保防制度，並加強與政府保防部門之聯繫、合作，以強化本身「機密保護」的能力，共同維護個人及國家的利益。

（本篇摘錄自法務部調查局清流月刊 98 年 9 月號）

資安稽核常見問題

學習稽核應對概念與技巧，對稽核人員與受稽單位都一樣重要。

◎黃小玲

前　言

資安稽核時常發生問題，有時是稽核人員的疏失，有時是受稽單位的準備不足，更或有時是「莫非定律」光臨，所有問題一起出現在同一個時間點。

前陣子速食業者油品稽核事件，鬧得沸沸揚揚，從一開始的速食業者用油到底多久換一次、油品更換紀錄造假事件、發現速食業者滅火器逾時 8 年，到最後議論麵包適當保存期限是多久？究竟，稽核可否界定範圍？符合國家規定等不等同符合消保官的稽核準則，以及稽核人員的標準與受稽單位的觀點如何一致？

以上這些問題，就從一個小小的稽核開始。資安稽核也是稽核的一種，從這個事件來看幾件資安稽核可以借鏡的地方。

壹、天上掉下來的禮物要不要接？

在上述油品稽核事件中，滅火器應該不在消保官的稽核計畫中，但是當發現這樣的缺失時，要不要寫入稽核缺失表內？要不要繼續追蹤改善與否？新聞沒有進一步的報導。若這樣的缺失發生在資安稽核情境中，稽核人員若見獵心喜，決定改變方向往消防檢查方向前進，如此一來可能延誤或只得變更其他稽核行程以繼續追查。稽核的評估重點是在已事先定義好的稽核範圍內，稽核重點若在油品逾時不換，則應確保過程不致失焦；滅火器過期，則列入稽核註記，下次稽核時再加強檢視或是交付不同單位列入考核重點。

稽核技巧：稽核首重規劃，縱有天上掉下來的禮物，稽核人員還是應該著重在原有規劃之稽核目標與行程上。

貳、稽核員永遠是對的？

稽核場景一：稽核人員對著機房管理人員露出想一探究竟的表情說：這個機房每日檢查表（包括機房溫濕度、系統及環境異常等）內的筆跡與墨色都一樣，且數月來都是填寫「OK」，而且連明天的紀錄都已填寫，我懷疑資料是不是造假？機房管理人員不置可否：每天都是我填寫，筆跡與墨色當然都一樣，至於明天的紀錄是不小心填太快，只是一時疏忽。

稽核技巧：稽核員可以假設自己像名偵探柯南，但偵探可以推理，稽核則講求客觀性證據。因此，稽核員不應自行判斷這個紀錄表是造假的，擅自認為這樣的狀況一定是不實紀錄。稽核若沒有證據顯示異常或不符合，則不能憑藉著稽核人員的天縱英明而完成稽核報告。

參、世界上最遠的距離

稽核場景二：稽核員在稽核會議上報告今日的稽核時程後，發現會議室內的受稽單位代表紛紛露出詭異的笑容。稽核員順利完成早上 9:30 至 10:30 的稽核行程，準備前往下一個辦公場所進行接下來一小時的稽核。陪同人員這時才悄悄地跟稽核人員說：不過我們另一個稽核場所來回要一個半小時哦！稽核人員這時才頓悟，稽核最遠的距離不在你跟我之間，而在受稽核單位明知來回要一個半小時，卻事先不告訴你。

稽核技巧：稽核人員與受稽單位應仔細確認稽核計畫內的所有規劃，包括範圍、業務複雜度與時間的安排是否妥適等。

肆、全部都是機密，通通不許看

稽核場景三：稽核員看著防火牆管理者說：我想看看你所負責的防火牆服務埠開?的申請表格。管理者頻頻搖著頭說：這類的申請表格，我們內部列為機密，不好意思，如果沒有正式經過申請審核，我無法提供。稽核員莫可奈何地說：好吧，那可不可以讓我看一下你針對防火牆所做的風險評估報告。防火牆管理者說：抱歉，那也是機密文件！

稽核技巧：通常在資安稽核開始時，會要求稽核員簽署所謂的保密切結書。基於保密切結的情況下，如果內容真是涉及機密，受稽單位當然可以拒?。但稽核員若只想檢視處理機密資訊的過程，倘仍一味地拒?，則稽核也無從判斷資安防護程序的嚴謹度。其實利用保密切結的簽定或部分內容遮蔽的技巧，即可顧及機敏資訊不外洩，又可收稽核之效。

伍、人員跟你玩躲貓貓時，怎麼辦？

稽核場景四：稽核順利開始，每位稽核員都有 2 至 3 位受稽人員待命，準備接受實地檢閱或文件紀錄的對應。很快地，稽核員發現他前面一個人都沒有，剛剛一片熱絡的情況，瞬間不復見。稽核員想想：他剛請第一位受稽人員去拿一分管理文件，因為沒回來，所以只好轉換稽核項目，請第二位負責人去拿系統帳號申請紀錄；第三位受稽人員，好像是說他所負責的資安教育訓練需要會辦人事室，所以需要去人事室拿紀錄過來。問題是：怎麼三個人都一去不回呢？距離第一個人離開的時間至少 20 分鐘了吧！終於第一個人回來了，上氣不接下氣地說：對不起，請問你剛剛的稽核問題是什麼？我們系統管理者不確定你要的是那份管理文件？

稽核技巧：首先，稽核人員必須了解維持稽核計畫可以確保稽核品質，但稽核時的情境題，千奇百怪，如果只是墨守成規或不懂得變通，則稽核效果有限。第二個問題是，如果受稽人員真的不懂得稽核員在問什麼問題時，務必要問清楚，才不會造成雙方認知的差距。

陸、Hands on or Hands off（接手或不插手）

稽核場景五：稽核員看著 AD Server(目錄伺服器)的系統管理員說：我想看一下單位內的帳號與密碼安全性設定原則。管理者慌亂地說：自從上位管理者離職後，我都沒改變設定。繼之，他不熟練地操作著，努力想秀出稽核員所要看的系統設定畫面。努力一陣後，他看著稽核員說：可不可以由你操作比較快？稽核員想想有道理，接手將滑鼠點了幾下，果然很快找到設定的畫面。就在此時，突然有人走進機房叫喊著：同仁紛紛反應電子郵件出現錯誤訊息，無法正常收發 e-mail，也有人反應無法登入網域。管理者與稽核員面面相覷地互喊：不是我！

稽核技巧：稽核員不論多麼熟悉所稽核之系統，都應避免直接接觸線上系統，以免發生干擾正常維運的狀況。

柒、稽核證據像魔術一樣消失時

稽核場景六：一天的稽核終於結束，到了結束會議。稽核人員一一報告今日的稽核缺失時，突然技術部門主管開口：不好意思，因為我昨天才發 mail 請我部門所有人員注意合法軟體的問題，您真的在我部門發現有同仁的軟體版權有逾期的問題？可不可以請問是我部門那個同仁？稽核員被如此一問，有點愣住：我記得應該是坐在三樓入口右手邊那位先生。技術主管疑問：可否再明確一點呢？或是等一下我們一起前往那位同仁位置上看一下？

稽核技巧：對稽核人員最糟糕的可能情境之一是：稽核證據在轉身時就消失。上述事件稽核人員當然可以再次前往現場進行稽核確認，不過很可能的狀況會是：非授權軟體早已被移除乾淨。如何確保稽核證據不會像泡沫般消失，除了稽核陪同人員的見證外，稽核人員應紀錄所有稽核發現的人、事、時、地、物，並將所有違反事項詳實記載於工作底稿內，如此皆有助於稽核證據的再次真實呈現。

捌、結論

學習稽核應對概念與技巧，對稽核人員與受稽單位都一樣重要。通俗地說，稽核是稽核人員與受稽單位某種競智的表現。但是最佳稽核情境應該是雙方基於互信互利的基礎，對事件稽核的準備與過程中，皆依計畫進行，其所產出的獨立性稽核報告能得到受稽核單位的認可，彼此遵守稽核規範與準則，則可大幅避免出現資安稽核的謬失。

（作者為國家資通安全會報技術服務中心組長）

（本篇摘錄自法務部調查局清流月刊 98 年 8 月號）