行政院國家科學委員會補助專題研究計畫■ 成 果 報 告
□期中進度報告

非公務機關（人員）安全認證制度

計畫類別：□ 個別型計畫　　□ 整合型計畫　□ 其他補助計畫
計畫編號：NSC 92－2745－P－009－001－
執行期間：92 年 8 月 1 日至 92 年 11 月 30 日

計畫主持人：交通大學電信工程系教授　闕河鳴
共同主持人：交通大學電機與控制工程學系教授　楊谷洋
　　國防大學軍事學院教授　廖宏祥
計畫參與人員：

成果報告類型(依經費核定清單規定繳交)：□精簡報告　■完整報告

本成果報告包括以下應繳交之附件：
■赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、
　　列管計畫及下列情形者外，得立即公開查詢
　　□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：交通大學電信工程系

中　華　民　國　九　十　三　年　一　月　二十五　日

－ 目　　次 －

非公務機關（人員）安全認證制度

第一章　導論

第一節　研究背景

在過去，台灣主要倚賴政府相關部門—特別是軍方—進行跟國家安全有關的政策與科技研究。民間部門－包括各種法人、智庫、甚或企業等等－很少有機會能夠參與這其中的過程。這種情況所造成的限制除了抵銷了這些民間部門所可能提供的創造力與改革動力，也讓民間部門無法在安全研究上做出有力的貢獻。

隨著時代的變遷，安全研究領域的參與門檻已經逐漸降低，許多非政府機關部門的智庫、法人機構或企業以及這些單位內的個人開始參與國防安全相關計畫，甚至是由政府部門主動邀請參與安全研究的相關計畫，並因此得以與聞國家安全機密。不過隨著參與的擴大，其他問題也逐漸浮上檯面，包括目前國內法令規章並不完備，各政府相關部門－特別是與國防安全相關之部門－對於所謂的「安全認證」（security clearance）的認識不若美國等先進國家，在執行過程上也往往不夠嚴謹。其結果是民間非公務機關或人員雖得以參與安全相關研究，但卻容易滋生弊端，更很可能在無意中導致國家機密外洩。

從政府的角度來看，爲了保障國家安全以及全體人民的整體利益，有些機密資料（不論是來自政府機構或來自非政府機構）必須存在，而且必須嚴格保密，一旦這些資料外流，人民利益與國家生存就可能遭受極大的威脅。因此，進行安全認證以保護機密資料不致因爲人爲因素而外洩實有其必要。換言之，從正面的角度來看，安全認證的施行乃是希望任何個人在維持、追求其利益的過程中不去危害到全國人民的利益，更不至於因此威脅到國家安全。

在了解了這樣的需求之後，我們有必要針對以下幾項問題進行分析：

壹、 何謂「安全認證」？它的定義爲何？過去的沿革爲何？現行我國政府機關對於安全認證的認知又是如何？實際的安全認證措施（包括立法、以及實際執行過程）如何？過程中間面臨哪些問題？

貳、 西方國家－特別是美、英等國－針對安全認證的立法以及執行又是如何？是否有任何可供作爲在建立安全認證制度上的參考？

參、 如何建立一套完整、特別是針對非公務機關或人員的安全認證程序？在立法上該如何配合？政府部門又該配合採取哪些措施？哪些認證措施及程序應該修正？可能侵犯人權或隱私之問題又該如何解決？以及最後

肆、 政府部門應該如何貫徹執行安全認證制度？

當然，本研究除了要了解上述的問題之外，更重要的意義在於藉由這項研究的進行，達成一定的目標。這些目標包括了：

壹、 提供政府在針對非公務機關（人員）進行安全認證過程中具體的執行建議，並促進行政與立法部門合作，催生安全認證機制的建立；

貳、 藉由安全認證機制的執行，免除國家機密資料被不當的外國情報機構、人士所獲取，從而危害我國家安全。

參、 促進並提升非公務機關及人員對於我國家安全研究之參與，同時藉由這一過程，爲我國家安全之研究提供更多的創造力與改革動力；

肆、 促使安全認證議題獲得更多的了解與更高度的重視。

本計畫主持人所任職之交通大學與鄰近之新竹科學園區，一向爲我國高科技產業重鎮，在本計畫主持人主持下，再加上數位計畫共同主持人對高科技產業及國防相關事務的瞭解，以政策研究、訪談、舉辦研討會的方式，針對上述問題進行透徹之分析，可以預期將提出對「非公務機關人員安全認證」有相當程度貢獻的成果。此外更希望能透過促成長久制度的建立，以轉換我國民間的力量爲國家安全研究或國防工業發展所用。

第二節　相關名詞之定義

壹、　安全認證之定義與沿革

爲有利於本研究計畫推動與達成研究目標，首先有必要針對「安全認證」作一明確的定義，同時對安全認證的沿革做一適當的釐清。

所謂的「安全認證」，在本研究中泛指爲維護國家機密不致外洩，所因而衍生必須針對人員、設施、資料、以及資訊傳播所進行之各項查核措施，凡是通過安全認證措施者，得依照安全認證之等級高低而獲得不同之權限，並得以接觸不同層級之重要國家機密文件、設施或儲藏位置。安全認證可以分階段、分等級、分項目、定期或不定期進行。以人員安全認證爲例，在進行安全認證時，可以針對人員之基本住所、學歷、工作經驗、婚姻狀況、健康情形、是否有犯罪前科或酗酒、賭博等不良行爲記錄等進行初步查核，並且可以依照人員任職前、任職期間以及離職後分階段進行查核；既可以在該人員任職一段期間後重新查核，也可以依照主管之認定隨時不定期進行查核（或測謊）以確保人員之可靠性，若未能通過，應使其轉任其他職務，減少其與國家機密接觸之機會。不過不論查核的方式爲何，必須注意的是，安全認證的通過並不代表該人員可以永久享有接觸重要國家機密文件或設施之權限，安全認證只有在進行查核的當時具有正確性，一旦查核過後，其正確性將隨時間增長而遞減。

事實上，「安全認證」制度在台灣的歷史中存在已久，只不過在文書上或執行上從未正式使用過「安全認證」這一詞，而是採用所謂的「忠誠（貞）調查」。不過與現代意義的「安全認證」最大的區別是，在當時所謂的「忠誠（貞）調查」跟設施器材、資訊（特別是電腦、網路等）等幾乎毫不相干，主要都是針對人員所進行。這種狀況除了肇因對設施、資訊等查核的認識不足之外，跟當時的時代背景實有相當密切的關係。

在威權統治時代，「統治者」等同於「國家」，對國家忠誠即等於對統治者忠誠，忠誠的認定標準常隨著當權者而改變。因此在當時－特別是兩位強人統治的時代，不論是針對公務機關（人員）或者是非公務機關（人

員），實施忠誠（貞）調查的主要目的實有二，一是確認受查核者對於國家和所任職機關是否認同；另外一項更重要的則是確認受查核者是否效忠於領導者，並且對於領導者的命令能夠貫徹執行。單純從法理來看，這兩項目的如果是在民主法治臻於成熟的國家中並不發生問題，但是在威權體制之下，忠誠（貞）調查的執行往往是爲了當權者服務，而且幾乎完全採行秘密調查，調查之初既不告知當事人，調查完成的結果更不會讓當事人知悉。結果導致這些所謂「忠誠（貞）調查」常常變相演變成連帶判斷受查核者的政治立場是否與當權者相符合，如果不相符合，那麼調查的結果就成爲當權者打壓異己的工具，這也是爲什麼在進行本研究調查訪談過程中，許多受訪者都不約而同會把「安全認證」和「白色恐怖」聯想在一起的主要原因。

即便時空轉換，當時序進入二〇〇二年，台灣已經全面邁向民主法治化的同時，行政部門雖然體認到「安全認證」對於維護國家安全的重要性，並針對公務人員草擬與「安全認證」相關法案時，卻仍不免將草案擬定之初，將其定名爲「公務人員品德及忠誠特殊查核辦法草案」[1]。這種情況，除顯現行政部門對於西方先進民主國家行之有年的「安全認證」未能有更深入的了解之外，事實上在某一程度上也顯示出政府機關在制定安全認證制度的同時，依然受時代背景之深刻影響。

貳、 非公務機關（人員）之定義

在進行本研究的同時還將面臨到另外一個定義上的問題，那就是所謂「非公務機關（人員）」的定義。」

以當前台灣的現有公務體系來判斷，當我們談到非公務機關（人員）的時候，最直覺的判斷是以「是否爲政府所設立（以機關而言）或者是否通過國家考試、並經過正式聘任，具有公務人員身份者（以人員而言）」作爲區分的標準。相較於公務機關（人員），如果非與政府有直接隸屬關

[1] 事實上也正因爲台灣從上到下各階層對於「忠誠（貞）調查」的刻板印象，導致在二〇〇二年行政部門提出此項草案之時，立即遭到在野黨強力的杯葛與反對，並且認定此項法案係爲當權者服務，可能變相成爲民進黨政府打壓具在野黨身份的公職人員的工具，也從而使得當初這項立法的本意完全被扭曲。

係、非屬政府正式部門、同時所聘用之人員也非具公務身份者便可稱爲「非公務機關（人員）」。

但是如果就實際與重要國家機密有所相關的人員或機關來評斷，上述標準顯然就有所失當。舉例來說，成立於一九七三年的財團法人工業技術研究院。在定位上，它應該屬於民間法人單位，並非公務機關；但是在實質上，它卻是由政府正式立法設立，並且在該機構內所從事的許多相關研究計畫都與政府之國防軍事技術、經濟技術等事務息息相關。換句話說，工業技術研究院是一個在法律定位上屬於民間團體，但實質上卻與重要國家機密、國家安全極爲密切相關的單位，其接觸國家機密等級的程度幾乎與公務機關相同甚至更高，那麼這種單位我們究竟該定位它屬於公務機關抑或非公務機關？如果將其定位爲公務機關，因而排除其在安全認證計畫的研究及規範範圍之外，那麼本項研究計畫將因此喪失相當重要的意義和成分。同理可推，其他許多機關和成員（例如大學教授、政府部門內的政務官、國會議員、國會助理等等）等，在區分上也都面臨同樣的問題。

本研究計畫的主要目的既在制定針對「非公務機關（人員）」之相關安全認證措施與辦法，因此所謂的「非公務機關（人員）」之定義自然無法以上述的區分作爲標準。那麼該如何區分出所謂的「非公務機關（人員）」？其實西方國家的經驗正足以提供參考。

以西方先進國家而言，這些國家在進行安全認證的過程中，並不是依據所謂的「公務機關（人員）」或「非公務機關（人員）」來做區分，相反地，他們是以該機關、人員之工作職務範圍是否有接觸國家機密之可能性作爲是否必須進行安全認證的基準。造成這種情況的主要原因除了西方國家的公務人員並非經過考試任用之外，更重要的原因在於西方國家在進行安全認證的過程中，就已經清楚的了解到，安全認證的最終目的在於維護國家機密、確保國家安全，而基本上不管是公務體系或者非公務體系的機關或人員都有可能接觸到國家機密，既然如此，在安全認證的措施上就不應該有所區別，而應該一體適用，這樣才有可能在合於法裡的基礎上擴大管制的範圍而不至於發生濫用查核權力的情況，同時又可確保國家安全無

遭受損害之虞。

有鑑於此，本研究在定義所謂「非公務機關（人員）」時，採用了西方國家的標準，除了將正式的官方機構與公務員排除在本研究的預設規範範圍之外，所有那些雖不具官方位階、或者雖不具正式公務人員資格，但在進行工作或執行任務的過程中確有可能因此接觸國家機密的機關、企業、法人單位或者這些單位內的成員、甚至包括個人（例如前述所提及之政務官、國會議員、國會助理等等）在內，將全部包括在本研究所定義的「非公務機關（人員）」的範圍之內。

參、 國家機密之定義

本研究的主要目的既在針對可能與聞國家機密之非公務機關（人員）擬訂具體的安全認證規範，那麼自然必須對所謂的「國家機密」下定義。

爲便於研究過程的進行，以及爲便於制定後續規範措施之基準，本研究所謂的「國家機密」係依據二〇〇三年二月我國所正式頒佈的「國家機密保護法」中對於「國家機密」之定義。根據該法，所謂的「國家機密」乃是指「爲確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依本法核定機密等級者」。[2]至於機密的等級則依照洩漏之後可能對國家安全所造成的損害程度分別分爲「絕對機密」、「極機密」以及「機密」等級。

惟爲彌補與上述定義之可能缺口，行政部門亦於同（二〇〇三）年七月特別修正增訂「軍事機密與國防秘密種類範圍等級劃分準則」，該準則對於機密之定義與等級區分也成爲本研究對於機密定義之輔助基準。[3]根據該項準則，所謂「軍事機密」，乃指「與軍事作戰具直接關連，爲確保軍事安全或利益而有保密之必要，並經依法令核定機密等級之文書、圖畫、消息、電磁記錄或物品」。至於「國防秘密」則指「軍事機密以外，爲確

[2] 國家機密保護法，第二條。

[3] 目前這項準則雖已公布，但在該準則在二〇〇二年送立法院查照時，卻被認爲其中所規定的機密範圍過於廣泛，有抵觸憲法言論自由的情況，因此遭到立法院決議退回，並要求國防部重新修正。到本（二〇〇三）年十月底，已經立法院初審通過。***聯合報***，「軍機劃分準則 立院初審通過」，民國 92 年 10 月 28 日，A11。

保國家安全或利益，而有保密之必要，由國防部主管並經依法令核定機密等級之文書、圖畫、消息、電磁記錄或物品」。

第三節　研究方法

本研究的目的主要在促進並提升非公務機關、人員參與進行與安全相關之研究，爲了達到這項目的，本研究認爲有必要建立一套完整的安全認證制度與程序，以確保在進行研究的過程中，不致因爲人員、設施或資訊查核的漏洞導致機密的外洩。爲了達成這項主要目的，本研究將針對下列主題進行研究：

壹、 台灣現行－特別是針對非公務機關、人員－的安全認證程序，－其中包含現行法令、措施、手續等等；
貳、 西方先進國家－例如美、英等國－在安全認證上的立法、執行及其比較研究；
參、 現行我國安全認證過程所面臨到的困難與問題；
肆、 安全資料文件的分類；
壹、 人員的認證；
伍、 各項設施的認證；
陸、 通訊與資訊安全；
柒、 安全認證的問題與具體的執行建議；

在研究方法的運用上，本研究計畫的進行將以文獻探討爲主，進行訪談、舉辦研討會蒐集相關資料、實際參訪調查及海外實地調查爲輔。在文獻研究方面，西方先進國家如美國、英國等對於安全認證制度的建立與執行都已經累積有相當多的文獻，舉其例如：美國 12829 號有關人員安全管制機制法令。我國在這方面的法規制度雖然無法與西方國家相較，但是對政府所資助的研究計畫，特別是在高科技方面，已經擬定有「政府資助敏感科技計畫安全管制作業手冊」，藉以保護高科技研究發展計畫所獲得的智慧財產或成果（含知識、技術等）不至於流入國外地區，影響我國家安全或導致喪失競爭優勢，這些文獻將是進行本研究過程所不可或缺的重要

參考資料。

另外，爲了彌補文獻研究所可能產生「過份強調理論」的研究疑慮，本研究也特別設計實務上的安排，包括與政府部門安全單位、一般研究單位、科技研究單位內實際接受安全認證、或直接負責安全認證執行之相關人士進行訪談，藉以進一步了解當前政府部門或一般研究單位、智庫等在實際執行安全認證上的程序時所根據的法源、實施的措施，以及其中所可能面臨到的問題，並且於期中舉辦一次研討會，邀請其他相關人士擴大參與討論。另外有鑒於美國、英國對於安全認證制度研究上累積有相當豐富的經驗與實務，在研究過程中也將安排研究人員出訪國外，進行實地的訪問與調查。在兩項主要研究方法交互配合與運用的情況下，預期將能使本研究的過程更加完整，同時將使本研究所提出的具體政策建議以及解決方案更爲可行。

第二章　我國現行安全認證制度之探討

第一節　我國現行安全認證之法源依據

要瞭解非公務機關或人員是否能藉由安全認證制度參與一個國家的安全相關研究，首先我們必須去瞭解該國所推行的安全認證制度是否存在、或者若已存在，那麼這套制度的法源依據爲何。如果法令與制度俱在，那麼法令的制定是否完整？安全認證制度的推行是否同時兼顧到個人隱私權以及個人根據法令所應受保障的其他各種權利？安全認證制度在執行的過程當中又面臨到哪些問題與限制。藉由這些分析，我們才能夠對安全認證制度做徹底的檢討，也方才能夠就其中的問題提出具體的政策建議與改進方案。

壹、　台灣現行與安全認證相關之法令

就台灣而言，當前政府機關對於公務機關以及人員的安全認證大致上已經建立一套制度，雖然說不上完整，但畢竟已經行之有年。

根據本研究的訪談結果、以及資料蒐集發現，台灣目前並沒有一套完整的、範圍涵蓋文件資料、人員、設施、資訊安全與科技等項目的安全認證法令規定，安全認證甚至不曾出現在任何一套法律制度當中，而僅是以類似的名詞、或類似國外安全認證制度的規定安排在有限的法令當中，有些與安全認證息息相關的重大法令條文甚至還只是在草案階段，尚未以行政命令形式通過或正式立法通過，這些立法過程上的遲緩，對於安全認證制度上的影響亦不可謂不大。

但是如果就安全認證牽涉到安全認證的起源、過程以及認證的單位等等因素，如果總的來說，目前台灣所施行與安全認證相關的法令大致有以下各項：

一、　法律部份：

(一)、國家安全法（1987.07.01）

國家安全法於一九八七年制定並通過，其制定背景始於當年開始，政府正式開放國人前往大陸，但有鑑於兩岸關係的敵對狀態尚未解除，為維護國家安全及維持社會穩定，特制定本法，分別就公務機密資料之蒐集與傳遞限制、入出境、集會結社、管制區等項目做出規範，同時亦擬定相關罰則。

(二)、國家安全局組織法（1994.01.01）

本法係根據憲法第二條及國家安全會議組織法第八條制定。其目的主要在針對專責處理國家安全情報及特勤工作之安全部門－國家安全局－的設立及執掌範圍制定規範。全部條文共計廿三條。

(三)、法務部調查局組織條例（1980.08.01 修正）

除國家安全局之外，法務部調查局因為也參與並負責危害國家安全或違反國家利益之調查工作，甚至已經成為當前主要負責執行安全認證機關。全文共廿七條，就調查局所負責之執掌與內部組織人事分別加以規範。

(四)、國家機密保護法（2003.02.06）

過去台灣在機密資料之維護上一直缺乏明確的法令規範。隨著時代進步、資訊流通速度一日千里，為有效因應環境變遷，機密保護法乃應運而生。本法共四十一條，分別針對機密的核定、區分等級、保密期限、應該如何維護，又應該在什麼狀況下解除機密情況等加以規範，本法亦同時指出洩漏機密時之罰則。

(五)、公務人員任用法（1986.04.21）

本法主要規定公務人員之任用、升遷、職等、以及查核。全文共四十條。其中第四條規定：「各機關任用公務人員，應注意其品德及對國家之忠誠，其學識、才能、經驗集體格，

應與擬任職務之種類職責相當。如係主管職務，並應注意其領導能力。前項人員之品德及忠誠，各機關應於任用前辦理查核。必要時，得洽請有關機關協助辦理。其涉及國家安全或重大利益者，得辦理特殊查核；有關特殊查核之權責機關、適用對象、規範內涵、辦理方式及救濟程序，由行政院會同考試院另定辦法行之。各機關辦理前項各種查核時，應將查核結果通知當事人，於當事人有不利情形時，應許其陳述意見及申辯。」此項法律乃針對公務體系之人員進行「安全認證」之最重要、同時也是最明確提及「安全認證」的重要法律，同時也是日後制定「涉及國家安全或重大利益公務人員特殊查核辦法」之主要法源依據。

二、　行政命令部份：

(一)、從事及參與國防安全事務人員安全調查辦法（國防部，2001.05.16）

本辦法屬於行政命令，主要係依國防法第三十二條第四項制定。其目的在於針對那些參與國防相關事務的國防部所屬機構或人員、部隊之人員，以及其他因業務關係從事及參與國防安全相關事務人員等進行安全調查，以確保國防事務相關機密的維護。

(二)、機密檔案管理辦法（2001.10.24）

本辦法乃依據檔案法第十六條規定訂定，是爲因應尚未通過機密保護法之環境，並針對機密檔案之管理、存放、借閱、複製等情形加以規範。本辦法全文共廿五條。

(三)、軍事機密與國防秘密種類範圍等級劃分準則（國防部，2003.07.14 修正）

本準則係依路海空軍刑法第七十八條規定訂定，全文共廿一條。主要的目的在彌補國家機密保護法對於國家機密定義之可能缺口，並特別針對軍事與國防機密加以定義，並劃分其

種類與等級，以便對直接與國家安全相關之軍事、國防機密做更詳盡之規範與保護。

(四)、檢察機關處理涉及國家機密案件保密作業辦法（法務部，2003.08.06）

本辦法係依據國家機密保護法第廿四條第二項規定訂定。主要在於檢察機關因職務上之需要，可能經常會接觸到國家機密，爲確保國家機密在檢察機關執行任務時有外洩之情況，因此訂定本辦法。內容中同時也規定檢察機關人員於離、退職之後亦不得擅自洩漏機密。

(五)、涉及國家安全或重大利益公務人員特殊查核辦法（2003.08.29）

本項辦法乃是依據公務人員任用法所訂定。過去針對公務人員參與國家安全之重大任務時應該如何進行安全認證、查核哪些項目、應該由哪些機關或單位專責執行查核等情事並沒有法令的明確規範，因此本辦法的通過爲上述問題提供了解決辦法。未來公務員所從事之職務若涉國家安全、外交機密、科技、情治、財經、大陸等六大類事務，都將列入查核範圍。不過由於係以行政命令的方式通過，在法律的位階上將無可避免有所缺陷。[4]

(六)、行政院所屬各機關資訊業務整體委外作業實施辦法（1998.04.08）

本辦法之擬定主要係行政院爲推動下轄之各機關資訊業務、加速電腦化及網路化以促進資源整合共用、達到節省成本之目標而擬定。辦法全文共分分廿九條，重點項目在於其中對於整體委外之作業程序以及資訊安全及機密維護兩大

[4] 有學者就認爲公務人員任用法第四條所規定訂定特殊查核辦法雖係有法律授權的合法行爲，但是該辦法所訂定的內涵卻逾越立法機關當時的授權範圍，並認定該辦法內容將嚴重侵害公務人員之基本人權。參見國家政策研究基金會，忠誠查核與基本人權座談會實錄（台北：國家政策研究基金會，民國九十一年十一月十八日）。

部分的規範。

(七)、行政院及所屬各機關資訊安全管理要點（1999.09.15）

本要點之頒佈主要目的係行政院爲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、設備及網路安全以保障民眾權益。

(八)、政府資助敏感科技計畫安全管制作業手冊

由於我國已加入世界貿易組織（World Trade Organization，WTO），高科技研發成果及貨品之輸出入條件有可能放寬，而敏感之高科技研發成果更可能在各種交流場合不自覺流入國外（含中國大陸），另外在網路上傳輸政府敏感資料也應受到保護。爲此，行政院國家科學委員會邀集中央研究院、行政院科技相關部會及機關成立科技小組，著手建立國家科技安全管制機制，一方面防止外國（含中國大陸）非法取得台灣地區之高科技研發成果，強化其經濟、軍事方面競爭力;另一方面利用科技方法保障我國政府敏感資料於網路上傳輸之安全。本作業手冊可以說是「安全認證」措施的科技版，手冊當中對於如何制定敏感資料的等級、公務機關與非公務機關對於安全認證所應負之責任，以及如何執行相關之安全認證措施有詳盡的規定，可以說是安全認證在科技領域當中首次進行之法令與執行措施之完整結合與運用。

三、　尚處於擬定階段的草案

(一)、國家情報工作法草案

本法目前尚處於草案階段，未來通過後，將使情報工作及情報工作安全受到法律規範，同時也可確保國家安全與利益。本法共計十九條，分別針對情報之相關定義、執行、來源、保障、以及相關罰則制定規範。

(二)、科技保護法草案

本法亦處於草案階段。其制定的目的在保護科技研發成果、促進科技發展及提升科技競爭力，同時確保科技資訊及研發成果不致因不法行爲而外流導致損害。

(三)、臺灣地區特定高科技人員進入大陸地區任職許可辦法草案

本辦法係依據臺灣地區與大陸地區人民關係條例第三十三條第二項規定訂定。其目的在規範擔任特定高科技公司之人員進入大陸地區後可能有洩漏高科技機密資料或其他妨害國家安全利益之行爲，全文共十二條。

第二節　我國現行之安全認證制度

根據實際調查訪談、並參考法務部調查局的現有資料研析，同時配合本研究的分類，以下分別就政府部門對安全認證的認知、安全認證的執行、以及人員、設施、資料以及資訊系統的安全認證等項目來依次探討當前台灣安全認證制度。

一、　對安全認證的認知

根據實際訪談結果顯示，目前國內政府部門對於「安全認證」這一詞彙並不了解，有些探討相關法令的刊物甚至將其直譯爲「安全清除」。實際受訪人員在首次聽到「安全認證」一詞時，也往往將其與資訊或某些證照資格聯想在一起，但是一旦訪談人員將「安全認證」詞彙轉變成「忠誠（或忠貞）調查」時，受訪者即可立即表示完全理解。這一問題也顯現出國內在參照國外推行制度時，因爲翻譯語意上的混淆，連帶對制度的引介和實際施行造成很大的困擾。

其次在受訪人員探討「安全認證」時，受訪者往往傾向將「安全認證」推定爲具有某種程度的「政治意涵」，有些甚至仍以「傳統的白色恐怖」來看待。不過頗值得注意的是，受訪者對於現行執行安全認證前並無法事先告知受認證人員、也不會在認證過程結束後告知其審核結果幾乎全數表示欣然接受，甚至對於不知道結果亦坦然以對，這與西方國家在推行安全認證制度時同時重視個人人權、隱私權不受侵犯的情況有相當的差異性。

二、　安全認證的執行機關

在「涉及國家安全或重大利益公務人員特殊查核辦法」尚未公告執行之前，事實上台灣並沒有一個法律規定直接負責執行安全認證的機關或部門。在此之前，負責進行安全認證－特別是針對公務人員部份－主要還是有賴各政府機關的政風單位，除非遇有重大可能（或已經）危害國家安全利益的案例出現，否則一般政府部門並不會請法務部調查局出面。

目前由於前項法令已經頒佈施行，法務部調查局已經名正言順成爲台

灣現在以及未來執行安全認證的主要機關。不過必須說明的是，由於這項法令乃屬行政命令，在法律位階上無法與立法院所通過之法律相提並論，未來所有政府機關是否將貫徹執行恐怕亦大有疑義。在訪談中部份受訪者就對法務部調查局的位階表示懷疑，同時也對政府機關是否能力行這項命令也抱持相當保守的態度。

最後，對於本研究主題而言，這項法令很明確的針對公務人員而來，至於非公務機關或人員在從事「涉及國家安全或重大利益」的事務時，是否一併受到這項法令規範。一般而言，還是必須有賴實際負責業務的部門來決定是否委請法務部調查局協助執行安全認證。

三、 保密資料的分類（機密等級區分與防護）

與國家安全有關資料並需訂定機密等級者，至少應包含以下項目：

（一） 軍事計畫、武器系統及其演練；

（二） 外國政府軍政、軍、經資訊；

（三） 情報活動、情報系統及其來源、方法、密碼等；

（四） 外交關係、外國政府在國內活動資訊及機密來源；

（五） 涉及國家安全相關之科技或經濟資訊；

（六） 維護國家重要科技之計畫；

（七） 涉及國家安全相關之計畫。

針對上述所提之資料，政府部門有必要制訂並區分其機密等級以便於做更嚴格的規範。這些機密等級的制訂至少應分爲包括三類：

（一） 「絕對機密」：任何沒有經過適當授權公佈而洩露，將導致國家安全致命性受損的資訊或文件類屬之。例如協助敵對國家、分化盟國外交關係導致對國家安全產生致命影響者、洩露國家核心防衛計畫或密碼及通訊情報系統、機密敏感性情報運作，或與國家安全攸關之重大科學或科技研發資料。

（二） 「極機密」：任何非經適當授權公佈而洩露，將導致國家安全嚴重受損的資訊或文件類屬之。例如分化盟國外交關係導致嚴

重影響國家安全者、洩露重要軍事計畫或情報運作，或與國家安全相關之科學或科技研發資料。

（三）「機密」：任何非經適當授權公佈而洩露，將導致國家安全受損之資訊或文件類屬之。例如國家本土及海外之陸海空兵力部署資訊、機密軍事設施之訓練維護及相關檢查技術資料，機密軍事武器研發、設計、測試、生產以及性能資料等。

所有上述機密資料皆必須給予適當且足夠的保護措施，使其能夠有效且合理防止遭受損失及破壞，或是被外人取得。這些機密資料保護包含以下三類：

（一）口頭討論之防護：所有接觸機密資料之人員皆須警覺，並禁止在公共場合或大眾運輸工具，及未加防護措施之通訊媒介中，提及並討論機密文件資訊及內容。

（二）周邊環境的防護：用於存放各類機密資料及文件資訊之措施，必須具備偵測及防止未經授權之機密資料存取動作。

（三）緊急措施：發展一套保護機密文件及資訊之緊急應變程序，除考慮其適切性外，必須能做爲各種緊急狀況發生時之反應參考。

就台灣而言，上述機密區分等級在通過「國家機密保護法」之前，政府部門的文件機密等級區分爲「絕對機密」、「極機密」、「機密」以及「密」等。在該法通過後，已經取消了「密」等分級。不過另一項問題是，在實際進行機密等級分類時，由於保守觀念使然，承辦人員在將文件做機密等級分類時，往往將實質上並不具備機密性質之文件、或者甚至是公開可以從媒體、報章雜誌、網路上取得之資料一律列爲「機密」以上等級文件，這種作法對於機密文件之保護不但沒有助益，反而可能造成日後在進行安全事務相關研究之困擾。整體而言，若不考慮上述情況，經由訪談調查結果，前述所提之國家安全資料絕大多數都保管在高層政府部門，[5]一般研究

[5] 根據訪談結果，所謂「高層政府部門」包括了總統府、國家安全會議、國家安全局、以及國防部、國防部軍事情報局、外交部、法務部調查局等單位。

人員非經特殊個人管道及簽署保密切結書並無法取得。不過，這種必須透過特殊管道才能取得機密資料的情況，事實上反而提高了洩密的可能性。[6]

不過就這些資料的保護措施而言，目前政府單位對於機密資料的備份與異地（不在同一個區域）儲存並沒有落實，因此一旦遇有緊急狀況－特別是火災或地震等－可能造成相當大的損失。

四、 人員的安全認證（personnel clearance）

在既有之國家安全資料機密等級分類上之下，政府可統一規定人員安全認證規範、核發審查作業，以及與任何必要接觸機密資料的人員必需遵行之管制規範，這一規範統稱爲「人員安全認證」（personnel clearance）。人員安全認證的資格審查爲進行廣泛且詳細之人員安全背景調查，必要時並得實施測謊試驗。人員安全認證的結果得以證明受審查者應確定應包括：

（一） 經由政府部門首長或其授權委派之官員決定其其資格；
（二） 具公民身份，且效忠國家；
（三） 具堅強之性格且值得信賴；
（四） 誠實、可靠、謹慎且深具判斷能力者。

一般而言，目前台灣所施行的安全認證措施比較明確者，當屬人員認證。不過僅限與安全事務、國家重大決策研究相關之部門會特別進行人員的安全認證。通常這些單位在進行人員的安全認證時，會執行以下幾項措施：

（一） 人員錄取（簽約）前的背景調查：
透過調閱人員過去的學校、軍方紀錄，以瞭解其過去之表現、

[6] 舉例來說，一般研究人員透過與政府安全部門內人員之人際關係交往，並建立一定程度之情誼後，可能獲得取閱國家機密文件之管道。但是這種並非建立於制度的管道，一旦因爲研究人員忠誠的轉移、或受其他因素影響，而將所獲取之機密文件再轉交其他人，此時所造成之洩密情況嚴重性可能更超過一般，其所造成之損害也難以用特定的法律加以規範。

有無犯罪紀錄，或詢問其所認識的人士，透過私人管道進行安全認證。

（二） 人員基本資料的調查，調查項目包括：

1. 刑事案件紀錄。
2. 行政懲戒處分或處罰紀錄。
3. 品德、考績資料。
4. 國籍、戶籍資料。
5. 年籍、經濟狀況及學歷、經歷資料。
6. 身體健康狀況資料。
7. 其他有關違反安全之資料。

（三） 管區警員對受認證人員住家之環境背景調查。

（四） 主管定期性的考核。

（五） 政風部門不定期的審核安全認證結果。

人員的安全認證一般而言是比較可以被政府部門所理解的安全認證項目之一，在台灣通稱爲「安全認證」或「忠貞查核」。不過同樣必須補充說明的是，上述這些項目的查核主要還是以公務人員爲主，非公務機關及其人員是否採行同一套措施進行認證並沒有明確的規定或模式。更有甚者，即使在執行這些安全認證措施時有一套標準的作業程序可遵循，但實際上會加以貫徹執行的單位、部門卻屈指可數，更不用提那些與國防軍事密切相關的科技研發單位－如工研院、資策會與民間大學－或企業。這種情況所在多有，不發生問題的時候並不會特別受人矚目，但是等到一旦發生嚴重的損害國家安全、利益情事時，往往會造成很嚴重的後果。

五、 設施的安全認證（facility security clearance）

到目前爲止，台灣現行安全認證制度中最弱的一環－不論是在法律規範或是在實際的執行的過程上－就是「設施的安全認證」。就定義而言，所謂的「設施安全認證」乃是一種決定「某法人的工作環境與設備，是否具備接觸機密性資訊、或執行機密性合約資格」之判定。而設施安全認證的基本條件，乃是以法人必須接觸機密性資訊才能執行工作爲基礎，而且該法人必須於本國法律規範下，於國內創立並實際存在。此外，法人也必

須具備良好之商譽及法律紀錄可供查詢，不能有受外資擁有控制或影響。至於而外資法人安全認證，任何具有外資股份控制權及外資影響力之法人，皆須另外執行安全評估以降低安全上之風險，達成外資法人的安全認證。惟不論是國內法人或外資法人，任何法人的行爲絕不能與國家利益有任何程度的牴觸。

法人的工作環境與設備應提供存放機密文件於經過安全檢驗合格之容器、保險庫或密閉空間，並需要額外之防護措施。這些環境與設備可能包括了：

（一） 限制性區域：工作期間如有必要於開放空間內處理機密資料，必須設置以限制區域以作爲接觸機密文件之特定限制區。
（二） 密閉區域：一律須加以控管，防止未經授權之進入及接近。
（三） 額外防護措施：如入侵偵測系統及警衛人員。
（四） 容器、櫥櫃、保險庫及密閉空間：之這些設備的鑰匙、掛鎖及號碼鎖之防護。
（五） 先進的接近控制系統及裝置：包括自動化的接近控制系統及電子、機械或電機裝置，這些裝置將可作爲取代控制進入限制性或密閉區域之警衛人員。

就台灣而言，誠如前述，翻遍各項與安全事務相關之法令規定，完全找不到可以作爲處理上述問題依據的相關法規，這對於引進法人單位或相關組織來進行與安全相關的研究而言是相當大的阻礙與致命傷。由於法人無法經由公正、明確的安全認證機關取得認證，政府部門和法人機構彼此之間缺乏互信，當然也更談不上引進法人進行與安全事務相關之研究。

另外與設施有關的如政府部門重要機密資料的儲放容器、建檔等設備之採買也面臨同樣的情況，參與競標的承包商在得標後進行之施工與所提供之設備並無法經過一個公正、廣爲接受的認證機關來處理其安全認證。在大多數情況下，僅以簽具「法定切結書」的方式以圖遏制可能的洩密行爲，但就法論法，切結書是否能夠發揮其應有之法律效力、又切結書所規

定之處罰罰則是否真能足以嚇阻承包商之違法行為仍有待考量。

六、　資訊的安全認證

「電腦」與「網路」為現代辦公環境中不可或缺之工具，因此就非公務機關而論，經過認證的法人或其他機關組織在進行與政府相關的安全研究計畫時，必須指派資訊系統安全經理，以監督網路機密安全，並確認資訊系統符合安全要求，此項措施稱之為「資訊系統安全認證」。

此外，網路安全整合趨勢已經無可避免，未來每個網路系統必須擬妥安全防護計畫，定期做資料備份與異地儲存。在此同時，面對不同、各具備之有管轄權的安全機構參與同一計畫時，應安排單一網路安全管理人員，以達到事權統一的效用、並對整體網路安全系統負責。網路安全管理人員本身也必須確認網路安全計畫之安全政策需求。

網路安全需求依實際需要而定，但必須具有以下基本條件：

（一）　對網路威脅、進行安全服務與機制的描述：
網路必須提供以下服務：使用控制、資料流程控制、資料分割、審核、通訊整合。

（二）　特殊網路安全需求：
網路各元件應有一致整體的安全規劃，網路內部連接之安全控制，資料傳輸的控制與防護，通訊協定與安全防護整合，必須有適當的防火牆（firewall）以控制人員使用及資料傳輸。

（三）　相容性：
連接新系統時必須有相容性，系統可支援區域性安全措施。

（四）　密碼傳輸或其他傳輸安全防護系統：
機密資料在網路中進行傳輸時，必須使用安全防護傳輸系統，或國家安全局認可之密碼編譯系統或其他保密設施，以保護資訊傳輸安全。

當資訊被歸類為機密資訊時，使用之軟體與硬體必須遵循機密等級之

要求，同時在操作上也必須具備基本的操作認證技術。舉例來說，這些操作認證技術包括有「使用者之身分證明」、「密碼」、「代幣」、「生物測定」、「指紋辨識及智慧型卡片」等等。

以台灣目前之情況而論，在訪談過程中，絕大多數受訪者都表示對於上述資訊之防護表示熟悉。以法務部而言，法務部就有一套非常完善的資訊安全防護體系，從實體的電腦機房管理、斷電處理程序到人員的管理及訓練都有非常詳盡的說明與規定。[7]行政院亦針對資訊安全之管理及委外分別擬定「行政院及所屬各機關資訊安全管理要點」以及「行政院所屬各機關資訊業務整體委外作業實施辦法」。不過與前述幾項安全認證相同的是，這些規範都僅只適用於規範公務機關體系，對於未來可能或已經承接政府安全研究之非公務機關、人員並沒有明確的規範。

[7] 參照法務部網站，http://www.moj.gov.tw/chinese/c_rule.aspx

第三節　小結：我國現行安全認證制度之特色與檢討

從前兩節所述可以了解，目前安全認證制度在台灣可以說尚處於相對原始的階段，從法源的制定到制度的實際推行都面臨相當不足的情況。不過法令、制度這些問題上尚可以透過不斷的學習國外經驗以逐步解決，但是對於安全認證的錯誤認知或者先入爲主的觀念則必須等待時間來加以矯正或化解。

表一是本研究針對台灣目前所推行安全認證制度的一項分析列表，可供作爲分析台灣安全認證制度的參考。

表一、我國現行安全認證制度之執行

安全認證項目	查核項目	針對公務機關（人員）	針對非公務機關（人員）	備註
人員安全認證	招募（簽約）前查核（刑事犯罪紀錄、酗酒、賭博習慣、財務狀況、社團活動、心理及個性障礙）	∨	N/A	實際實行僅限與國家安全相關之部門
	填寫基本安全認證資料	∨	ㄨ	有些單位附帶要求指紋紀錄
	定期／年度查核	∨	ㄨ	
	就職期間之查核	∨	ㄨ	
	離職或轉調其他單位	∨	ㄨ	
	有關業務之討論、安全教育訓練	∨	ㄨ	
設施安全認證	空間規定及區隔	ㄨ	ㄨ	僅限軍事部門有較嚴謹規範
	辦公自動化及相關設備	ㄨ	ㄨ	
	儲存容器與異地備份	N/A	ㄨ	
文件資料保密等級	機密等級設定與區分	∨	N/A	
	物品使用之管理與規範	∨	N/A	
	通訊設備（電話、傳真、手機）之使用與管理	∨	N/A	
資訊安全認證	公務電腦使用規範與密碼存取	∨	ㄨ	
	相容性、使用與管理、機房管制	∨	ㄨ	
	密碼加、解密傳送	N/A	ㄨ	
	網路安全與管制	∨	ㄨ	

附註：

1. ˇ代表「有」，ㄨ代表「無」，N/A 代表「查無資料」或「無法確定」

具體而言，台灣安全認證制度面臨以下的問題與缺失：

一、　缺乏明確的法源，各項規範散見於各部門，缺乏對「安全認證」的整體規劃；

就台灣安全認證制度的主要缺陷來說，台灣目前所面臨的最大問題在於法令規範相當缺乏。就公務員部份，法令或許不足，勉強以行政命令或相關單位組織條例來規範安全認證的執行，但是針對非公務機關或人員的規範除了國防部之外，幾乎付之闕如。

二、　即使已經有相關法令規範，卻還是劃地自限；

就以與本研究最爲相關之「涉及國家安全或重大利益公務人員特殊查核辦法」爲例，這其中最主要兩大問題包括：第一、本辦法明確指明所規範的對象爲「公務人員」，非公務人員如果執行涉及國家安全或重大利益之工作或任務時，完全無法被規範；第二，即使本辦法明確規定法務部調查局爲主要負責進行安全認證之機關，但是不遵守此項辦法的結果並不會產生嚴重的法律後果。根據該辦法第九條的規定，即本辦法第四條、第五條雖然明訂各機關需根據條文請法務部調查局進行特殊查核，但「未依第四條、第五條規定函請法務部調查局辦理特殊查核者」卻僅只需要「負相關違失責任」。換句話說，這種責任到底是刑責、罰鍰或其他，本辦法並沒有規定。

再以國防部制定之「從事及參與國防安全事務人員安全調查辦法」爲例，其中規範雖然詳盡，最後卻並沒有規範任何罰則，換個角度說，負責執行安全調查的保防單位即使未依規定對於相關人員進行安全調查，其所應負之責任爲零，這等於爲未來的執法提供了極大的漏洞。

三、　除法務部調查局外，缺乏公正、廣被認可的安全認證機構；

從公務機關業務繁瑣、無法兼顧所有情事的角度來看，專以法務部調查局作爲安全認證的主要單位在執行上確實會面臨很大

問題，遑論安全認證的過程需要投入相當之人力與經費。要解決這種情形，除了必須進行透過立法調整法務部調查局之相關結構與預算等龐大工程之外，另外一個較有效率的解決之道就是由政府出面，與民間企業或其他足資執行安全認證的機關單位合作，由政府聘請專人對這些單位進行先期審核與驗證，最後再將這些單位列爲合法、並經政府驗證之單位，使這些單位取得相當程度之公信力，再以契約方式聘請這些單位針對有需要之單位、或從事國家安全相關之法人機構或個人進行必要之安全認證工作。

四、 無法貫徹制度；

正如本章所探討，台灣當前雖然在安全認證的制度上處於相當原始狀態，但並不意味完全缺乏這套制度。可是往往政府部門在與非公務人員（機關）進行有關安全研究計畫過程時，根本無法貫徹執行安全認證工作，部門內的政風單位不是變成負責其他業務的示範部門，就是爲迎合主官之意，自動放棄監督之責，使得政風單位無法發揮應有之功能。

五、 各單位未能利用資源整合，建立統一的安全認證資料表格；

各政府部門的本位主義仍然濃厚，在尚無統一事權機關的情況下，各單位往往自行其事，對於基本安全調查或更高階的安全調查缺乏統一運用的觀念與作法，結果是各部門作法各不相同。按照這種情況，如果一個非公務機關、人員跟不同的政府部門合作進行國家安全相關的計畫，其結果可能會演變成該組織必須因應來自各個不同部門的安全認證檢查，造成人力、資源上嚴重浪費。

六、 缺乏對於安全認證的了解與重視；

根據實際訪談結果顯示，目前國內政府部門對於「安全認證」這一詞彙並不清楚其內涵，有些探討相關法令的刊物甚至將其直譯爲「安全清除」。實際受訪人員在首次聽到「安全認證」一

詞時，也往往將其與資訊獲某些證照資格聯想在一起。但是一旦訪談人員將「安全認證」詞彙轉變成「忠誠（或忠貞）調查」時，受訪者即可立即表示完全理解。這一問題也顯現出國內在仿造國外推行制度時，因爲翻譯語意上的混淆，導致制度的引介和宣傳、推行造成很大的困擾。

七、 機密資料的定義與其他問題；

目前國內對於所謂「機密資料」的等級認定雖然在通過國家機密保護法之後有比較明確的標準，但是其中仍然有很大的解釋空間。至於定義機密的根據，除了依據權責機構及業務承辦者這項依據之外，沒有辦法再有其他可供參考的依據。在這種情況下，仍有可能因爲承辦人員的認定導致某些非機密性資料被標示爲「機密」。此外，在資料的分類、歸檔、影印、攜出入等方面上還是缺乏更爲嚴謹的規範，資料外洩的可能性非常高。

八、 目前安全認證程序普遍將重點放在「人」的身上，而忽略了「設施安全認證」也佔有同等的重要性；

現行國內的安全認證制度主要還是將重點放在人員方面，文件資料、資訊系統次之，對於所謂「設施安全認證」也缺乏認識與了解。殊不知，人員安全認證固然重要，但是如果沒能輔以設施的配合，機密資料外流的可能性依然存在、風險性亦然。這也是前一節所提到，這是台灣安全認證制度中最脆弱的一環。

九、 與國防相關的重要科技部門或機構對於安全認證的缺乏重視，甚至在執行上完全付諸闕如，重要科技資料可隨時爲外人所探取；

根據受訪者訪談記錄顯示，目前與國防相關地重要科技部門或研究機構完全沒有採取所謂的安全認證措施，最嚴重者甚至是可以任由外人任意獲得接近機密資料或軟體的機會，洩密的可能性幾乎無所不在，但是卻也不見有權責的主管單位針對此一問題謀求解決之道，這對於機密防務、資訊安全、甚至整體的

國家安全與利益實爲無可忽視的一大隱憂。

十、 民主法治的觀念未臻成熟，以致於缺乏對領導人、甚至國家的認同，並連帶影響對「保密」的規定與要求。

台灣的政治情勢在判定上不能說不特殊，比方說因爲歷史因素所導致兩岸關係的疏離與敵對，連帶造成日後國家認同差異的產生等就是一例。再加上民主化未臻成熟，使得部份軍事或安全部門人員在任職過程中對於國家領導人、甚至國家定義產生認知錯誤，連帶影響其對於機密資料的防護，對於相關規定也未能善盡職責遵守，在這種情況下，國家安全或利益可能會因此而蒙受重大損失。

台灣的安全認證制度遠不如西方國家那樣縝密而成熟是可以肯定的，最起碼目前所面臨的十大問題就是一個相當艱鉅的挑戰。面對這些問題，當務之急便是提升對於國外安全認證制度的了解，同時參照國外優點，加以改進。這也是接下來的章節所要提到的內容，不過無論如何這其中改進的關鍵還是在於政府部門的積極介入與努力。

第三章　現行美國安全認證制度之探討

近代美國的安全認證與保密資訊法源可追溯至第二次世界大戰結束以後，美國政府對於軍事、國安部門一連串的整併改造。與安全認證相關的法源可分爲一般法案與總統行政命令兩大類，政府單位的作業要點或規定均由這兩大類法源衍生而出。現就美國關於安全認證與保密資料之法源與相關規定作一簡介。

第一節　美國之法源與相關規定

壹、法源

一、一般法案

（一）一九四七年國家安全法（National Security Act of 1947）

一九四七年國家安全法係於第二次大戰後由杜魯門總統簽署，法案內容分爲兩大要點：第一，外交政策的組織演變：成立國家安全會議（NSC）、中央情報局（CIA），以作爲總統形成外交政策之得力助手。國家安全會議的成員包括正副總統、國務卿、國防部長及其他成員，如中央情報局局長等。第二，軍事組織的再造。原戰爭部（United States Department of War）與海軍部（United States Department of the Navy）合併爲國防部（United States Department of Defense）。

（二）一九五〇年國內安全法（Internal Security Act of 1950）

一九五〇年國內安全法乃是當時美國政府爲了防範共產黨勢力在美國擴張，特別訂立此法以打擊共產黨。在本法案第三節「國家安全局人事安全程序」中，明白規定所有國家安全局聘僱之人員均需通過徹底實地調查與接觸機密情報的安全檢查程序（第 831 條）。國家安全局內設置評估委員會，負責對接觸機密情報人員之忠誠與適任進行評估，並提出報告與建議（第 832 條）。

（三）一九五四年原子能法 （Atomic Energy Act of 1954）

一九五四年原子能法的立法目的在於確保放射性原料與周邊的物質被妥善保管與使用。其中規定，政府機關應以規定、規章、命令等方式，確保核能原料與周邊物質被妥善保管與使用，以維護國防安全及民眾健康（第 161 條）。凡與保密資訊或國防資訊有關之機構，均應盡一切努力保護保密資訊不被洩漏。另，凡申請使用、持有、保管核能物質或需興建相關設施者，均要通過能源部的考核，確定其具有申請許可的資格（第 182 條）。以上各條文賦予能源部長保護機密資訊不被洩漏的權力，並要求能源部針對其本身以及有相關業務往來之承包商訂立放射性物質的保護標準。

（四）一九九六年經濟間諜法（The Economic Espionage Act of 1996）

在本法第 1831 條中規定有經濟間諜罪：

1. 通則：任何人意圖或明知其犯行將有利於任何外國政府、外國機構或外國政府代理人，而故意為下列行為者，應處以 15 年以下有期徒刑，或科併 50 萬美元以下罰金。（團體：科 500 萬美元以下罰金）

（1）竊取、或未經授權而佔有、取得、攜走、或隱匿、或以詐欺、詐術、或騙術獲得營業秘密者；

（2）未經授權而拷貝、複製、筆記、描繪、攝影、下載、上載、刪改、毀損、影印、重製、傳輸、傳送、交付、郵寄、傳播或轉送營業秘密者；

（3）明知該資訊係被竊取、盜用或未經授權而被佔有、取得或轉換之營業秘密，而收受、購買、或持有者

（4）意圖為第一款至第三款之任一犯行者，或多人共謀為第一款至第三款之任一犯行者，其中一人為達共犯之目的已著手實施者。

二、 總統之行政命令

（一）行政命令第 10450 號（1953.04.27）

本命令明訂政府雇員之安全調查需要。各機關雇員均需有基本安全調查、調查範圍視其職務需求而定。所有安全調查均需包括：指紋紀錄、警政機關紀錄、求學、受雇紀錄等。

（二）行政命令第 12333 號（1981.12.04）

本命令之主旨爲美國的情資活動。美國的情資活動目的應在於提供總統與國安會制訂外交、國防、經濟政策所需之資訊，並保護美國國家利益免於外國威脅。

與情資活動有關之單位或官員：國安會、外國情報諮詢委員會（National Foreign Intelligence Advisory Groups），情報單位如：中央情報局、國務院、財政部、國防部、國防部長轄下之情報單位、能源部、聯邦調查局。本命令尚分別規定其單位架構、首長職責及功能等。

（三）行政命令第 12356 號（1982.04.02）

本命令之目的係將國家安全資訊之保密區分、解除保密區分及維護，訂定統一的系統。重要內容包括：保密區分之等級，以及應予保密的資訊種類、保密資訊之維護等。

（四）行政命令第 12829 號（1993.01.06）

目的：設立國家產業安全計畫（National Industrial Security Program, NISP）以保護授權給與美國政府有契約關係的法人使用之保密資訊。重要規定包括：國家產業安全計畫由國安會進行政策指導，執行單位爲國家資訊安全監督局、NISP 之作業要點內容以及 NISP 執行的方式等。

（五）行政命令第 12958 號（1995.04.17）與行政命令第 13142 號（1999.11.19）

此二行政命令之目的在於制訂美國政府對公務人員接觸機密等級區分制度、要求國家安全資料保密區分應加註機密識別等級等。行政命令第 13142 號係增修行政命令第 12958 號之用。重

要規定包括：原始資料機密化（說明原始資料分類爲機密的標準、有權區分機密的機關、應列爲機密的資訊種類、列爲機密的時間長短、區分及註記方式）、衍生資料機密化、解密及降密等、機密保護、機密資料分發控制、執行及審查、成立「機關間安全化訴願委員會」（Interagency Security Classification Appeals Panel） 以處理相關問題，成立「資料安全政策諮詢委員會」（Information Security Policy Advisory Council）對總統、國家安全顧問、白宮預算管理局局長提出資料安全政策建議。

（六）行政命令第 12968 號 （1995.08.02）

目的：爲可能獲准對於機密資訊進行初步接觸或持續接觸之雇員，建立一套具一致性之聯邦人員（包括民間包商在內）安全認證計畫。本命令主要內容包括：機密資訊之接觸、接觸機密資格之複審、上訴與救濟制度、雇員的責任等。

三、其他

（一）國安指令第 63 號 （1991.10.21）

本指令的主要內容爲單一範圍之安全調查。主旨在於避免行政部門採取之調查措施重複且耗費過多，因此規定相關安全調查之最低調查範圍及標準。重點包括：安全調查的時間範圍、國家機關紀錄的查對、對受調查對象的面談、調查內容等。另外還規定調查結果得於各機關間移交，並具有同等效力。調查結果每五年再重新確認即可，中間不必重新調查。若有理由顯示該人員可能不符合調查標準，則需重新進行調查確認。

第二節　美國的安全認證執行

壹、保密資訊分級

在民主國家中，人民有權獲得充分的資訊自由，以充分瞭解政府的運作。但是有些重要資訊關係到國家安全與人民利益，必須加以保護。否則一旦外洩，將可能引起重大的損失。爲了妥善保存這些資訊，各國政府均有專責機構並制訂許多相關規定。同時也要求因業務而需接觸、使用保密資訊的人員，必須通過安全認證，確保其嚴守保護資訊的責任。美國由於掌握許多軍事武器、高科技等與國家安全有重大關係之資訊，因此就資訊保密與安全認證工作制訂了許多規定。

一、保密資訊分級之名稱

美國政府將保密資訊區分爲三個等級，「機密」（confidential）、「極機密」（secret）、「絕對機密」（top secret）。

（一）密：用以標明資訊或資料，若有未經許可及外洩或類似情形者，而依理性判斷此情形將會使國家安全受損者。例如：對載有美國境內或海外之美地面、空軍部隊力量資訊的損害、機密性之戰爭用軍火訓練、維修及檢查等相關技術性資訊、武器特性、測試資料、設計及生產資料等。

（二）機密：用以標明資訊或資料，若有未經許可及外洩或類似情形者，而依理性判斷此情形將會使國家安全嚴重受損者。例如：會導致外交關係分裂而明顯影響國家安全者、對某計畫或某政策有明顯損害而與國家安全有直接關係者、特別之軍事計畫或情報行動資訊，或會損害到上述行動之資訊、與國家安全有關之特別科學或技術發展等。

（三）極機密：用以標明資訊或資料，若有未經許可及外洩或類似情形者，而依理性判斷此情形將會使國家安全遭受極爲嚴重損害者。例如：針對美國及其盟國之武裝敵對行爲、導致外交關係分裂而對國家安全產生致命影響、損害重要國防計畫、或複雜之密碼與通訊情報系統、敏感情報活動曝光、洩漏與國家安全有重大關連之特別科學或技術發展

等。[8]

二、保密資訊的種類

下列的分類爲有關美國政府要保護的資訊類別：

（一） 人員資訊：包括政府人員；與政府有業務往來之法人；軍事人員等。

（二） 活動安全：如情報收集與分析；敏感的行動、人員、財產之遷移；敏感的訓練；通訊、網絡聯繫；科技研發及敏感科技；敏感科技的生產；保護核武、生化武器的資料；保護武器、爆裂物及相關設備之資料。

（三） 資訊：如保密資訊；尚未分類資訊；系統設計；情報設備；取得專利權之資訊；系統性能與弱點；敏感的資料；敏感的金融資料。

（四） 設備：如產業場所/基地；總部；區域辦公室、行政大樓；訓練設施與環境；法人之設施環境；儲存設備及環境；生產設備；研發實驗室；發電廠；設施、機具之停放場所；機棚；駐在地等。

（五） 設備、原料：如運輸車輛或設備；維修設備；操作設備；通訊設備；安全設備；武器；自動資訊系統設備。

三、保密資訊之分級

（一） 唯有揭露後可合理推定將損害國家安全的資訊才可列爲保密資訊。

（二） 當對資訊是否應列爲保密資訊存疑時，應列爲「機密」保護之。對於保密資訊分級合適性存疑時，以較高之分級標準保護之。

（三） 若總統、機關主管或依法指定之官員以書面做出資訊分級之判定時，得撤銷原有之分級，或將以公開之資訊重新列爲保密資訊。

[8] John Pike, “Security and Classification, ” <http://www.ostgate.com/classification.html >

四、保密資訊分級之職權

以國務院規定爲例：

（一） 極機密：國務卿或由國務卿、助理國務卿依法指定高級官員。通常被指派之官員職位均不低於助理國務卿。如：部長，代理大使、駐節海外之獨立領事等。

（二） 機密：除了有權區分極機密資訊之官員外，尚有國際合作發展機構（AID）與公共聯繫辦公室（USIA）主任等。該職權可委任予國務院之高級官員。

（三） 密：除上述官員外，海外私有投資公司之總裁亦享有此權限。

（四） 被授權分級職責之個人，不得將職權重新委任予他人。

五、列爲保密資訊的時間長短

以國家資訊安全監督局之規定爲例：

（一） 資料列密後，應登註密等、列密人、列密機關、解密指示、解密時間、列密原因等。依行政命令第 12958 號規定，資料列爲保密資料的時間長短係以其敏感性、日期、事件重要性等作爲判別標準。在將資料列密時，解密期限不應超過十年，該日期以最初決定密等之日期開始起算。如該資料性質特殊，或與國家安全有重大關係，可不受十年解密期之限制，但必須在文件上加註。如文件年限已超過廿五年，則可自動解密，並決定該文件是否應永久保存。

（二） 免受十年解密限制的資料範疇有：

1. 情報來源、手法、運作，或密碼系統及其運作方式。
2. 足以協助發展或使用大規模毀滅性武器之情報。
3. 美國武器系統發展、武器系統內使用之科技情報。
4. 美國軍事謀略、國家安全緊急規劃。
5. 外國政府情報。
6. 破壞美國與外國政府關係、洩漏機密情報來源之資訊，在十年後仍將嚴重損害外交運作者。
7. 負責保護美國總統、副總統、及其他與國家安全有關特定人士官員者。

8. 違反法令、條約或國際協定之資訊。

六、衍生資料保密分級（derivative classification）

依行政命令第 12958 號規定，經參考或使用原始機密資料後，又產生的資料，也應將其列爲機密。衍生資料的密等由原始資料的密等來決定。在衍生資料的段落中，必須指出使用資料的來源。

唯有因改寫或刪除，使衍生資料明確喪失其所以被列爲保密資訊之理由，始可除去或降低衍生資料之密等。

七、撤銷及降低保密資訊之分級

（一）保密資訊一旦不再影響國家安全，即應儘速撤銷或降低其保密分級。

（二）有權撤銷或降低資訊密等的官員，與區分資訊密等之官員規定相同。

八、保密資訊之維護

（一）通過安全認證者，且其利用資訊爲合法、必要時，得利用保密資訊。

（二）各機關應管制，以確定保密資訊之安全。

（三）保密資訊非經原始機關之同意，不得在其他機關以外傳布。

（四）經總統指派的機關首長，可以書面指示創立「特別利用資訊計畫」。CIA 局長有權創立有關情報活動的利用計畫。創立「特別利用資訊計畫」的首長，亦應維持報告系統。資訊安全監督局局長對各報告系統有利用權。

九、資訊安全監督局（Information Security Oversight Office, ISOO）

資訊安全監督局乃是根據行政命令第 12356 號而成立，係美國政府體系中，負責安全認證之重要機構。其主要功能如下：

（一）經國安會核定後，發佈資訊保密之相關指令，該指令對各機關有拘束力。

（二）監督各機關資訊保密之工作。

（三）審查各機關之施行規定、內規、要點等。如與本命令牴觸，ISOO 局長在國安會同意後，應要求修改該規則。

（四）對相關政府單位及法人進行實地監督，要求法人提供報告及必要的合作。如 ISOO 的要求對國家安全有重大影響，該單位或法人得向國安會請求拒絕 ISOO 之指令。

（五）審查官員申請區分資訊保密等級權力之案件。

（六）處理來自政府內外的抱怨或建議。

（七）透過國安會，向總統報告諮詢委員會的建議。

（八）召開並主持機關間會議。

貳、人員安全認證

在既有之國家安全資料機密等級分類上，政府可統一規定人員安全認證規範，核發審查作業，與任何必要接觸機密資料的人員必需遵行之管制規範。而人員安全認證（personnel clearance） 則於工作人員必須接觸或執行任何機密性工作或服務時必須取得。機密資料之管理者是以「有無需要」（Need-to-Know）來決定，哪些人可獲得授權接觸或使用機密資料。

人員安全認證的調查程度，依調查對象獲得授權接觸或執行的保密資訊層級而不同。美國政府的人員安全認證程序爲，先進行一般之安全認證調查，若受調查對象能夠接觸的保密資訊密等越高，所要接受的調查也就越詳細，費時也更久。

爲了避免各政府機關採取之調查措施重疊且耗時，造成行政資源浪費，美國政府特於 1991 年 10 月 21 日頒佈的國安指令第 63 號（National Security Directive No. 63）中，指示全國各政府機關通用之相關安全調查最低調查範圍及標準。

一、國安指令第 63 號：

（一） 人員安全調查的時間範圍：過去 10 年或年滿 18 歲後（以時間較短者爲準），調查範圍可視需要擴大。

（二） 國家機關之查對：聯邦調查局應對調查對象、其配偶/同居人進行調查，調查包括：指紋紀錄、與該人員有關之相關國家紀錄（如：中情局、聯邦人事管理局、移民歸化局等相關紀錄）

（三） 填報資料：需翔實填寫與國家安全相關的標準表格 SF 86（Standard Form 86）、兩張指紋卡 FD-258 （FBI applicant fingercards）

（四） 面談：受調查對象除要填寫問題表格外，尚須接受面談。面談係由受過訓練之安全調查人員或反情報人員進行，調查過程中，發生重大訊息或矛盾時，應進行額外之面談，另外，在政策許可下，得進行測謊。

（五） 安全認證中，必須查明下列有關受調查人的資訊：

1. 出生：出生日期地點與獨立的出生證明
2. 公民資格：調查對象需爲美國公民（應取得公民資格之獨立證明、國外出生之近親，亦應有公民資格或法律地位之證明）
3. 教育狀況：由學術機構以封緘成績單之方式取得學位/文憑之獨立證明，或所有教育紀錄不再調查範圍內，需確認該調查對象有高中以上教育程度。
4. 受雇情形：調查範圍內所有受雇情形。至少應包括最近兩年之紀錄。任職六個月以上之工作，應約談兩位上級或同事。（無六個月以上者，至少應約談一位主管或同事）超過 60 日以上之失業期間，均應確認，如先前有關聯邦職務軍職等，亦應確認。
5. 證明人：需有四位（至少三位係由調查單位主動接觸），證明人應對調查對象在社會生活上有認識，所有證明人加起來的認識時間應涵蓋整個調查範圍。
6. 鄰近地區：居住六個月以上者，應訪談最近五年內之鄰居。確認目前之居所，必要時得清查其租賃紀錄。無任何居所超過六個月者，應對其鄰居加以訪談。
7. 信用狀況：過去七年內調查對象曾居住、受雇、就學達六

個月之所有地點之財務、信用狀況確認。

8. 地方機關之查對：查對調查範圍內曾居住、受雇、就學達六個月以上所有地點之相關警方紀錄。目前居所的紀錄查對。
9. 公開紀錄：離婚、破產、其他民刑事訴訟之確認

（六）調查結果得於各機關間相互移交，並應視爲符合調查標準。調查結果每五年再重新確認即可中間不必重新調查。若有理由顯示該人員可能不符合調查標準，則需重新進行調查確認。通過初步安全認證的人員，將視其接觸保密資訊的密等而繼續不同程度的安全認證調查。

二、聯邦調查局之安全認證程序

（一） 一般安全認證程序：

1. 填寫 SF 86 表格（Standard Form 86）
2. 兩張指紋卡 FD-258 （FBI applicant fingercards）
3. 進行背景與紀錄調查

（二） 秘密安全認證: 其工作必須接觸到「密」、「機密」等級的資訊者，FBI 將會對其進行秘密安全認證。通過查核者，在他人陪伴下，可接觸使用機密資訊。一般多爲「非」FBI 特別小組成員、「非」在 FBI 辦公室出入者。

（三） 秘密安全認證程序：

1. FBI 向各政府單位查詢該員之各種過去紀錄（犯罪紀錄、金融財務紀錄等）
2. 填完 SF86 和 FD-258，通過秘密安全認證後，必須簽署保密協定。（non-disclosure agreement）
3. 秘密安全認證一般耗時約 45-60 天

（四） 極機密之秘密安全認證：其工作必須接觸到「極機密」、可單

獨使用「極機密」資訊者，一般爲 FBI 特別小組成員、經常在 FBI 辦公室內部工作者，其調查程序：

1. 同「秘密安全認證程序」
2. 背景調查之時間範圍追溯至 10 年前之紀錄
3. 簽署保密協定
4. 極機密之秘密安全認證耗時約 6-9 個月

（五）背景調查的項目：

1. 犯罪紀錄、信用紀錄、
2. 與該員進行面談
3. 如該員需接觸或使用極機密之保密資訊，則應調查該員背景、紀錄、出生、教育、職業、兵役紀錄、民刑事犯罪紀錄、財務信用、健康、精神疾病、藥物酒精使用情況。
4. 以上的調查，該員之家人、朋友、配偶（離婚者亦包括）之相關紀錄均要一併查核，另 FBI 將派人至該員住家附近與鄰居面談。

三、國防部

爲了整合國防部龐大的安全調查工作，美國國防部自 1972 年由尼克森總統簽署法案成立 Defense Security Service （DSS）三十多年來，國防部已逐漸將安全認證之工作集中由 DSS 處理。

（一） 調查對象：國防部之軍、文、及往來法人之員工，以決定其是否適合進入軍事產業、可否接觸、使用、持有機密資訊等。

（二） 認證程序包括：從調查局或國外有關機構詳細調查申請者的個人相關資料、財務調查、約談與申請者認識之人士，推薦者、同事、朋友、老師、鄰居、其他個人。DSS 會集中注意調查對象的行爲和特質，尤其是誠實度、是否值得信賴、財務狀況、犯罪紀錄、情緒穩定度及其他類似的特質等。

（三） 調查對象必須填寫調查表標準表格 Standard Form 86（SF-86）或利用電子問卷。（Electronic Personnel Security Questionnaire, EPSQ）

（四） 受過訓練的認證官會把調查對象的資料與定型的標準做比較，以決定該對象是否可通過安全認證。安全認證應確定所核發對象之忠貞度、信賴度及可靠度符合國家安全之要求。認證包括：忠貞度、對外國偏好程度、個人操守、飲酒習慣、豪賭行爲、財務狀況、犯罪紀錄、社團活動、心理及個性之障礙、不當使用資訊科技系統、受外國影響程度、性別取向與行爲、財務考量、藥物使用習慣、違反安全記錄等。另應定期使用測謊器測試，以對個人審驗問卷調查之正確性。

（五） 人員安全認證調查歸 The Personnel Investigations Center, PIC（位於馬里蘭州）管理，最後的報告會交由適當機構進行裁決。

參、設施安全認證

美國政府仰賴經過安全確認的設施來管理其安全認證計畫。設施安全認證是用以決定某法人的工作環境與設備，是否具備接觸機密性資訊或執行機密性合約之資格判定。此爲政府單位與民間法人承包商間合作伙伴關係的基礎。

一、申請設施安全認證的法人：

以法人必須接觸機密性資訊才能執行工作爲基礎。而且法人必須於本國法律規範下，於國內創立並實際存在。法人必須具備良好之商譽及法律紀錄可供查詢，不能被外資擁有控制或影響。而外資法人安全認證，任何具有外資股份控制權及外資影響力之法人，皆須執行安全評估以降低安全上之風險。同時任何法人絕不能與國家利益有任何程度的牴觸。

二、設施安全認證的內容：

1. 法人的工作環境與設備應提供存放機密文件於經過安全檢驗合格之容器、保險庫或密閉空間，並需要額外之防護措施。
2. 限制性區域，工作期間如有必要於開放空間內處理機密資料，必須設置以限制區域以作爲接觸機密文件之特定限制區。密閉

區域，一律須加以控管，防止未經授權之進入及接近。

3. 額外防護措施，如入侵偵測系統及警衛人員。
4. 容器、櫥櫃、保險庫及密閉空間之鑰匙、掛鎖及號碼鎖之防護。
5. 先進的接近控制系統及裝置，自動化的接近控制系統及電子、機械或電機裝置，將可作爲取代控制進入限制性或密閉區域之警衛人員。

三、能源部：

參考聯邦法典第十編中有關核能管理委員會（Nuclear Regulatory Commission）之規定（本規定不適用於極機密之資訊）

（一）何時需要申請設施安全認證？

任何需要接觸、使用、儲存保密資訊或特殊核能原料（Special Nuclear Material, SNM），或因業務而需單獨進出管制區域之法人，都必須立即向主管單位申請設施安全認證。

（二）提出申請時，必須註明法人名稱、設施位置、以及是否獲得其他單位之設施安全認證等。如先前未獲得其他設施安全認證，則必須提供標準安全工作之守則、安全措施以及建築物之藍圖等資訊。

（三）設施安全認證過程：若申請之法人已通過其他政府單位之設施安全認證，核能管理委員會一般都會接受該單位之申請並視同通過設施安全認證。程序如下：

1. 該法人提供之資料應證明其安全設施與實行計畫符合國家利益，且未受到一定程度的外國影響或控制。評估的標準爲：是否有遭到外國間諜威脅的可能？是否有未經授權之科技轉移？保密資訊的等級？是否遵守相關法令規範？若該法人受到外國勢力影響（如：所有權之轉讓、負債、單位高級主管之變更），必須在三十天內通知核能管理委員會。
2. 核能管理委員會進行適當之安全複檢
3. 法人之重要管理人員均需通過人員安全認證
4. 負責安全之人員必須爲美國公民

在整個調查完成之前的過渡時期，CSA 可先核發暫時之設施安全認證

（四）一旦通過設施安全認證，該單位或人員必須經過 CSA 核准才得以變更名稱、地點、安全計畫、設施藍圖等。並在進行變更 30 天前，將所有變更以書面通知 CSA 及核能管理委員會，以便上述兩單位進行評估。CSA 會將評估結果以書面通知該單位。

（五）法人除了應明確禁止員工在於安全維護裝置之場所與電話通路上討論保密資訊外，更應對工作場所進行管制。法人應建立並維護一可阻止及偵察非法入侵及保密資訊從其場庫辦公室被移動之系統。

（六）所有進出工作場所之人員，必須接受隨身物品檢查。並需建立緊急狀況時保護保密資訊之程序。

（七）對外收發紀錄：應保有收發資料之日期、密等等級、資料從何處收到或發往何地等紀錄，至少保留兩年。

（八）保密資訊之傳送，應由工作場所內連續接收系統行之。並以連號號碼登載，影印號碼應放於極機密文件及所有相關處理文件上。如需於工作場所外傳送，則必須將保密資訊裝置於不透明材質之封袋中，並以兩層封存。封袋外僅標明接、送者之地址，不註明內含資訊之保密等級。收據應由收件人簽收，並保存兩年以上。

（九）極機密資料之傳送，必須先獲得主管機關許可，可使用「國防專差服務」（Defense Courier Service）。若由商業運輸業者代為傳送保密資訊，則運輸範圍僅限於本國境內，該運輸業者也必須是獲主管機關核准傳送保密資料者。若有必要，可使用專差、護衛，以保護傳送之保密資訊。

（十）儲存及儲存裝備：由美國總務署（General Service Administration, GSA）將儲存保密資訊之容器、貯藏室、隔間材料、門鎖、鑰匙等器具設備建立並頒行統一標準、規格，並將經認可之製造商與儲存裝備列於聯邦供應表（Federal Supply Schedule）中。

（十一）　限制性區域：限制性區域需有明確範圍界定，但不一定要有硬體區隔。該區域內之所有工作人員均需注意是否有未經許可進入該區域的人士。

（十二） 密閉區域：因儲存的保密資訊其體積或本質特性，或因作業需要，必須建構一儲存保密資訊的密閉區域。建立密閉區域必須由主管安全機關核准，並依其要求之標準興建。密閉區域必須利用管制出入的器材，避免發生未獲授權者進出該區域的情況。在密閉區域內開啓任何儲存容器，均需先獲得主管安全機關之核准。

（十三） 儲存容器、密閉區域之門鎖、號碼鎖、鑰匙等應限定最少數需要者才知悉相關資訊，每月必須清查、每年需應新或輪替，管理人員如有更換，其管理之門鎖、鑰匙亦必須清查更換。

（十四） 管制出入器材：法人所建立的管制出入系統，必須可辨識進出管制區域或密閉區域之人員爲何、並可立即判定該人員是否有權可進出該區域。該系統必須符合主管機關所頒佈的各項標準。

1. 在能源部保護機密物質指示（Control of Classified Materials）中，規定：1. 機密物質與用具的使用或儲存地點，是否有機密用具之說明

2. 避免訪客或洽公人士看到機密用具
3. 陳列室之位置、參觀路線、警衛、防護措施
4. 機密物質或用具之運送途中有一定之安全程序
5. 所有機密物質或用具的輸送方式（人力、飛機、火車、信件）及每一輸送管道所使用之頻率均需記載。
6. 由於能源部管轄許多機密物質的性質特殊，有許多儲存場地是露天的，因此能源部特別針對類似特殊場所制訂保護標準。如：使用警報器、人員巡邏、儲存場所之構造、隔間，鄰近區域列爲保護區等等。

（十五） 設施安全認證終止的原因：

1. 該單位或設施不再需要接觸、使用、儲存、再製、傳送、輸送或處理保密資料。
2. 核能管理委員會認爲繼續授予該單位或設施此等認證，不符合國家安全利益。當設施安全認證遭到終止，核能管理委員會將以書面通知該單位或設施。

四、國防部：

隸屬美國國防部的 Defense Security Service 在「國家產業安全計畫」（National Industrial Security Program, NISP）中，每年都要代表國防部及其他廿一個政府部門，對約八十萬名相關產業人員進行安全調查。是項計畫乃是爲了確保民間產業、大學等機構在履行政府合約或進行與國家安全相關計劃時，能確保其機密設施與資訊之安全。同時，DSS 也負責監督並協助在 NISP 計畫中超過一萬一千項機密設備、一千萬份機密文件的安全維護。DSS 爲法人提供的安全認證包括下列數項：

（一） 授權法人設施是否可存取機密資訊，
（二） 確認法人是否有保護機密資訊的適當安全設施，
（三） 與法人合作，確保其依照「國家產業安全操作手冊」（NISPOM）進行安全系統的安裝與維護。

「最初之設備安全認證」包括：確認法人之管理部門與主要人員是否符合 NISP 之規定、該法人是否受外資影響、控制，並對相關設備進行檢驗等。「年度設施安全認證」用以進行全面性設施安全認證，包含：安全複審、提出建議與協助、行政調查、自動化資訊系統鑑定、法人之安全認證流程、政府單位協助與安全簡報等。DSS 亦爲法人之工作人員進行安全認證。

法人一旦獲得與機密資訊相關的政府契約後，DSS 就會進行設施安全認證調查。包商的設備與主要管理人員都必須通過安全認證。接下來 DSS 的「產業安全官」就會展開下列工作：

(1) 訓練法人負責維護機密資訊之從業人員，
(2) 核准機密資訊的儲存設備，
(3) 核可存取機密資訊的自動化資訊系統，
(4) 應法人請求，提供其安全部門與員工相關之建議與協助，
(5) 協助法人進行安全調查，包括調查是否有洩密情形、進行補救

措施等，

(6) 確保國際間機密資訊的交換（政府對政府）遵照適當協議進行，每年要重新檢證包商的安全措施，確保所有資訊均安全無虞。

肆、資訊與通訊安全認證

美國的資訊與通訊安全認證如下：

一、能源部：相關規定可見 DOE Cyber Security Directives, 200 series：

（一） 負責能源部資訊安全工作之單位：Computer Incident Advisory Capability（CIAC），其主要任務在於追蹤可能之網路安全威脅，並協助各單位處理此種情形。

（二） 網路與資訊安全威脅之種類：

1. 外來威脅：外來之駭客刻意入侵網路資訊系統或意圖散播電腦病毒等。
2. 內部威脅：能源部網路資訊系統之使用者，故意或意外違反安全規定。

（三） 資訊與通訊安全注意事項；

1. 避免病毒或其他網路安全威脅透過電子郵件系統散播，避免濫用電子郵件系統；
2. 可與遠端連線之可攜式電子裝置（如手機、手提電腦等）需避免遭到他人竊聽或截取通訊內容；
3. 傳真機、影印機、印表機等，亦需管制以免資訊外流；
4. 辦公位置：在轉換辦公位置或公務用電腦時，必須確認已徹底清理，避免遺留任何保密資訊；
5. 不得任意在資訊設備中加載未經許可之個人軟體、分享軟體等。

第三節　民間法人與美國政府之安全考核

由於美國政府將許多研發、生產或運輸的工作委由民間公司或單位辦理，因此必須建立一套安全認證的方針，以確保機密資訊的安全。

壹、美國政府對重要民營事業機構之考核制度

美國政府委託民營生產、研發之國防、航太、資訊、關鍵材料、生化技術等高科技民間公司之相關考核制度如下：

一、政府與委託民營辦理之高科技公司先進行協商，並「定義」研發或生產之物件何者爲「機密」，何者爲「非機密」。

二、對於前項定義爲「機密」等級者，政府將對公司負責人進行安全及背景調查（美國規定公司負責人需具有美國籍）。另對該民間公司執行及參與「機密」事項之員工名單亦逐一進行安全認證。

三、經安全認證無虞後，政府與該廠商簽訂「保密協議規定」（non-disclosure agreement）。

四、另，該公司亦會要求參與「機密」事項之員工簽署類似保密協議規定，內容包括若洩漏從事之業務機密（政府解密公佈或超越解密年限者不在此限），將接受法律制裁等內容，中途離職者亦受該規定約束。

五、合約民間廠商對執行機密業務之新進員工亦需提報政府相關部門作安全認證，另該民間廠商之安全部門亦將負責平時之保密及查核工作。

貳、國家產業安全計畫（National Industrial Security Program, NISP）

美國政府除了制訂對民間公司的考核制度外，更依據第 12958 號行政命令創立「國家產業安全計畫」（National Industrial Security Program, NISP），以保護授權給與美國政府有契約關係的法人使用之機密資訊。

一、 創立國家產業安全計畫

（一） 創立 NISP 之目的：保護授權給法人使用之國家機密資訊，NISP 應適用於所有之政府單位

（二） 要保護的資訊分類:參12356號行政命令及原子能法之規定

二、 政策指導

（一） NISP 由國安會進行指導

（二） 執行及監督單位：根據 12356 號行政命令而設立之國家資訊安全監督局（Information Security Oversight Office, ISOO）

（三） ISOO 需執行的工作：發展、公佈國安會核准的指令，以執行本命令

（四） 監督政府單位及法人是否確實執行本命令

（五） 複審各單位之施行規定、內規、要點等。如與本命令抵觸，ISOO 局長在國安會同意後，應要求修改該規則。

（六） 對相關政府單位及法人進行實地監督，要求法人提供報告及必要的合作。如 ISOO 的要求對國家安全有重大影響，該單位或法人得向國安會請求拒絕 ISOO 之指令。

（七） 向相關單位首長或代表報告違反本命令的情形，以便採取補救措施。相關報告應直接交遞相關單位首長。

（八） 透過國安會，向總統報告諮詢委員會的建議

三、 諮詢委員會

（一） 委員會成員：ISOO 局長（擔任主委）、NISP 相關之政府單位代表、法人代表。

（二） 委員會功能：對 NISP 有關事項提供諮詢意見

四、 作業要點內容：

（一） 部會分工：以國防部長爲首，其他相關部門主管爲輔（能源部長和核能管理委員會主管負責有關 1954 原子能法規定受保護資訊方面、CIA 局長負責情報來源與機密），負責頒佈、維持作業要點

（二） 作業要點應規定機密資訊管理辦法。包括：政府與法人議價、協商、簽約、契約執行期間、契約終止等期間

（三） 應列明保護機密之需求、限制其及他必要之安全措施。機密資訊包括限制性資料、之前的機密、情報來源、敏感資訊、特殊計畫等

（四） 制訂作業要點時應考慮的重點：

1. 機密一旦洩漏，對國家安全可能造成的危害
2. 現有、或未來可能導致機密洩漏的威脅
3. 執行保密方式的長、短期花費

五、 執行監督

（一） 國防部長應爲主要執行者。職責爲監督法人、決定接觸機密的層級。由 DSS 負責認證的各政府單位應同意由國防部長代爲執行上述職權。

（二） CIA 局長之權限：使用機密、監督法人，或在明文協議下，與國防部長共同擔任主要執行者。

（三） 主要執行者與相關單位協商後，爲了有效實行國家產業安全計畫，有權頒佈表格或其他相關標準。.

六、 計畫執行

（一） 相關單位應指派資深官員擔任該單位執行 NISP 的承辦人

（二） 委託 DSS 進行認證的各政府單位，其有關 NISP 的規定，應與本命令與作業要點之規定相符。本作業要點發佈後 180 天內，該單位必須開始實施各自的相關規定。各單位可參考作業要點的內容，或完全依照作業要點規定。

（三） 各單位主管應確保作業要點之執行，遇有違反本手冊情形時，應迅速採取改正措施。

（四） 執行 NISP 作業要點之花費每年要報帳，彙整報至國家資訊安全監督局 Information Security Oversight Office 主管，以爲向總統報告之依據。

（五） 國防部長等相關首長應確保政府採購法規定應配合 NISP 規定。

（六） 所有會使用到機密資訊的政府合約、作業手冊或證照核

發，均應符合 NISP 規定。在合法、可能的情形下，也應溯及既往，將過去不符 NISP 的契約等加以改變。

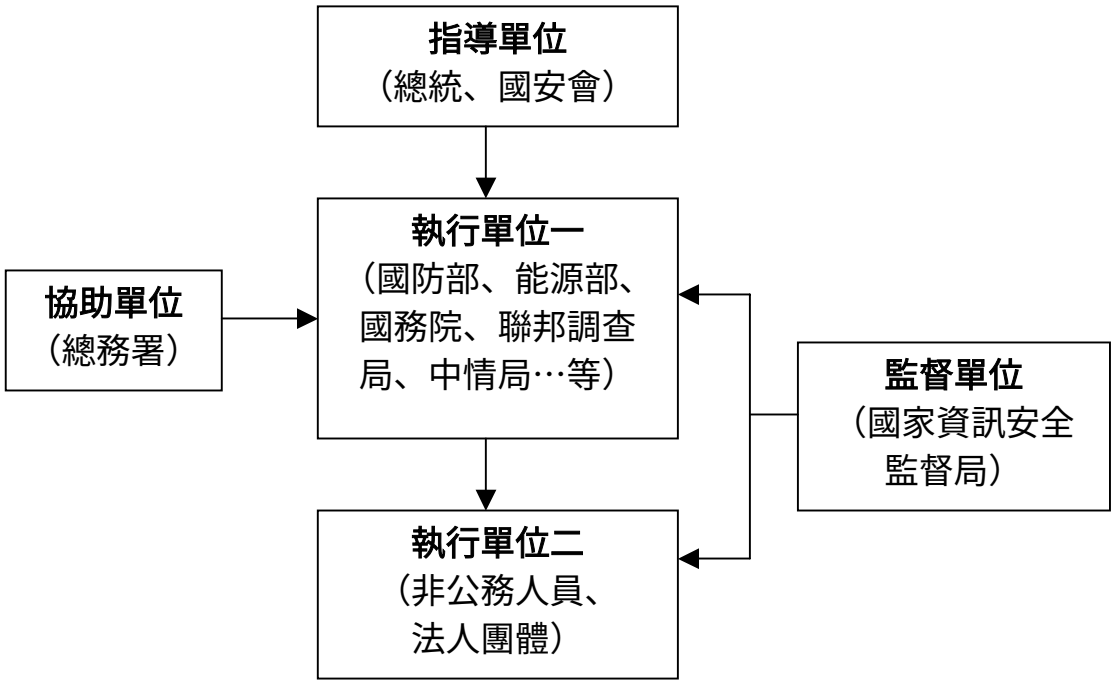
第四節　小結

綜合以上美國政府有關保密資訊與安全認證之法源與規定，我們可以歸納出以下數項值得我國參考之作法：

壹、　法源完備，體系分明，規定清楚：

美國自第二次世界大戰結束後，就開始整併國防與國家安全之機構，並制訂許多法令。其中，經國會通過的法案有四項，即一九四七年國家安全法、一九五〇年國內安全法、一九五四年原子能法、一九九六年經濟間諜法。直接相關之總統行政命令有第 10450 號、第 12333 號、第 12356 號、第 12829 號、第 12863 號、第 12958 號、第 12968 號及第 13142 號等，共計八項。經過不斷的增修，相關的法源可謂相當充足，使得保密資訊與安全認證的工作有清楚的法源根據，減少執行時可能引發的爭議。

綜合美國的相關規定，我們可以下圖來簡單表示美國的安全認證體系。從下圖中可以發現，美國安全認證法令層級相當清楚，各單位的權責劃分亦同，彼此相互配合不重疊，也因此在實際執行上極具效率。



貳、 工作整合、避免資源浪費

雖然在政府機關中需要實施資訊保密與安全認證的機關相當多，但所有執行機關的規定與作業要點均統一參考前項所列之法源規定而制訂，再依各機關不同的特性與需求稍作更改。總體而言，各機關間的執行標準與程序均大同小異，不易出現各自為政、執行品質落差太大的問題。也因為這個特點，使得各機關間的執行成果與紀錄可以互相承認移交，避免不必要的行政資源浪費。

此外，許多單位都成立專責機構來處理日益龐雜的資訊保密與安全認證工作。以國防部的 DSS 為例，該單位不但負責國防部之安全認證，同時也開放接受各機關之委託、協助民間法人的安全認證工作。此一趨勢同樣也可節省龐大的行政資源。

參、 安全認證執行方式公開、清楚

美國的安全認證、資訊保密規定均儘可能地公開相關資訊，在各機關的網站中可見清晰易懂的問答集與各種資訊，幫助受調查對象瞭解調查工作的真正意義與內容，消除可能的錯誤觀念；此外，也有助於需要申請安全認證的個人或法人瞭解所有的認證流程和需求。不但便民，更教導人民正確的保防觀念。

肆、 設計嚴謹、執行官員訓練有素

所有的資訊保密與安全認證工作，均有嚴謹的設計和詳盡的規定，不但有持續的查核，甚至小到存放文件的容器規格和門鎖都有嚴格的標準。雖然看來十分細瑣，但卻對國家安全提供綿密的保障，使洩密或危害國家安全的機率減到最低。此外，各機關均設有教育訓練課程，執行工作的官員也都必須通過各種訓練，提高人力素質，同時也保障執行工作的成果品質。

伍、 標準化作業、線上作業可提高效率，節省經費

美國政府累積了數十年的經驗，將許多安全認證的程序表格化。透過特殊與嚴謹的設計，在表格中便可獲得大部分所需的資訊。若有不足之

處，再輔以面談、測謊等方式。爲了因應無紙化的趨勢，在網路安全無虞的前提下，美國政府也開始利用網路進行線上填表作業，教育訓練的教材也可從網路下載。充分利用科技所帶來的便利，不但提高工作效率，更可爲國家節省大筆公帑。

第四章　現行英國安全認證制度之探討

除了美國之外，在安全認證制度的實行上，英國的作法也相當值得參考。不過必須說明的是，英國的資訊並不若美國公開，特別是在某些資料的蒐集上，英國會以機密爲由拒絕公開，因此本章節的撰寫皆以目前所能蒐集到的公開資料爲限。

第一節　英國之法源與相關規定

壹、 法源依據

英國的法律具有延續性，因此跟安全認證有關的法令最遠甚至可以追溯到一九一一年。以下僅就相關法令規定做一簡單介紹：

一、 相關法律

（一） 一九一一年公務機密法（The Official Secrets Act 1911）

本法係以修正案重新修訂一八八九年的公務法案。所規範的內容相當廣泛，包括間諜活動、資訊不法傳遞、禁區、企圖違反本法之行爲處分、逮捕權、藏匿間諜之處分與起訴等。修訂本法的主要目的在於防止任何人爲本身之目的，導致國家安全及利益受到損害。特別是從事資訊的不法傳遞或間諜犯罪行爲。

（二） 一九二〇年公務機密法（The Official Secrets Act 1920）

本法係修正一九一一年公務機密法，修正重點包括以僞裝身份進入禁區、擅自僞造文件或印章、處分之加重等。

（三） 一九三九年公務機密法（The Official Secrets Act 1939）

本法係修正一九二〇年公務機密法之第六章，主要重點在於明確化警察總長之權力。

（四） 一九八九年公務機密法（The Official Secrets Act 1989）

「一九八九公務機密法」的目的在於取代一九一一年公務機密

法之第二節，其修訂的目的在保護更多具有限制性的公務機密。在這項法律當中，特別重新定義機密與情報，加入與國際關係相關資訊流傳的規範，同時特別值得注意的是針對資訊的保護提出更爲明確的限制。條文的最後也說明，本法和「一九一一年公務機密法」、「一九二〇年公務機密法」、「一九三九年公務機密法」可以合稱爲「一九一一年至一九八九年公務機密法」。

（五）　一九九四年情報工作法（Intelligence Services Act 1994）

「情報工作法」的目的在於提供英國秘密情報局（the Secret Intelligence Service）與「聯合情報組織」（the Government Communications Headquarters）之行動獲得法源依據，並且使相關情報工作單位在進行國際情報、反情報工作時得以受到情報與安全委員會（the Intelligence and Security Committee）的監督。

（六）　一九九八年資料保護法（Data Protection Act 1998）

資料保護法的目的在爲提供法源，以保護資料的傳遞、取得、保存、使用與公開。主要項目包括了資料的定義、敏感個人資料、資料的特殊用途、防範資料濫用影響國家安全或造成其他損害、違反資料保護法的罰則等。

（七）　二〇〇〇年資訊自由法（Freedom of Information Act 2000）

本法修正了一九九八年的資料保護法（Data Protection Act 1998）與一九五八年的檔案法（Public Records Act 1958），爲個人以及政府的資料公開提供了法源依據。最重要的內容在於對於如何合法取得政府資訊做了詳盡的規範，也使得英國政府在解密政府機密文件時有所依據。

（八）　二〇〇一年反恐、犯罪及安全法案（Anti-terrorism, Crime, and Security Act 2001）

此法案爲因應美國九一一恐怖攻擊事件以後所制定的法律，除

對恐怖主義活動、犯罪有進一步規範之外，條文中也提到對於資訊公開所必須納入的一些新規範。

（九） 二〇〇三年核能工業安全規範（Nuclear Industries Security Regulations 2003）

爲主要規範英國核能工業之安全規範，對於核能原料的定義、取得、安全之維護、人員之安全認證等各個主題都有詳盡的規範，本法乃是一項全新的法案，於二〇〇三年九月開始正式施行。

第二節　英國現行的安全認證

英國和美國同樣相當重視安全認證，不過在用詞上略有不同，比方說美國在詞彙上使用了 security clearance，但是英國則是使用 security vetting。但是即使使用詞彙不同，在目的以及作法上大致還是相同的。

壹、 現行執行安全認證的機構

目前在英國執行安全認證的主要機構乃是英國的「國防調查局」（Defense Vetting Agency, DVA），這個機構每年負責 14 萬件左右的查核與認證，也可以說是英國政府目前最大的政府安全認證機構。

目前英國國防調查局主要針對那些在各軍種單位及國防部擔任文職的人員、以及在某些特定政府部門、或者是國防工業任職的人員進行安全認證。該部門負責確認這些人適不適任，確認後並給予認證，使受認證人員得以接觸政府的各項設施、有價資產或者是敏感性的資料。

貳、 資料的保密分級

與其他國家不同的是，在英國對於機密文件的資要保密並沒有等級的分類。根據英國公務機密法的規定，所謂的「機密或情報」，泛指所有或任何部份機密或情報單位本身之工作；或支援該單位之工作；而所指有關機密及情報之資訊，包括該類機構或支援該機構之人士所留置或傳送所有或部份之資訊。換言之，就英國對機密保護之特色而論，英國所採用的標準係以一般性、涵蓋面較廣的方式來函蓋所有應受保護的機密資料，而不採用等級之區分。

參、 人員的安全認證

在英國國內，所謂的人員安全認證（或稱人員查核）指的是清查執行某些特殊任務或者那些在工作職務上有需要獲得安全認證的人員，這些任務或工作橫跨國防部以及各軍種單位。當然，那些在企業中服務，但是其

工作範圍與國防密切相關的人士也必須獲得安全認證。此外，政府某些特定部門也會委託安全認證單位來進行調查任務。

簡單來說，執行人員安全認證的主要目的在於確保受查核人員在得到認證許可之後，可以接觸機密資料而不致發生濫用資料並導致機密外洩的情況。不過即使如此，查核過程還是無法百分之百保證這些受查核人員的可靠性，這是因爲進行人員查核後所得的簡要結果只有在調查的當時可以算是正確的，在那之後，人員的可靠性就有賴安全認證人員不斷的監督和判斷，並持續評估與認證。

安全認證程序有時候確實可以看出一個人個性上的缺陷，也可以讓政府部門了解哪些人在某些特定環境下可能或有安全上的顧慮。這些人當中，有些可能因此無法獲得工作，另外一些人則將被持續的監督或者被轉調到從事比較不敏感的工作職位上。簡單地說，安全認證查核目的就是希望那些背景有問題、或者人格有缺陷的人自動打消申請從事與國防相關工作的念頭。

至於安全認證的查核項目則包括以下：

一、 反恐調查（Counter-Terrorist Check, CTC）－通過這項調查的人士將可獲得接近那些可能遭受恐怖主義攻擊的政府建物或政府機構，但不包括那些受保護的機密文件。

二、 安全調查（Security Check, SC）－這項調查是最常進行的一項調查。那些從事長期性工作，或者經常可以無限制接觸機密，抑或有可能接觸最高機密檔案或資料的人必須通過這項調查。一般來說，這項調查每十年重複進行一次。而如果是約聘人員則每五年必須重新調查一次。

三、 進階調查（Developed Vetting）－從事那些最敏感任務或工作的人，包括可以無限制接觸最高機密資料的專任人員必須通過這項更高階的查核。進階調查乃是定期性的執行。

四、 基本調查（Basic Check, BC）－DVA 也會執行一些少量的基本調查，以確保人員與身份資料的吻合。不過一般來說，各機關

單位的人事部門或者與國防相關的企業會自行進行這些查核。這項調查乃是上述三項查核程序的最基本前提。

除了執行並檢視認證之外，DVA 有時也會做負責跟進的工作，一旦對人員安全認證情形有疑問可以隨時在認證過程中、或者在認證結束後提出。這種事後的調查工作又通稱爲「事後輔導」（Aftercare），此種工作跟其他階層的安全認證也或多或少有一些關聯性存在。

肆、　資訊的安全認證

資訊安全（Information security）乃是爲了確保資訊之閱聽、改變、傳播和其他使用情形均在獲得授權的情況下進行。資訊安全一旦遭到破壞，被竊取的資訊可能會用來施行詐欺、非法的個人資料調查、商業間諜行爲或恐怖活動等。因此，資訊安全是保障國家安全極爲重要的一環。

在一般的觀念中，都認爲保障資訊安全需要昂貴的設備與高超的技術。然而，保障資訊安全最重要的支柱卻是在於建立一套有效的管理辦法，以及使用者的安全概念。爲了與政府單位和作，各機關法人團體應該嘗試建立一套實際與有效的政策與標準，同時負責執行資訊安全政策的人員必須有充分資訊、訓練紮實，並具備適當的警覺性。

就英國現行規範資訊安全的標準而論，其內容共有六大項，簡介如下：

一、　英國標準局 7799 號規定（British Standards Institution BS7799）

BS 7799 是有關資訊安全規定中最重要，也最爲人所熟知的一項。BS7799 經過貿易與工業部（DTI）的發展、以及各公私機關的施行之後，已經演化成兩個版本：BS7799 和 ISO17799（International Standards Organisation）。這兩項標準中的規定涵蓋絕大部分有關資訊系統的使用情形。BS7799 分爲兩大部，第一部係指導原則，亦即前面所提及之 ISO17799，第二部爲施行細節。

二、　BSI 資訊科技安全基本規則（BSI IT Security Baselines）

BSI 本爲德國負責制訂資訊科技安全的機構，全名爲 Bundesamt fur

Sicherheit in der Informationstechnik，之所以會出現在規範當中主要是由於由於英國乃是歐盟的一員，因此德國所制定的規範也爲英國政府所採納。本規則的目的在於迅速處理一般安全問題、提高 IT 系統的安全性，以及簡化 IT 安全政策的制訂過程。這是一項超過 1600 頁的詳盡指南，內容極爲豐富專業。

三、 資訊科技管理項目（The Control Objectives for IT, COBIT）

本規則係由內部專業審查代表（Internal Audit Professional Representative body, ISACA）彙編而成，其目的在於建立一套規範架構，適用於大型法人的 IT 安全管理項目和相關的支援工具等。其中包含管理指南、管理項目和其他補充文件等。

四、 資訊系統安全通則（The Generally Accepted System Security Principles, GASSP）

GASSP 是爲了配合美國政府的電腦安全標準而制訂。其所根據的參考資料包括經濟合作發展組織（OECD）的相關規定和前述的 BS7799 等。

五、 資訊科技管理指南（Guidelines for the management of IT Security, GMITS）

GMITS 又稱爲 ISO/IEC TR 13335 1-4, 這是一套資訊安全管理的詳盡指南，主要是爲專業安全人員所編定。其中包含一系列有關管理概念、管理與計畫、技術。

六、 資訊科技基礎建設文庫 （Information Technology Infrastructure Library, ITIL）

ITIL 係由中央電腦與通訊局（Central Computer & Telecommunications Agency, CCTA）彙編推廣而成。這一套文件資料庫提供 IT 基礎建設的管理基礎與安全管理方式。

在上述所有資訊安全的規定中，最重要，也最具代表性的是 BS7799。BS7799 係一套最具影響力、也是廣被全球承認的資訊安全管理標準。其

目的在於建立一套有效的資訊安全管理系統 （Information Security Management System, ISMS）。BS7799 內容共分爲有兩大部分，第一部爲指導原則和相關解釋，第二部爲一套模型，教導其他機關法人單位如何建立、管理 ISMS。BS7799 不但可增加法人的工作效率，更可減少操作時的風險、確保資訊安全。

英國的資訊與通訊安全認證即爲 BS7799 認證，獲得 BS7799 認證的機關法人單位法人，即代表其資訊安全系統符合國家標準。也唯有獲得 BS7799 認證的法人才能承攬英國政府的業務。不過由於第 BS7799 二部分爲不公開之機密資訊，故僅能就第一部份進行討論。以下將逐一簡介之：

一、 安全政策（如何獲得 BS7799 認證）

（一） 認證單位：英國認證局（UK Accreditation Service, UKAS）。

（二） BS7799 認證程序與需求：

專業審查員將會對申請認證的法人進行完整的調查，確認該法人之資訊安全系統是否有效且適當運作。審查項目包括：

1. 完整性：該法人的資訊安全系統是否符合 BS7799 之所有規定；
2. 適用性：BS7799 的規定是否適用於該法人；
3. 執行狀況：該法人的資訊安全系統是否有完善的管理。申請認證的法人應繳交執行報告（Statement of Applicability, SOA），其中列明 BS7799 第二部之所有需求，以及該法人執行 BS7799 第二部之措施、矯正錯誤的方式。

一旦通過審查，該法人即可獲得 BS7799 認證。官方認證單位每六個月會再進行複查，以確保該法人確實遵守相關規定。獲得認證之後，還必須遵守下列規定，才能保持認證的資格：

1. 定期對資訊安全系統進行內部檢查：檢查項目包括負責人員是否持續監管該系統、也要提供紀錄以茲證明。此項檢查通常有一套標準的檢查表，執行檢查的人員爲該法人內

部人員。一旦在檢查過程中發現任何違反安全規定的情形，執行人員必須呈交報告。此項規定的目的在於要求法人具備迅速處理問題的能力。

2. 更新資訊安全系統之執行報告（SOA）：SOA 應該反映出系統的最新狀況，因此必須每日更新。

二、 組織安全

內容爲如何建構組織資訊安全管理方式。包括：

（一） 法人如何管理資訊安全；

（二） 相關人員、組織之責任。負責資訊安全的最高層級應爲該法人之董事會或同等管理階層。安全規範必須適用於所有員工，包括臨時雇員、與該法人有契約關係，並可能接觸到人員、辦公場所或設施的第三者等。

三、 資產分級與管理

內容爲將資訊處理設備列爲重要資產，並加以管理。在有形資產方面，法人必須有完整的資訊設備清單，如：電腦、印表機、其他儀器等。除此之外，法人所擁有的資訊也應視爲重要的無形資產。因此，法人必須建立資訊資產紀錄表，這也是資訊資產之清單。可列爲資產的資訊有資料庫、人事紀錄、各種模型、原型、測試樣本、契約、軟體授權、公關文件等。清單上還需註明負責管理人員以及其他特殊規定等。

四、 人員安全

內容爲有關資訊安全的人員訓練、責任、調查程序以及緊急應變措施等。法人必須確保各契約或員工手冊內容清楚、無爭議；安全規則的適用範圍包括可合法接觸法人資訊的單位或個人、臨時雇員或有契約關係的個人、其他法人等。除了責任規定外，法人也必須保障員工的權利。其資訊安全規定不應違反資訊保護法令。

五、 環境與設施安全

內容爲對於環境與設施的安全保護以及進出控管等。相關環境必須有

一定的安全設備，除了提供儲存資料的適當環境外，亦需防止資訊設備遭到非法或未經授權的接觸或使用，避免遭到意外或天災的損害等。

六、　通訊與操作管理

內容爲日常活動中關於資訊處理設備的正確操作與管理。由於大部分法人的資訊設備每日都要使用，因此有關日常活動的規範相當重要。有關防毒軟體、意外處理的程序、網路群組、多媒體、電子商務、電子郵件、網站、公用系統等，都包含在其中。

七、　使用控管

有關資訊及資訊系統的進出、使用管理。負責人員應利用一些管理方式來維護系統的安全，如密碼系統、進出系統的管制、定期檢查使用者的帳號、防止有人透過公用系統非法取得機密資訊等。相關規定必須符合法人的需求、有足夠的安全性，也必須取得法人雇員的信任。

八、　系統發展與維護

內容爲如何在保障安全的前提下，設計並維護一套整合的資訊系統。安全又整合的資訊系統是提高工作效能的重要基礎之一。因此，負責人員必須考量所有的安全需求，包括檔案安全、密碼的應用、登錄的規定等等。

九、　業務持續運作

內容爲當該法人的日常業務活動遭到阻礙時，應如何排解。規定範圍涵蓋大型災害到細微的內部問題。由於現在的商業活動發達，各法人機關的關係密切，可謂牽一髮而動全身。不論是重大災害或僅是某個小錯誤，都可能影響到資訊安全。爲了將意外減到最低，法人必須有持續運作的計畫、災害影響分析、執行與測試計畫等事前準備。

十、　法律條文規範

載錄適用之相關國際法、國內法令與標準。所有的規定、程序、計畫都必須符合英國與歐盟之法令。法令範圍包括健康與安全、資料保護、電腦濫用管理、智慧財產權、人權等等。

第三節　小結

綜合以上英國政府有關保密資訊與安全認證之法源與規定，我們可以歸納出以下值得我國參考之作法：

壹、 法律定位清楚，同樣的法令可以因時制宜不斷修正前法並持續累積，以彌補前法之不足

就英國而言，英國的法律具有累積性，前法規範不足時，可以透過修正案之方式不斷加以修正，並且累積至規範足夠，加以與安全認證相關的法源定位相當清楚，這使得保密資訊與安全認證的工作有清楚的法源根據，減少執行時可能引發的爭議。

貳、 有專責並且具備公正性的安全認證機構可以隨時針對政府部門、甚或私人企業、組織機關需求執行安全認證工作

以英國國防部的 DVA 爲例，該單位不但負責國防部之安全認證，同時也開放接受各機關之委託、協助民間法人的安全認證工作，此種情況與美國類似，此一趨勢同樣也可節省龐大的行政資源。

參、 安全認證的程序相當齊備

所有的資訊保密與安全認證工作，特別是人員的安全認證方面，英國政府投注相當的人力以及資源從事這方面的工作。這種制度的長久推行使洩密或危害國家安全的機率減到最低，也相對提供了國家安全縝密保障。

第五章 現行日本安全認證制度之探討

嚴格地說，日本沒有獨立的官方軍工企業，而是在政府的大力扶持下，建立以私營企業爲主的軍事工業。在日本，武器裝備的研製生產均由防衛廳通過契約委託私營企業完成，即由防衛廳採購實施部根據武器採購需求，利用價格競爭原則選擇生產企業，按「契約方式」從國內軍工企業採購。

在此種情形下，日本軍事機密的控管與其他國家不同，並非藉由國家安全法或反間諜法，而偏重一般民刑法的適用。甚至由於受著憲法第 9 條之放棄武力與和平條文的限制，日本在理論上是沒有所謂軍事機密的問題，對於洩漏行政或國政上的國家機密也不存在一般的處罰規定，反而是在國家公務員法、地方公務員法以及自衛隊法限制公務員洩漏國家機密的義務，對公務員唆使或幫助其洩漏國家機密者，則可處以刑法上的制裁。

第一節 日本軍事產業的特徵

第二次世界大戰使日本的軍事力量和軍事工業受到沈重打擊，但韓戰爆發爲日本軍事工業的發展提供契機。此後幾十年，日本建立起門類齊全、水平較高、寓軍於民的軍事工業體系。日本的軍工產業體系（日本自稱爲防衛產業）由飛機、艦船、被服、食品等範圍廣泛的各種產業領域構成。日本軍事工業以民營企業爲主，武器裝備的研製生產均由防衛廳通過契約委託私營企業完成。

目前，日本約有 2000 家主要企業生產軍品，軍工從業人員約 7 萬人，約占本國工業從業人員的 0.1%。軍工產業的總產值約占國內工業生產總值的 0.6%左右。有的公司軍品訂貨額已占公司總額一半以上。大型軍事工業公司主要有三菱重工業公司、石川島播磨重工業公司、川崎重工業公司、富士重工業公司、三井造船公司、住友機械公司等。這些公司可生產包括坦克、飛機、艦船、飛彈及通信偵察等電子器材在內的各型武器，且許多領域的技術已達世界領先水準。尤其是在複合材料及微電子領域，日

本軍工企業已遠超過軍工大國美國的前面。波斯灣戰爭及科索沃戰爭中，北約部隊所用的精確制導武器中的核心晶片大都是由日本軍工企業生產的。僅戰術飛彈一項日本自給率已占九成以上。

由於軍需定貨穩定，利潤高達 10—12%，因此日本企業無不熱衷於軍工生產，僅 90 式主戰坦克的製造就涉及到日本全國 1300 多家企業。爲對這些民間企業進行有效組織和管理，日本通過各種手段和形式加強與主要企業連繫。做法之一是每年把由自衛隊退役的一批上校以上高級幹部安排到有關企業擔當要職。訂貨越多的企業，所接納的這些官員就越多；其二是成立民間軍工產業團體，如兵器工業會、經團聯軍工生產委員會等；其三是各大企業均設有專門的軍工生產機構，如日立製作設有「軍事技術推進本部」，住友重工設有「軍事工業綜合室」，日立造船設有「艦艇武器本部」，這些機構專門負責與防衛廳進行連繫和協調。

由於日本的軍品生產是由防衛廳採購實施本部透過契約方式委託民間企業承擔，因此其軍事工業有以下幾個主要特點：

一、 軍品生產高度集中。防衛廳採購實施本部的主要軍品訂貨契約有將近 70%集中在 30 家大企業，而其中前 6 家企業就占軍品訂貨額的 50%左右，其中三菱集團是一權獨秀。排名在 30 以外的軍工企業主要承擔材料與零組件的生產。

二、 軍民相容程度高，軍事工業融於雄厚的民用工業體系中。日本的軍工企業全部爲民間企業，軍品銷售額在企業總銷售額中所占比例很小，一般很少有超過 20%的，大多數都在 5%以下，企業對軍品銷售的依賴性小；而整個軍工行業的產值在工業總產值的比例更低，約只占到 0.5%～0.6%。日本武器裝備的大部分研製任務和全部任務由防衛廳通過契約形式委託民間企業實施。

三、 政府及軍方與軍工企業間的關係密切融洽。政府與軍工企業的主要紐帶有兩個：一個是通商產業省（通產省），一個是防衛廳直屬的技

術研究本部。通產省通過制定暫地措施法實施政府的軍工產業政策，其主導方向是扶植所謂增長性工業（其中包括資訊產業和軟體產業），而其主要著重支援樣機的研究與開發，改進商業系統的生產與製造。技術研究本部的主要任務有兩項：一是進行軍民技術的研究與發展工作，監控軍工企業民用技術和兩用技術的發展，確立哪些民用技術具有軍事應用價值，並建議防衛廳予以採購；二是限制外國公司接觸日本正在開發的技術，監控並防範軍用價值高的兩用技術的外流。軍工界則是通過社團法人機構向政府施加影響和壓力。

第二節　相關法令

如前所述，由於日本憲法第 9 條規定放棄武力與和平條文的限制，理論上是沒有所謂軍事機密的問題，因此對於洩漏行政或國政上的國家機密，也不存在著一般的處罰規定。但是，在國家公務員法、地方公務員法以及自衛隊法上則限制著公務員洩漏國家機密的義務，而且對公務員唆使或幫助其洩漏國家機密者，則可能處以刑法上的制裁。

一、　國家公務員法與地方公務員法

國家公務員法規定，對公務員唆使或幫助其洩漏國家機密者，可能處以刑法上的制裁。不過，「機（秘）密」包括形式機密與實質機密兩類，所謂國家公務員法等所保護的「機（秘）密」究竟所指爲何？一般而言，形式機密是指行政機關以機密所表示，而禁止公佈給一般人知曉的資訊；實質機密是指從內容而言是值得以刑罰所保障的資訊。

在法院的判決上，日本最高法院認爲所謂的「秘密」，「並不只是國家機關將某一事項在形式上指定是秘密而已」，並且應該是「非公開的事項，並在實質上有被認爲是值得保護之秘密的價值。」（徵稅紛爭事件的判決（最二小判昭和 52 年 12 月 19 日刑集 31 卷 7 號 1052 頁））。此一實質機密說，在後述的外務省秘密洩漏事件上也被最高法院所採用。

二、　自衛隊法

現行自衛隊法第 59 條規定自衛隊員保守秘密的義務，規定對違反者處以 1 年以下徒刑或處以 3 萬日元以下的罰款。2003 年 10 月 16 日，日本政府在向國會提交恐怖對策特別措施法案的同時，還提交一份自衛隊法修正法案。自衛隊法修正法案中，採用一度定爲廢案的「國家機密法案」的部分內容。由於此次國會的焦點集中在支持美國的反恐怖行動，因此「防衛機密」問題並未受到太大關注。但是，「防衛機密」涉及範圍廣泛，觸及「洩密」或「教唆」規定而成爲該法案處罰對象者不限於自衛隊員，還包括政治家、國家公務員與防衛機密有關的企業的雇員、新聞記者等。

由於 1980 年的防衛廳間諜事件，自民黨議員乃於 1985 年 6 月遞交「國家機密法案」提案，但當時由於遭到在野黨、學術界、法律界、新聞機構等的強烈反對，所以被定爲廢案。1985 年的提案將「防衛機密」和「外交機密」合爲一體，稱之爲「國家機密」，主張對單純的國家秘密洩漏者判處 10 年以下徒刑，對向國外提供情報的間諜活動者判處死刑或無期徒刑。

此次自衛隊法修正案第 96 條第 2 項中，加入「防衛機密」制度。不過，該條款只以「防衛機密」爲對象，沒有涉及「外交機密」和爲國外提供情報的間諜活動的內容。「防衛機密」制度規定，「防衛機密」是指防衛廳長官認爲「國家防衛有必要保守秘密的事項」，其內容包括從「自衛隊的運用」到「設施的設計」共 10 項，幾乎涉及所有防衛內容。根據「防衛機密」制度，洩密罪將被判處 5 年以下的徒刑，教唆罪將被判處 3 年以下徒刑。

在《反恐特別措施法》的背後，旨在強化防衛秘密安全的《自衛隊法修正案》幾乎沒經過討論。此項法案擴大包括民間人士在內的處罰對象、範圍和刑量，內容上與已被廢棄的提案《國家機密法》（又稱《防止間諜法》）有一定重復，這項新法案將對向外透露軍方消息的自衛隊隊員加倍懲罰，重要的是民間人士也要實行刑罰。擬定這項法案是爲了限制軍事消息流入民間，以免輿論和爭議帶給自衛隊不利影響。同時，法案也對報導軍事新聞進行限制，公務員及政治人物如觸犯該法案將被判徒刑。在新法案下，報導有關軍事消息的記者將被判最長 3 年的監禁。

三、　爲了保護美國對日提供的武器的秘密，制訂有《日美相互防衛援助協定中的秘密保護法。

四、　外交機密法

日本已訂有外交機密法，限制自衛隊或官員將軍事機密泄露到國外，日本政府更依此制定決定秘密內容與種類的「外務省秘密保持規定」。

五、不正競爭防止法

近年來，美國曾連續發生日本研究人員涉嫌竊取基因樣本之案件，並以違反美國經濟間諜法被起訴，引起日本各界深切反省檢討。同時，由於日本企業界與研究機構普遍對於智慧財產管理不夠嚴謹，使重要產業技術大量外流，以致海外仿冒品及盜版品猖獗氾濫，嚴重損害日本產業的經濟利益，並可能因軍事技術外洩而危及日本的國家安全，成爲日本產業發展的一大隱憂。

日本政府對於營業秘密之保護，係以「不正競爭防止法」加以規範。所謂營業秘密，並無具體內容與範圍；大致可分爲技術機密以及商業機密兩種。前者如製造技術、生產方法，或模組設計圖樣等；後者則有如配方、客戶名單以及銷售操作手冊等。一般而言，凡未能取得專利權、著作權或商標權等法律賦予之權利地位，但在商業上或產業上具有經濟性或有用性之技術或資訊，在未公開周知的情況下，以秘密型態加以管理保護者，均得視爲營業秘密。至於侵害營業秘密之「不正競爭行爲」，係指以竊取、詐欺、強制脅迫等不法手段取得營業秘密，或明知（或有重大過失而不知）該訊爲非法取得之營業秘密，仍予以使用或揭露之行爲。舉例而言，如內部員工竊取客戶訂單或銷售業績報告等機密文件，交付競爭企業之產業間諜行爲；或技術人員竊取客戶名單或交易資料，販賣給第三人以獲取不當利益之行爲等，均屬於不正競爭行爲；而競爭企業或第三人進一步利用或揭露該營業秘密之行爲，亦爲不正競爭防止法之規範對象。近來對於營業秘密保護規定有許多重要的變革。

根據經濟產業省委託日本智慧財產協會所做的調查顯示，有二成的企業曾與員工在資訊管理問題上發生糾紛；有六成的企業則認爲不正競爭防止法對營業秘密的保護仍不夠充分；更有約八成企業贊成在附條件情況下增設刑事罰責以加強營業秘密的保護。據此，經濟產業省即進行檢討營業秘密法制規範，並於 2002 年 3 月修訂不正競爭防止法，除加強民事保護措施外，並對於洩漏企業機密以及產業間諜行爲採取刑事罰則。

此外，日本政府亦訂定「企業秘密管理指針」，明確列舉企業秘密管理之具體方法，作爲企業加強營業秘密管理機制之參考準則。由於行政指

針僅係行政指導的明文化，本身不具法律規範作用，故日本政府擬將本指針納入日本工業規格（JIS）認證制度之一環，作爲未來企業制定智財管理制度之規格標準。本指針揭示營業秘密管理之標準，其中將營業秘密之管理分成「最低限管理水準」以及「期待管理水準」兩部分。前者主要是以不正競爭防止法相關判例爲基礎，歸納在法律上受到保護，至少符合機密管理性、經濟有用性以及非公知性等要件，所應具備的「最低限管理水準」。

然而「最低限管理水準」仍可能無法避免紛爭之發生，爲防範紛爭於未然，本指針依據國際營業秘密管理之實務與法制動向，提示完善營業秘密管理之「期待管理水準」，應具備之資訊管理方法與組織架構等。首先，依照機密等級之不同，對於使用及揭露之人或地點範圍加以限定，例如分成「使用人之限制」、「使用與揭露範圍之限制」、「使用或揭露地點之限制」等，對於近用秘密資訊之過程，予以記錄或監視。其次，應進一步對企業內部之使用目的以及揭露對象加以規範，課以管理階層、正職員工、外聘員工、離職員工、交易客戶等不同的守密義務，並應將營業秘密的範圍、使用權限以及揭露範圍等具體事項，明定於工作規則或契約書內。

六、關於禁止不正當存取行爲的法律

日本企業爲了保護用戶資料等機密資訊，也研究開發反駭客保密技術。有的企業採取定期更換口令的方法。日本汽車工業會 30 家成員企業正在建立自己的「假想專用線網（VPN）」，即使用共同的通信順序和密碼，像用專線一樣安全穩定地傳送資訊。日本電氣公司（NEC）不久前開發成功發收雙方共用鑰匙的「密碼共控 A」保密技術。富士通公司成功地計算出關於素數的「模組多項式」，其項數多達 1 萬 3 千項，係數多達 2000 位元，即使使用大型電腦進行解密運算，也需要極長時間。據認爲，它將有助於開發「橢圓曲線密碼」技術。 日本在研究反駭客技術方面可以說已經走在世界各國的前列。日本政府更於 2 月 13 日正式實施《關於禁止不正當存取行爲的法律》，加強對駭客等不正當行爲的處罰。

第三節　結論

有人認爲，波斯灣戰爭是由日本打贏的，因爲美軍在此戰中賴以取勝的電子技術武器，其核心零件—微電子矽片至少有 80%是由日本企業生產。依美國國防部近年的報告顯示，日本是世界第二科技大國，許多尖端技術（如光纖技術、半導體、超導技術、智慧型機器人等領域）均居世界領先地位。雄厚的科技實力爲日本軍事技術和軍事工業的發展提供得天獨厚的條件，再加上近來日本政府不斷加大對軍事工業和國防科技研究開發的財政投入，對軍事科研的經費投入持續保持 10%以上的高增長。日本一家研究機構曾爲文表示，如果日本真正地介入國際軍火市場，可以控制電子戰設備市場的 40%，航空器市場的 25%—35%。在此情形下，日本對於軍事工業實有加強安全認證的必要性。

其實日本關於保護機密的法律已經有許多種。如爲了保護美國對日提供的武器的秘密，制訂有《日美相互防衛援助協定中的秘密保護法》，在《公務員法》和《自衛隊法》中也有保守秘密義務的規定，但動議者們提出的理由是日本沒有限制民間人士和外國人從事諜報活動的法律。日本內閣官房長官、政府發言人中川秀直表示「根據國際法的原則，即便是駐日外交官從事諜報活動，日本也無法進行逮捕和起訴，日本必須在現有的法律範圍內進行取締」。

由於許多意見認爲，如果沒有《防諜法》，日本就可能成爲「間諜的天堂」。於是，2000 年 9 月 12 日，日本聯合執政三黨之一的保守黨幹事長野田毅率領幾名國會議員造訪首相官邸並向森喜朗首相諫言，要求政府著手起草並向國會提議討論制訂《防諜法》。日本關於《防諜法》的議論已有過多個回合。在東西冷戰時期，每每發生間諜事件，國會就醞釀制訂一部限制外國人在日開展情報活動和禁止日本人對外提供情報的法律，然而皆因人權問題而無法成立。

第六章　結論與具體規範措施

在前面章節中已經分別就我國、美國與英國的安全認證制度進行探討。在本章中，將分別就以下各項課題進行總結分析。

壹、 立法之改善

立法之改善顯非可以於短期內見效之工作，惟政府部門仍應主動負起推動立法之責，除更應與立法部門進行溝通，廣納立法部門之意見，同時提升行政、立法部門對於安全認證制度重要性之了解，同時也藉溝通之過程，糾正行政或立法部門對於安全認證制度所懷抱之偏差觀念。簡而言之，在立法方面的工作主要有以下各項：

一、 儘速通過與安全認證有關之重要立法

目前我國在安全認證的法源依據明顯不足，有些重要的法案甚至還停留在草案階段。而從法案的制訂時間看起，最早的法案係一九八〇年的法務部調查局組織條例，至關重要的國家安全法遲至一九八七年才制訂，比美國的一九四七年國家安全法整整晚了四十年。更甚者，在安全維護領域中，國家機密保護法、從事及參與國防安全事務人員安全調查辦法、機密檔案管理辦法等等，都是最基本的重要法源，然而上述法令竟然是到二〇〇〇年後才逐漸制訂。立法不足與嚴重延宕，對國家安全造成的影響不可謂不大。

因此，儘速制訂相關法律，以形成我國在安全維護與認證的完整法律體系乃是當務之急。不過，在急需立法之際，法律的品質仍須特別注意。行政機關在推動相關立法時，不但要進行深入研究，廣納專家意見，以建立詳盡的草案；在進入立法階段時，更須小心避免立法品質受到立法委員的素質與議事效率影響。否則，有缺陷的惡法所造成的傷害比沒有法令更嚴重。

二、 制訂不同位階的法令，提供全面的法源依據，擴大適用範圍、減少爭議

從我國現有相關規定的位階來看，除了少數位階較高的法律，如國家安全法、國家機密保護法外，其餘多屬行政命令、組織條例或施行辦法。法令位階顯然偏低。

爲了擴大法令適用範圍，提供明確的規範以減少爭議，本研究建議應該制訂不同位階的法令與施行細則。高階法律乃係制訂整個政策的大方針與原則，並提供強大的法律效力以爲依據。較低階的法令與組織章程、施行細節則是詳細規範所有可能發生的情形，以清楚明確的條文確保執行時不至於發生爭議，提高執行效率。

三、 擴大法律規範範圍，建立完整的安全維護與認證體系

以我國現有法律所涵蓋的規定事項來看，在規範對象上，明顯偏重於公務人員，缺乏對非公務人員或機關的規範；在規範事項上，則多屬國防、情報層面，無法形成完整的安全認證體系。

我國目前尚須增加法令規範的項目有：除國防人員外，其他公務人員之保密與安全認證、非公務人員（機關）安全認證、設施安全的認證、區分保密資訊的標準，密等的降級與撤銷、安全教育與訓練、定期執行測謊以及查核認證等。此外，在制訂相關法律時，也應注意保障人權、設立救濟制度。

貳、 委託法人機構代爲執行安全認證

依據「涉及國家安全或重大利益公務人員特殊查核辦法」國內政府單位唯一獲有安全認證權責的單位僅法務部調查局，從法理上來看，法務部調查局所負責的業務範圍本來就包括「掌理有關危害國家安全與違反國家利益之調查保防事項」[9]，因此上項辦法之規定等於是讓法務部調查局得以「實至名歸」。

不過就實際業務執行情況而言，法務部調查局除了必須負責維護國家安全與利益之外，尚須處理包括犯罪調查、研究、訓練與科技、以及洗錢

[9] 法務部調查局組織條例，第二條。

防制等各項工作，其工作項目林林總總加起來至少達九項，業務不可謂不繁雜，這是其一。其次國內公務人員人數之龐大，若要貫徹執行安全認證的程序，恐非法務部調查局的編制內人員所能承受，未來如果一併要求法務部調查局針對非公務機關（人員）進行安全調查，恐怕更是雪上加霜。更別說政府部門爲了精簡部門、達到體系瘦身之目的，還一度要求法務部調查局必須裁員。[10]

目前唯一可行之道是必須由政府部門出面，特別針對非公務機關（人員）之安全認證一事，將權力下放給具有公信力的其他民間法人機構。當然這些民間法人機構的篩選必然要具備某些條件，這些條件包括：

一、 必須通過法務部調查局的安全認證，查核事項包括所有安全認證所指稱的各主要項目，至少包括人員、文件、設施、資訊都符合政府部門對一般公務部門－特別是安全部門－的要求，到獲得政府完全授權其執行安全認證工作之前，必須每一季或至少半年需接受定期或不定期查核；

二、 必須與國防、外交、大陸事務、國家安全、科技、經貿等重要政府部門建立一定程度之合作（契約）關係，由這些政府部門提供進行安全認證所必需之教育訓練；

三、 必須在獲得政府部份授權並執行相關安全認證工作至少兩年以上，並經法務部調查局驗證其安全認證之績效與成果，方可獲得政府部門全盤授權，並得以負起針對非公務機關（人員）安全認證之任務。惟仍須接受政府定期或不定期查核，以驗證其執行績效與成果。

事實上就政府授權其他法人單位代理政府執行原應屬政府部門之工作範圍業務並非毫無前例可循，特別是在資訊安全領域中，這些例子更是所在多有，包括像網域名稱（Domain Name）受理註冊的授權、以及所謂的「金鑰認證中心」（Certificate Authority, CA）等等。

[10] 中國時報，「業務量一增裁員令就下」 法務部今向人事局要人」，民國 91 年 6 月 21 日。

以「金鑰認證中心」爲例，最主要是由於網路頻寬技術不斷的發展，網際網路有被廣泛應用在商業活動之趨勢，也使得人類日常生活將離不開網路，包括一般生活中常見的電子郵件、網路購物、網路銀行、網路報稅、網路股票下單等應用都與網路有著密不可分的關係。這些網路交易活動的共通點是－都要避免資料被竄改、資料被洩露曝光、被冒名交易、事後遭否認發送交易、事後遭否認收到交易等情況的發生。而爲解決這些網路安全問題所使用的「非對稱金鑰密碼系統」加密技術，均必須配合一個公正的第三者擔任「金鑰認證中心」，以協助解決網路身份辨識、保障網路資料傳遞與交換安全。其中的主要運用原理是，首先使用者必須透過一定程序申請到所謂的「私密金鑰」（private key），在透過公開的管道取得「公開金鑰」（public key），使用者在進行資訊傳遞的過程中，便由金鑰認證中心擔負起驗證「私密金鑰」與「公開金鑰」之間的相關性，同時驗證「公開金鑰」的正確性－未被竄改或僞造，最後不但達成資料的加密，同時也確保資料的正確傳遞無誤。而爲了達成這兩個主要任務，金鑰認證中心必須訂定安全控管政策（security policy），同時據此執行基本的憑證管理服務，包括將驗證過（certified）的公開金鑰製作成爲電子憑證（certificate）、並處理後續之憑證展期、憑證註銷、憑證公告、憑證儲存等工作。

按照上述說明，政府部門在理論上自然應當擔負起其中最重要的－扮演公正第三者－角色，但是這其中當然一方面因爲網路系統的開放性本較任何其他系統來得大，同時另外一方面也可以說是政府並沒有適當的編制單位或足夠的人力來因應網路上對於安全的無限需求，因此授權予一般民間法人單位去取得這樣的權力，分攤政府權責、並適時在網路安全領域上扮演關鍵角色反而遠比政府一手承接所有業務來得更加有效率，執行上也更能夠顯現成果。不過政府權力的下放，並不意謂金鑰認證中心的地位可以很容易取得，因爲金鑰認證中心所牽涉範圍並不僅止於其技術廣度、複雜度，另外還會牽涉到法律、社會、文化、商業交易習慣、資訊化普及度等層面，唯有照顧到這種種層面，金鑰認證中心才能夠有資格長久存在、並且運作順暢。

將同樣的經驗類推到安全認證領域中，其實我們同樣也可以循著上述

金鑰認證中心的軌跡來看出一些未來可行的解決方案，那就是讓政府對於民間其他法人單位設定一定的條件限制之後，並且充分授權，使得法務部調查局得以暫時解除在非公務機關（人員）這方面所需擔負之工作重擔，而僅全力集中在對公務機關（人員）的安全認證工作，而讓其他法人單位得以在非公務機關（人員）的安全認證上承接起責任。

不過我們還是必須指出，任何政府部門的授權行爲其背後還是必須要有強固的法律基礎做支撐。換言之，政府部門在進行此項授權的工作之前，還是必須尋求立法部門的配合，制定相關的法律規範以及配套措施，以免使得這項立意良好的措施反而演變成行政部門與某些民間法人單位之間產生私相授受的情況出現。在此同時，因爲委請其他法人單位進行安全認證的過程中還是可能會面臨契約關係因故終止、或該單位執行績效不彰，再或者該法人單位在執行安全認證過程中除了公信力之外還必須要有部份強制力的配合等等，這些情況都需要法律進行明確的律定與規範，以免日後產生更大的問題。

參、　「權」、「責」之認定與劃分

雖然本研究結果顯示，我國安全認證制度的建立尚不夠完整與健全，政府部門應該在此一方面負起絕大多數的責任，但這並不意味政府部門應該必須承擔所有的責任，在政府部門與非公務機關（人員）的「權」與「責」之間還是必須做一個適當的界定與劃分，這將有助於安全制度的有效施行。

一、　正確的安全認證程序認知：政府有權、非公務機關（人員）有責

安全認證制度的建立固然有其必要性與迫切性，但這不意味政府部門必須始終扮演主動與積極的角色，特別是針對非公務機關（人員）的查核更是如此。更進一步分析，非公務機關（人員）如果與公務機關（人員）身份有重疊的情況－比方說擔任政務官、國會議員或者國會助理等人員－政府部門當然有權力主動介入進行安全認證。但是對於不具備這些條件的非公務機關（人員），政府部門則可以扮演被動的角色。換言之，政府不

必主動介入非公務機關（人員）的查核，反過來，政府部門與非公務機關（人員）應該建立起正確的安全認證權責認知，由非公務機關（人員）主動依據政府所訂定的安全認證標準程序，備妥安全認證所規定之必要文件、以及相關準備（例如內部機密文件之分類、異地儲存重要資料與設備等），然後主動向政府部門提出申請安全認證，在通過查核之後，便可獲得正式參與未來與國家機密相關之研究等事務之資格。

以美國爲例，在美國的安全認證制度便是建立在政府有權（實施安全認證）、機關（或人員）有責（主動要求進行安全認證）的模式基礎之上。舉例來說，如果有非公務機構或人員欲承攬美國國防部陸軍總部所資助之安全研究計畫、並且可能從中與聞國家機密檔案、文件或設施時，按照規定，該機關（或人員）就必須主動事先將安全認證所規定的相關表格（如 SF86 表格）填妥，並且將這些文件送交陸軍總部，陸軍總部再轉送至 DSS，並由 DSS 進行一連串的安全認證程序，最後 DSS 再將查核的結果回報給陸軍總部，由陸軍總部來斷定受查核之機關或人員是否具備接觸國家機密的基本資格，決定是否與該機構或人員進行簽約及合作。

二、 角色與權責的後續轉化

就上面所提及的安全認證主動與被動角色來看，政府部門雖然在安全認證的啓始點上扮演被動的角色，但是當受查核的單位或人員已經依據標準作業程序提出申請並通過查核之後，政府部門就必須轉化其原先之被動角色爲主動，針對原先受查核之機關（人員）進行定期及不定期之再查核，受查核機關則轉化其原先主動的角色爲被動，必須接受權責機關的查核，以確保其接觸國家機密之資格能維持。之所以會產生這樣的角色與權責之轉化，主要在於受查核者，不論其爲機關或人員，將隨著環境以及所接觸的人、事、物而可能導致某些本質上或其他層面（比方說內部的保密防護措施）產生變化，爲了確保國家機密不致因爲這些變化而暴露於高風險之下，負責安全認證的機關乃必須轉被動爲主動。這也是爲什麼在本研究中會談到，「安全認證的結果只有在查核的當時是正確的」這樣一種情況。

肆、　政策執行建議

除了立法的補充外，施行細節與法令的貫徹執行也是建立完善安全認證體系不可或缺的要素。本研究的建議不僅針對非公務人員與機關，同時也希望公務機關能夠加以採納，以建立一個完整有效率的安全認證體系。

一、　清楚劃分安全認證體系的層級

我國現有的法規不足，無法明確建構安全認證體系的層級。以美國的安全認證體系爲例，其指導、執行、監督、協助等各層級之單位都劃分清楚，各司其職；彼此相輔相成，不會有權責不清或相疊，導致扞格之處。因此建議仿效美國的作法，建立一套清楚的層級，提高安全認證工作的品質與效率。

二、　設計縝密而專業的認證方式

由於美國和英國實施安全認證的時間比我國早，因此累積了許多寶貴的經驗。我國可以參考各國在認證方式上的設計，延聘包括國防、安全、核能、通訊、資訊、電腦、心理、醫療等各方面的資深人員或專家，針對所有認證的種類（人員、設施、通訊與資訊）設計出完善的認證方式，對國家安全會有極大的助益。

三、　落實安全教育與訓練，培養專業認證人員

有了良好的制度，還需要有優良的人力來確實執行，才能完全發揮安全認證的意義。在訪談過程中，我們發現我國的安全調查、執行、教育訓練經常流於形式，或因執行人員的良莠不齊而影響認證品質。因此建議嚴格篩選執行人員，在品德與能力上都應設定高標準；設計一套包括：執行人員的專業知識、調查技巧的訓練課程，培養可信賴的專業調查認證人員；同時也要持續進行定期與不定期的考核及再教育訓練。

四、　建立全國通用的安全認證標準作業程序（SOP），加強執行機關間橫向聯繫與資料庫的連線

如果第二、第三項建議都已達成，則可進一步建立全國通用的標準作業程序。因爲有了穩定而優良的認證方式與執行人員，就可以確保無論是

哪一個機關進行的安全認證，其品質都是一致的。各機關間得以承認彼此認證結果，有關的資料也可相互移交。此舉不僅可減少重複的認證工作，避免行政資源的浪費，更是便民的措施。

五、 善用科技，節省時間與經費

由於網路科技的發達，在資訊安全無虞的前提下，美國的安全認證、教育課程都已逐漸朝無紙化、網路化發展。利用網路就可以查詢相關的資訊、申請安全認證、填寫並傳送安全認證的問卷表格，甚至連訓練教材都可以透過特殊軟體從網路下載。我國的資訊產業發達，擁有眾多資訊人才，網路也相當普及，因此不妨善用這項資源，透過安全的網路設備，提高工作效率，節省大筆公帑。

六、 全面清查現有之資料、軟硬體設備，確保安全

由於我國沒有針對設施安全的詳細規定，許多應嚴加保護的文件、資料、設備，還有應該管制進出的區域，缺乏應有的安全措施，或是因設備簡陋老舊而影響安全，公務機關的情況甚至較民間高科技企業來得嚴重。因此建議仿照英美兩國，針對資訊、文件的使用，儲存的容器、空間等項目，設立一套統一的標準或規格，以便各機關遵循辦理。

七、 矯正錯誤觀念，提升政府部門及一般人對於安全認證重視與了解

最後，也是最重要，最基本的一項，就是當前安全部門內部認知與心態的矯正。錯誤觀念之一是台灣過去受到威權統治的影響，對白色恐怖的記憶猶新，因此許多人對於安全調查的認知與心態不盡正確、甚或嚴重扭曲，認為這可能會對個人（機關）造成迫害，進而抗拒接受安全認證調查，或不願提供詳盡而真實的資料。其二，在實際進行機密等級分類時，由於保守觀念使然，承辦人員在將文件做機密等級分類時，往往將實質上並不具備機密性質之文件、或者甚至是公開可以從媒體、報章雜誌、網路上取得之資料一律列為「機密」以上等級文件，對於機密文件之保護不但沒有助益，反而造成日後在進行安全事務相關研究之困擾。

此外，由於過去安全認證並沒有受到應有之重視，相關人員並不瞭解除了人員安全認證必須加以落實之外，尚須輔之以文件、設施以及資訊系統安全認證的整體搭配，導致執行與查核工作無法達到真正效用。這些都是亟待改進的問題。爲了達到本研究之目的－促成非公務機關及人員參與國防安全事務相關之研究－政府部門的積極介入與重視安全認證乃是非常重要、也是不可或缺的關鍵，同時也應該參考西方國家經驗，宣導並以公正態度執行安全認證制度，扭正這樣的錯誤觀念。

附　錄

一、SF86 美國國家安全職務問卷

美國國家安全職務問卷

請台端確實遵循各項指示，以免台端之表格無法進行處理。並請務必簽署第九頁之聲明書與第十頁之資料揭露授權書及註明日期。若台端有任何疑問，請去電提供表格之單位查詢。

本表格之目的

美國政府進行各類背景調查及複查之目的在於確認軍職人員、國家安全職位之申請人或現職人員，不問其爲政府之雇員或承包商、被授權人、證照持有人或受機關補助之人，均已通過必要之安全認證。我們主要依據取自本表之資料作爲調查台端是否得以接觸機密資料或特殊核子資訊或資料之依據。當事人唯有決定應徵需要通過安全認證之職爲時，才需填寫本表格。

台端提供我們所要求之資料均係出於自願，唯若台端未能提供我們要求完整資料，則我們或將無法完成對台端之調查，或不克及時完成該項調查。此等情形恐將影響台端之職務安置或安全認證之前景。

要求台端提供本表格所載資料之法源

視調查目的之不同而定，美國政府係依行政命令第 10450 號、第 10865 號、第 12333 號、第 12356 號；美國法典第五章第 3301 及 9101 條、第四十二章第 2165 及 2201 條、第五章第 781 至 887 條；及聯邦法規彙編第五章第 5-732、736 編之授權而要求本表格之資料。

因他人可能與台端有雷同之姓名或出生年月日，故我們要求台端之社會安全號碼以確保記錄之無誤。行政命令第 9397 號亦要求聯邦機關使用該號碼作爲各機關查驗個人身份之用。

調查之程序

國家安全職務之背景調查係爲取得相關資料，俾便瞭解台端是否可靠、可信、品行端正及忠於美國。台端於本表格所提供之資料均將經由調查予以確認。若有解決爭議之必要時，調查所涵蓋之期間可能超過本表格所含涵蓋之時間。我們將與台端目前之雇主聯繫作爲調查之一部分，即便台端先前於申請表或其他表格上表示相反之意思，亦同。

除本表格所載之問題外，我們亦將查詢特定人員對於安全規定之遵守狀況、誠實及正直之行爲、易遭利用或脅迫之弱點、詐騙行爲、欺瞞行爲，以及可能顯示該員不可靠、無信用或不忠誠之任何其他行爲、活動或交往情形。

對台端之面談

若干調查將包括與台端進行面談，作爲調查程序之正常部分之一。此種方式提供台端更新澄清與更詳盡解釋台端之表格中所述資料之機會，而往往得以使對台端之調查於更短之時間內完成。一旦我們與台端聯絡後，則盡快進行面談是相當緊要的。延後面談之時間對我們處理台端之調查造成延宕，而拒絕面談則可能導致對台端所爲調查遭延宕所取消之結果。

台端於前往接受面談時，將會被要求攜帶附相片之身分證明文件，例如有效之州政府核發之駕駛執照。此外，亦有可能要求台端攜帶其他文件以確認台端之身分。此類文件包括：任何合法姓名變更之記錄文件、社會安全卡及/或出生證明書等。

我們亦可能要求台端攜帶與台端對本表格所示問題之回答資料或其他需特別留意之事項有關文書。此類事項包括：外僑登記、逾期未付之貸款或欠稅、破產、法院判決、出質情形或其他財務上之負擔、涉及子女監護或扶養之協議、贍養費或財產上之和解內容、遭逮捕、定罪、緩刑及/或假釋之情形。

本表格之結構

本表格分爲兩部份。第一部份請交待背景資料，包括台端以往及目前之住居地、求學經過與工作經歷。第二部份則詢問台端之活動，例如被雇主辭退之事例、犯罪紀錄、服用禁藥及酗酒之情形。

於回答本表格之所有問題時，台端須切記由台端針對問題所提供之答案將與調查所獲致之資料一併加以考慮，俾達成妥善之決定。

填具本表格之說明

一、 請台端遵照分發表格人員之指示與其所提供之任何補充說明資料填寫本表。請台端清點需要遞交之表格份數，並以黑色墨水筆在遞交之表格正本及每份副本上簽署並註明日期。台端應保留一份完成後之表格副本作爲記錄。

二、 請以黑色繕打或正楷清楚地書寫台端之答案（倘台端填寫之表格，字跡難以辨識，我們將無法受理）。我們亦可能要求台端以經核可之電子格式提供表格。

三、 台端需回答本表格上之所有問題。若無回答之必要或該問題不適用，請於表格上註明（例如，填入「無」或「不是用」）。若台端發現無法確定某日期時，請盡量填入約略之日期，並以填入「約計」或「約略」之方式註明此情形。

四、 若台端於簽署本表格後有變更其內容之情形，需由台端加註姓名字首縮寫及日期。於若干有限之情況下，機關得依台端之意思修改表格。

五、 台端於填寫表格時需利用下欄中所列之各州代碼（縮寫）。城市或外國之名稱則請勿縮寫。

六、 爲加速對台端之調查，請填寫五碼之郵遞區號。提供本表格之單位會協助台端填寫郵遞區號。

七、 所有電話號碼均需包括區域號碼在內。

八、 本表格中所填入之日期均須以月/日/年或月/年之方式表示。請使用阿拉伯數字 1-12 表示各月份。例如，西元 1978 年 6 月 8 日，應以 6/8/78 加以表示。

九、 凡地址欄出現「城市（國家）」時，若該地址位於美國境外，則請於該欄位內亦填入國家名稱。

十、 若台端需要額外之填寫空間列出台端之居所或受雇/自雇/失業或就學記錄，則台端另需填具一份增補表格，及標準表格第 86A 號。若台端需要額外之填寫空間回答其他事項，則請使用空白紙張。台端所使用之每頁空白紙張，均須於頁首簽註台端之姓名及社會安全號碼。

台端資格之最終決定

對於台端是否有接觸機密資訊之資格，係由要求對台端進行調查之聯邦機關做出最終之決定。於前述機關做出最終決定前，可能會給予台端親自解釋、辯駁或澄清任何資料之機會。

提供不實或虛僞陳述之處罰

美國聯邦法典（第 18 章第 1001 條）規定，故意對重大事實爲虛僞之陳述或爲隱匿之行爲，係屬重罪，得處一萬美元以下之罰金，或科或併科五年以下之有期徒刑。此外，聯邦機關對於有重大變造或故意假造本表格之人員，通常會予以解雇、不予通過安全認證獲取消其資格；同時，此種情形將列入我們之永久記錄，作爲爾後職務安置之參考。基於台端被列入考量之工作具有敏感性，於認定台端是否通過安全認證時，台端之可信賴度乃至爲重要之考慮因素。

若台端能誠實並完整地回答全部問題，則台端將有較佳之機會獲得工作或通過安全認證。台端將有恰當之時機就台端於本表格中所提供之任何資料加以說明，並使台端之解釋內容載入記錄。

資料之揭露

台端所提供之資料係用以調查台端是否識適任國家安全職務；我們將保護該等資料不受未經授權之使用。背景調查資料之蒐集、維護與揭露係由隱私法所規範。請求調查之機關及進行調查之機關業已於聯邦政府公報中公告台端之資料將保存之記錄系統。台端得自分發表格人員取得有關公

告之副本。本表格中之資料及我們於調查中所蒐集之資料，得依隱私法（美國法典第五章第 552a 條第(b)項）之許可，不經台端同意而揭露與以下單位：

隱私法上之經常性使用	
1. 司法部，於(a)機關或其所屬任何單位；或(b)任何機關雇員以其公職之身分；或(c) 任何機關雇員以其個人之身分；(d)美國政府，爲訴訟當事人或對於訴訟結果有利害關係，且經慎重審查後，機關認定該等記錄對於訴訟係相關而必要者，故而機關認爲司法部使用該等記錄之目的與機關當初蒐集該記錄之目的相符時。 2. 程序進行中之法院或審判機關，於(a)機關或其所屬任何單位；或(b)任何機關雇員以其公職之身分；或(c) 任何機關雇員以其個人之身分，但司法部同意爲其代表；(d)美國政府，爲訴訟當事人或對於訴訟結果有利害關係，且經慎重審查後，機關認定該等記錄對於訴訟係相關而必要者，故而機關認爲司法部使用該等記錄之目的與機關當初蒐集該記錄之目的相符時。 3. 除第 24 題所示以外，於記錄之表面內容或與其他記錄內容結合後，顯是有違反法律或可能觸法之情形時，不問該等法律之性質係民事、刑事或行政，亦不論其法源係普通法、特別法、規章、規則或據其所發出之命令，得將相關記錄揭露與負責執行、調查或追訴該等違法行爲或有執行或實施該等法規、規則、規章或命令職責之適當聯邦政	5. 聯邦政府、州政府、地方政府、外國政府、部族政府或其他政府權責機關，告知其本資料記錄系統含有與續用雇員或保有安全認證、合約、證照、補助或其他福利有關之資料。其他機關或授權組織得決定是否取得個人之同意而請求全部之記錄內容。除非資料被認爲具充分可靠性而可支持將其轉送與機關內之另一單位或另一聯邦政府機關採取刑事、民事、行政、人事或管理行動，否則不得揭露資料。 6. 承包商、受補助之人、專家、顧問或義工，於有必要時履行與本記錄有關之功能或服務時。前述之記錄收受人應遵守 1974 年之隱私法及其修正內容。 7. 媒體或一般公眾，關於事實部分資料，而其揭露符合公眾利益且不構成對個人隱私之不當侵犯。 8. 聯邦、州或地方政府機關或其他適當之機構或個人，或經由既定之聯絡管道與外國政府，俾使情報機關執行其基於 1947 年之國家安全法及其修正內容、1949 年之中央情報局法及其修正內容，行政命令第 12333 號或其替代命令、相關之國家安全指令，獲經司法部長核准而依前述法規命令或指令發佈之機密執行程序下之職責。

府、外國政府、州政府、地方政府、部族政府或其他政府權責機關。 4. 於調查過程中向任何消息提供者索取資料時，就關於雇員之雇用或續用或其他人事行爲，或安全認證、合約、補助、證照、或其他福利之授與或保留等事項，以查明特定人員之身分、將調查之性質及目的告知該消息提供者並查詢所需特定資料類別之必要範圍爲限。	9. 任何國會議員或國會幕僚人員，以回應國會單位就保有該紀錄之對象所爲之書面請求進行之查詢。 10. 國家檔案暨記錄管理局，以進行美國法典第 44 章第 2904 及 2906 條所規定之檔案記錄管理檢查。 11. 聯邦管理暨預算局，就審查私人補助立法之必要事項。

公眾負擔訊息
本資料蒐集對公眾造成之負擔估計每次回應所需時間平均爲 90 分鐘，包括閱讀各項指示之時間、 搜尋現有資料來源之時間、蒐集與補正所需資料之時間，以及填妥並複閱資料之時間。倘對於前述公眾負擔之估計或本資料蒐集之任何方面有意見，包括有減輕該負擔之建議時，請將意見寄至華盛頓哥倫比亞特區(郵區 20415)西北區 E 街 1900 號 CHP-500 室，美國聯邦人事管理局之報告與表格執行官收。切勿將台端填妥之表格寄至前述地址。

SF86

國家安全職務問卷調查表

第一部份		僅供調查機關使用				代碼		案號				
僅供機關使用（請利用調查機關提供之說明填寫第 A 至 P 項）												
A 調查類別		B 其他範圍		C 機密等級		D 存取		E 行動代號		F 行動日期	月	日	年
G 地理位置			H 職務代碼			I 職銜						
J SON		K 官方人事檔案所在地		None NPRC At SON		其他地址：			郵遞區號			
L SOI		M 安全檔案所在		None at SOI NPI		其他地址：			郵遞區號			
N OPAC-ALC 編號				O 會計資料及/ 或機關案號								
P 申請人	姓名及職銜		簽署		電話號碼 ( )		日期					
填寫本表格之人員應自下列問題開始回答												
1. 全名（若台端姓名使用縮寫字頭，請加註(IO)，若台端姓名附有「小」、「大」、「二世」 若台端無中間名，請加註（NMN）等，請在中間名欄位後加註									2. 出生日期			
姓：	名：		中間名：		小/二世等等		月	日	年			
3. 出生地-州名請用二字代碼					4. 社會安全號碼							
城市	郡	州名：		國名（美國以外國家）								
5. 從經使用過之其他名字 請台端將曾經使用過之其他名字及使用該名之期間填寫於下欄。（例如：娘家姓、前夫姓、本名、別名或綽號等）。請於娘家姓前加註(nee)。												
姓名 #1	自 月/年至月/年至			姓名 #3	自 月/年至月/年至							
姓名 #2	自 月/年至月/年至			姓名 #4	自 月/年至月/年至							
6. 其他個人資料	身高：（呎吋）	體重：（磅）		髮色：	眼睛顏色：		性別：□女□男					
7. 電話號碼	公：（含區碼及分機） □日□夜（）			宅：（含區碼及分機） □日□夜（）								

8. 國籍(a)請參考右欄說明並於□內勾選適合台端之項目，依照其指示作答		我是美國或美國領地/屬地出生之公民（請回答 b 和 d 項）	(b)娘家姓名
		我是國外出生之美國公民（請回答 b 和 c 項）	
		我不是美國公民（請回答 b 和 e 項）	

(c)美國籍：若台端係美國公民，但並非在美國出生，請提供下欄資料至少一項，以資證明。

歸化證明書（在何處歸化）？

法院：	城市：	州代碼：	證照號碼：	發證年月日：

國務院表格第 204 號- 國外出生之美國公民申報書

請填寫申報日期，如有必要，並請說明。	申報年月日：	說明：

美國護照：

現行護照抑或過期護照。	護照號碼：	發照年月日：
(d)雙重國籍：若台端目前（或過去）擁有美國及另一國之雙重國籍，請將該國名填寫於右欄。		國名：

(e)外籍人士：若台端係外籍人士，請填寫下列資料：

台端入境美國地點：	城市：	州代碼：	入境日期：	外籍人士登記證號碼：	國籍：

9. 住址：

請自現址(#1)開始，將過去七年之詳細住址由近而遠逐項填寫於下欄。台端須將所有時期之住址均列出，並請務必列出實際居住之地址：亦即，勿使用郵政信箱做爲地址，莫使用永久地址作爲就學期間之地址等。另請務必盡可能列出詳細之地址：例如，勿僅填寫台端服役之基地或船艦，而請一併列出營區編號或駐紮港口。台端得省略派駐時間少於 90 日之臨時性軍事任務地點（此際應填入永久住址），如若居住於海外，則應使用 APO/FPO 地址。

關於過去五年之住址方面，請列出一名證明台端居住過當地之人士，最好該名證明人目前仍居住在當地（切莫列出全然與過去五年期間無關之證明人，亦請勿以台端之配偶、前配偶或其他親戚作爲證明人）。又關於過去五年之住址方面，若列舉之地址係「郵件候領處」、鄉間郵路或星號郵路，或難以確認之地點，請將該地址之方向與位置圖示附於附頁。

#1 現址： 起迄年月	街道地址：　　號#		城市 （國家）	州名	郵遞區號
證明人姓名：	街道地址：　　號#	城市 （國家）	州名	郵遞區號	電話號碼：(　)
#2 住址： 起迄年月	街道地址：　　號#		城市 （國家）	州名	郵遞區號

證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )
#3 住址： 起迄年月	街道地址： 號#		城市（國家）	州名	郵遞區號
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )
#4 住址： 起迄年月	街道地址： 號#		城市（國家）	州名	郵遞區號
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )
#5 住址： 起迄年月	街道地址： 號#		城市（國家）	州名	郵遞區號
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )

10. 學歷：

請將過去七年高中以上學歷由近(#1)而遠逐項填寫於下欄。請請列出專科或大學學位及其授與之日期。若台端離開最後一所就讀之學校已超過七年以上，請列出高中以上之最近學歷，而不問其就讀之時間爲何：

關於下欄之「代碼」，使用說明如後：

1- 高級中學 2-專科/大學/軍事院校 3-職業/技術/商業學校

關於台端過去三年之學歷，請列舉一名證明台端就讀該校之人士（例如老師或同學等）。切莫列出全然與過去三年期間無關之證明人。關於函授學校及推廣教育課程，請填寫其紀錄保存之地址。

#1 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )
#2 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )
#3 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：( )

翻閱次頁前，請填寫台端之社會安全號碼 ---→

11. 請台端自現職(#1)開始，填寫過去七年之工作經歷。台端應詳列所有之全職工作、兼職工作、軍職、超過九十日之臨時軍事任務地點、自營業務、其他有給工作、以及全部失業時間。全部七年之期間均須無間斷加以敘明，但無庸填寫台端十六歲以前之受雇狀況。例外：請列出一切聯邦政府之文職工作經歷，而不問其是否發生於過去七年之期間內。

代碼：請使用下列「代碼」表明工作類別：
1-現役軍人　2-國民兵/後備軍人　3-美國公共衛生服務團　4-其他聯邦員工　5-州政府（非聯邦政府）員工　6-自營業務（填寫業務名稱及證明人姓名）　7- 失業
8- 聯邦合約承攬人（請列出承攬人，而非聯邦機關名稱）　9-其他

雇主/證明人姓名：請於本欄中填寫台端雇主之名稱或台端自營業務或失業之證明人姓名。若台端填入軍職時，請填入任職地點或駐紮港口及軍種。台端應使用不同欄位以反映軍事任職地點或駐紮港口之變動。

同一職務之早期經歷：若台端有爲同一雇主於同一地點在不同期間工作之情形，請填寫此欄位。於第一個編號之欄位填入最近之受雇經歷後，請於其後之欄位填寫在同一地點之早期經歷。例如，台端若三度任職於科羅拉多州丹佛市之 XY 配管工程公司，台端應將最近任職日期及相關資料填入第一欄，並將先前兩次任職之日期、職銜及主管依次填入下面適當之欄位。

#1 現職 起迄年月	代碼	雇主姓名/證明人/軍職地點		職銜/階級	
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷（第一欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#2 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷		起迄年月	職銜	主管	

（第二欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#3 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷（第三欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#4 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷（第四欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#5 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷（第五欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#6 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（ ）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（ ）

主管姓名及街道地址（與工作地點不同者）	城市（國家）	州名	郵遞區號	電話號碼（ ）
同一職務之早期經歷（第六欄）	起迄年月	職銜	主管	
	起迄年月	職銜	主管	
	起迄年月	職銜	主管	

12. 最瞭解台端之人士

列舉三位住在美國且最瞭解台端之人士。該等人士應爲台端之好友、同儕、同事、大學室友等，且其綜合認識台端之時間應盡可能涵蓋過去七年。請勿列舉台端之配偶、前配偶或其他親戚，並盡量避免列舉出現於本表格其他欄位之人士。

#1 姓名	認識日期 起迄年月	電話號碼 □日□夜（ ）		
住家或工作地址		城市（國家）	州名	郵遞區號
#2 姓名	認識日期 起迄年月	電話號碼 □日□夜（ ）		
住家或工作地址		城市（國家）	州名	郵遞區號
#3 姓名	認識日期 起迄年月	電話號碼 □日□夜（ ）		
住家或工作地址		城市（國家）	州名	郵遞區號

13. 配偶

請勾選以下空格以表示台端之婚姻狀況，並於(a)項及/或(b)項提供關於台端配偶之資料。

□1- 從未結婚　□3- 分居　□5- 離婚
□2- 已婚　□4- 合法分居　□6- 鰥寡

(a)配偶　請填寫下列資料。

全名	出生日期	出生地（若非美國境內，請同時註明國家）	社會安全號碼
其他姓名（娘家姓名、）曾使用過之夫姓等，及使用該名之時間		國籍	
結婚日期	結婚地點（若非美國，請同時註明國家）		州名
分居日期	如係合法分居，登記地點爲何？城市（國家）		州名
配偶地址（與台端地址不同時填寫；）街、市及美國以外之國家		州名	郵遞區號

(b)前配偶　請填寫下列資料，如有需要，請續空白頁。

全名	出生日期	出生地（若非美國境內，請同時註明國家）	州名
國籍	結婚日期	結婚地點（若非美國，請同時註明國家）	州名

請勾選後填寫日期 □離婚 □鰥寡	月/日/年	如已離婚，登記地點爲何？	州名
前配偶地址（街、市及美國以外之國家）	州名	郵遞區號	電話號碼 （）

14. 親戚及夥伴關係

請將台端每位存或歿之親戚全名、正確之稱謂代碼、及其他相關資料填入下欄：

1-母(1) 2-父(2) 3-繼母 4-繼父 5-養父母 6-（養）子女

7-配偶前婚子女 8-兄弟 9-姊妹 10-繼父（母）之子 11-繼父（母）之女

12-異父（母）兄弟 13-異父（母）姊妹 14-岳父 15-岳母 16-監護人

17-其他親戚* 18-伙伴 19-目前同居之成年人

*代碼 17（其他親戚）- 僅填入不包含於 1-16 之外國親戚，且與台端或台端之配偶於情感上或義務上有密切持續關係者。代碼 18（夥伴）- 僅填入台端或台端之配偶於情感上或義務上有密切持續關係者。

全名（若身故者，請勾選）左邊之空格		代碼	出生年月日	出生國	國籍	在世親戚目前街址及城市（國家）	州名
		1					
		2					

15. 親戚及夥伴之國籍

若台端之母親、父親、姊妹、兄弟、子女、配偶或與台端間有類似配偶之關係者爲非美國出生之美國公民或在美居留之外國人，請於第一列填入該員與台端之關係（配偶、類似配偶、母親等）及該員之姓名與出生年月日（此項資料係用以詳細比對第 13 項及第 14 項之資料）。請於第二列填入該員之歸化證明或外籍人士登記號碼，並使用下列文件代碼表示其國籍之證明。另請填入其他適當之資料。

1- 歸化證明書：請填入發證日期及歸化地點（法院、城市及州名）

2- 國籍證明書：請填入發證日期及發證地點（城市及州名）

3- 外籍人士登記證：請填入該員入境美國之日期及地點（城市及州名）

4- 其他：請於「其他資料」欄填寫說明。

#1 關係	姓名		出生年月日
證明書/登記證號碼	文件代碼	其他資料	
#2 關係	姓名		出生年月日
證明書/登記證號碼	文件代碼	其他資料	

16. 軍中經歷	是	否
(a)是否曾在美國軍中服務？		
(b)是否曾在美國商船服務？		

請將台端以往在軍中服務之全部經歷填入下列欄位，包括後備軍人、國民兵及美國商船。請從最近之經歷(#1)開始填寫。若服務有中斷之情形，請列出各個時期。
代碼：請於下列代碼中選擇一項表示台端服務之軍種：
1- 空軍 2-陸軍 3-海軍 4-海軍陸戰隊 5-海岸防衛隊 6-商船 7-國民兵
O/E：請勾選代表軍官之「O」欄或代表士兵之「E」欄。
身份：請在台端服役期間之適當欄位內打「X」以表示身份。若係國民兵，則請勿打X，使用州代碼表示。
國家：若台端所服務之對象非美軍，請填入台端所服務之國家名稱。

起迄年月	代碼	兵籍/證照號碼	O	E	身份				國家
					現役軍人	現役預備隊	非現役預備隊	退役	

17. 國外經歷	是	否
(a)是否有在國外置產、經營事業或營利所？		
(b)目前或曾經受雇於外國政府、公司或機關或擔任其顧問？		
(c)除因美國官方業務外，是否曾於美國境內或境外與外國政府、外國政府機構（大使館或領事館）或其代表聯繫？（請勿列入例行性之簽證申請及出入境時之聯繫）		
(d)過去七年是否曾經使用外國政府核發之有效護照？		

若台端就(a)、(b)、(c)或(d)項回答「是」，請在以下空白處加以說明：填入日期、相關之公司及/或政府、及台端涉入情形之說明。

起迄年月	公司及/或政府	說明
起迄年月	公司及/或政府	說明

18. 曾經到過哪些國家

除依據政府命令所爲之國外行程外，請列舉過去七年台端曾到過的國家，從最近者(#1)開始。（以受扶養人或承包商之身分所爲之旅行亦需列入）

- 請使用下列代碼表示台端旅行之目的：1-公務　2-娛樂　3-求學　4-其他
- 請填入至加拿大或墨西哥之短期行程。若台端居住於鄰近邊界地區，並曾數度至鄰國進行短期（一日以內）旅行，則無庸列舉每次之行程，但須填入期間、代碼、國家及註記（「多次短程」）。
- 請勿將第 9、10 及 11 項提過之國家列入。

#1 起迄年月	代碼	國家	#3 起迄年月	代碼	國家
#2 起迄年月	代碼	國家	#4 起迄年月	代碼	國家
本表格第一部份到此結束。若台端爲作答第一部份而使用到第 9 頁、續頁或空白頁，請將上述問題之題號填入右欄空白中。					

標準表格第 86 號（EG）
1995 年 9 月修訂
號
美國聯邦人事管理局
聯邦法令彙編第五章
第 731-732 及 736 條

表格核准單位及文號：
聯邦管理暨預算局第 3206-0007

NSN7540-00-634-4036
86-111

國家安全職務問卷調查表

第二部份	僅供官方使用		
19. 軍中紀錄 台端是否曾自軍中不光榮退伍？若「是」，請於下列欄位列出退伍日期及退伍類別		是	否
月/年	退伍類別		
20. 徵兵紀錄 (a)台端是否係 1959 年 12 月 31 日以後出生之男性？若「否」，請逕答第 21 題，若「是」，請回答(b)項		是	否
(b)台端是否在徵兵期間服役？若「是」，請填寫兵籍號碼。若「否」，請說明合法免徵之理由。			
兵籍號碼	免徵之合法理由		
21. 醫療紀錄 過去七年中，台端是否曾向心理醫療專業人員（精神科醫師、心理醫師、諮詢師等）求診，或向其他醫療專業人員因心理狀況之問題而求診？		是	否

若台端之答案爲「是」，請於下欄中填寫治療日期及治療師或醫師之姓名與地址，但求診之內容僅涉及婚姻、家庭或節哀諮詢，而以台端之暴力行爲無關時，不在此限。					
起迄年月	治療師或醫師之姓名/地址			州代碼	郵遞區號
22. 離職紀錄 台端過去七年是否發生下列情事？若「是」，請自最近發生者開始向前追溯，提供遭解雇、辭職或離職之日期，及其他相關資料。				是	否
請選擇下列代碼並敘明停職理由： 1-被解雇　2-被告知遭解雇後辭職　3-因被指控行爲不當經雙方協議離職　4-因被指控績效不彰經雙方協議離職　5-因情勢不利之其他理由離職					
起迄年月	代碼	敘明理由	雇主姓名及地址（若非美國境內，請同時註明城市/國家）	州代碼	郵遞區號
23. 違警紀錄 請於本項中填入台端之相關資料，而不問其資料是否已「封存」或因其他原因自法庭紀錄中消去。但係基於法院依美國法典第 21 章第 844 條及第 18 章第 3607 條之授權而就聯邦禁藥法中之若干罪名所核發之除罪令者，不在此限。				是	否
(a)台端是否曾經被控或被判以重罪？（包括根據統一軍法典所爲者）					
(b)台端是否曾經被控或被判以違反槍砲彈藥管制法之罪？					
(c)台端目前是否有任何刑事案件繫屬中？					
(d)台端是否曾經被控或被判以與酗酒或服用禁藥有關之罪？					
(e)過去七年中，台端是否曾經接受軍法審判或其他依統一刑法典所進行之懲戒程序？（包括非司法、艦長懲戒權等）					
(f)過去七年中，台端是否曾經因違反任何未列入上述(a)(b)(c)(d)(e)項之罪名，被逮捕、控告或定罪？（交通罰鍰在美金 150 元以下者無庸列舉，但其違規情事與酗酒或服用禁藥有關者，不在此限）					
若針對上述(a)(b)(c)(d)(e)或(f)項答「是」，請在下列空格中說明。請勿於「罪名」欄內填入特定之刑法典，但請列舉實際之罪名或違法事項（例如：縱火罪、竊盜罪等）。					
月/年	罪名	處分行動	執法單位/法院（若非美國境內，請同時註明城市/國家）	州代碼	郵遞區號

24. 禁藥之服用及毒品相關活動

下列問題與非法服用禁藥及毒品相關活動有關。台端須完整而誠實地回答問題，否則將可能成爲影響聘任決定之不利理由，但台端之回答內容及其衍生資料均不會於往後之刑事程序中作爲對台端不利之證據。

(a)台端自 16 歲迄今，獲於過去七中，以較短之期間爲準，是否曾非法使用任何禁藥，如大麻、古柯鹼、純古柯鹼、大麻膏、麻醉品（鴉片、嗎啡、可待因、海洛因等）、安非他命、鎮靜劑類（巴比妥酸鹽、安眠酮、鎮靜劑等）、迷幻藥（麥角二乙基酸胺、天使粉等）或處方藥？

(b)台端是否曾於受雇爲執法人員、檢察官或法庭職員期間、持有安全認證資格期間，或擔任直接而立及對公共安全有影響之職務期間，有非法使用禁藥之情形？

(c)過去七年中，台端是否曾爲圖利自己或他人而涉及任何麻醉品、鎮靜劑、興奮劑、迷幻藥或大麻煙之非法購買、製造、運輸、生產、轉運、運送、收受或販賣？

若台端就以上(a)或(b)項回答「是」，請列舉日期、服用之禁藥及/或處方藥名稱，及各項藥物服用之次數。

起迄年月	服用之禁藥及/處方藥	服用次數

25. 酒精性飲料之服用 過去七年中，台端是否曾因服用酒精性飲料（例如烈酒、啤酒、葡萄酒）而導致任何與酒精有關之治療或諮詢（例如酗酒、或酒精中毒等原因）？	是	否

若台端之答案爲「是」，請於下欄內填寫治療日期及諮詢師或醫師之姓名與地址，但請勿重複上述第 21 題之回答內容。

起迄年月	諮詢師或醫師之姓名/地址	州代碼	郵遞區號

26. 接受調查紀錄 (a)美國政府是否曾對台端進行背景調查/或通過台端之安全認證？若回答「是」，請使用下欄之調查機關代碼作答。若回答「是」，但卻無法確定調查機關及/或個人機密等級，請分別選擇調查機關或個人機密等級「其他」項之代碼，並將「不知道」或「不記得」填入「其他機關」項下。若答「否」，或不知道或不記得是否曾經接受調查或通過安全認證，請勾選「否」。	是	否

調查機關代碼 1-國防部　2-國務院　3-聯邦人事管理局 4-聯邦調查局　5-財政部　6-其他（填入機關名）	機密等級代號 0- 未申請　1-密　2-機密　3-極機密 4- 機密專業資料　5-敏感性　6-L　7-其他

月/年	機關代碼	其他機關	機密等級代碼	月/年	機關代碼	其他機關	機密等級代碼

(b)救台端所知，以往台端之機密等級或調閱權限是否曾經被拒、被中止	是	否

或遭撤銷，或台端曾被政府機關拒絕錄用？若答「是」，請提供被拒日期與機關名稱。註記：行政上之降低或終止 安全認證等級非此處所謂之撤銷。						
月/年	被拒之機關部會		月/年	被拒之機關部會		
27. 財務狀況 (a)過去七年中，台端是否曾依破產法典任何章之規定（包括第十三章）聲請破產？					是	否
(b) 過去七年中，台端是否曾有任何薪資遭扣押或財產被收回之情形？						
(c) 過去七年中，台端是否曾因未繳納稅捐或給付其他債務而有財產遭到質權處分之情事？						
(d) 過去七年中，台端是否曾有未支付法院不利判決金額之情形？						
若台端就以上(a)(b)(c)(d)項回答「是」，請提供以下資料：						
月/年	訴訟列別	金額	訴訟當事人姓名	受理案件法院或機關名稱/地址	州代碼	郵遞區號
28. 債務問題 (a)過去七年中，台端是否曾有任何債務欠達 180 日之情形？					是	否
(b)台端目前是否有積欠任何債務達 90 日之情形？						
若台端就以上(a)(b)項回答「是」，請提供以下資料：						
發生日期	清償日期	金額	貸款或債務類別及帳號	貸方或債權人姓名/地址	州名	郵遞區號
29 公開之民事法庭程序 過去七年中，台端是否曾係任何本表格未舉列之公開民事法庭程序之當事人					是	否
若回答「是」，請於下欄提供有關該公開民事法庭程序之資料：						
月/年	程序類別	程序結果	當事人姓名	法院（若非美國境內，請同時註明城市及郡縣/國家）	州代碼	郵遞區號
30. 參加社團經歷 (a)台端是否曾經是以暴力推翻美國政府爲目的且因此從事非法活動之組織幹部或成員，或爲其效力，且明知該組織係以推動是類活動爲其成立之宗旨？					是	否
(b) 台端是否蓄意從事以武力推翻美國政府之任何行動或活動？						
若台端就以上(a)(b)項回答「是」，請於下列空白處敘明：						
使用續頁之說明						

第 9、10、11 項之答案欄不敷使用時，請利用標準表格第 86A 頁繼續作答。其餘項目如有任何補充資料，請一律使用下列空白繼續作答。若下列空白亦不敷使用，請使用空白紙繼續作答；惟每頁首應註明台端之姓名及社會安全號碼，並於各答案前標明題號。
爲求正確與完整，請台端將本表格第一、第二及附件部分填寫完畢後，再將所有答案檢查一遍，然後在下列切結書及第 10 頁之資訊揭露授權書上簽署並註明日期。
切結書 本人於本表格及附件之陳述乃秉持堅定之信仰與忠實之信念，盡個人所知作真實、完整而正確之紀錄。本人理解，明知且故意在本表格作虛僞不實之陳述得處以徒刑，或科或併科罰金（參見美國法典第十八章第 1001 條）。

簽署（請使用墨水筆書寫）	日期

標準表格第 86 號（EG）
1995 年 9 月修訂
3206-0007 號
聯邦法令彙編第五章
第 731、732 及第 736 條 86-111

表格核准單位及文號：
聯邦管理暨預算局第

NSN7540-00-634-4036

個人資料揭露授權書

請詳細閱讀本件個人資料揭露授權書，並請以墨水簽署及註明日期

本人授權任何調查員、特別調查員或其他聯邦政府機關正式委派人員對本人之背景資料進行調查，並向個人、學校、公寓管理員、雇主、刑事司法機關、徵信機構消費者報導機構、討債公司、零售商或其他消息提供者取得有關本人活動之任何資訊。本項資訊取得包括（但不限於）本人求學經過、搬遷歷史、學業成績、工作表現、出勤狀況、受訓情形、工作經歷、犯罪紀錄、財務及信用狀況。本人授權聯邦機關對本人進行調查，並將本人背景調查紀錄提供申請機關，作爲核發機密資料調閱證之審查依據。

本人理解，對金融或貸款機構、醫療機構、醫院、醫療專業人員及其他資訊提供者而言，另行揭露特定項目的資料乃屬必要，本人亦可能於稍後成爲此項揭露之聯繫對象。有關心理治療或諮商特定項目的資料揭露方面，針對與工作有關之特定問題，得徵詢醫師或治療師之意見。

依照美國法典第五章第 9101 條，本人進一步授權調查員、特別調查員或美國聯邦人事管理局、聯邦調查局、國防部、國防調查署正式委派人員，及其他任何經授權之聯邦機關向刑事司法機關調閱本人之犯罪紀錄，據以判定本人接觸機密資料及/或接受派任或續任國家安全機密職務是否適當。本人理解，依法本人得申請事項紀錄之副本，加以保留。

本人授權本人紀錄之監管者及其他有關本人資料之提供者，於調查員、特別調查員或經授權之上述聯邦機關正式委派人員提出申請時，得揭露是等資料，縱使先前有相反之約定者亦在所不問。

本人理解個人紀錄監管者及資料提供者揭露之資料，僅供聯邦政府爲本標準表格第 86 號所述目的之公務使用，且唯有於法律許可時，政府始得將其再度揭露。

本資料授權書副本經本人簽署者，其效力與本人簽署之正本相同。本授權書自本人簽署日期或本人與聯邦政府關係終止日起，效期五年，以先到期者爲準。

若台端針對第廿一題回答「是」，請閱讀本授權書次頁，並請簽名及簽註日期。

簽署（請用墨水筆）	全名（打字或正楷書寫務必清楚）		簽註日期
別名			社會安全號碼
現址（含城市及街道名稱）	州名	郵遞區號	住宅電話（含區碼）

標準表格第 86 號（EG）
1995 年 9 月修訂
3206-0007 號
聯邦法令彙編第五章
第 731、732 及第 736 條 86-111

表格核准單位及文號：
聯邦管理暨預算局第

NSN7540-00-634-4036

個人醫療資料揭露授權書

填寫本授權書之說明
本揭露授權書之目的係使調查員得以詢問台端之醫療人員下列三項有關台端心理衛生諮商情形之問題。台端對於本授權書之簽署將僅授權該等醫療人員回答下列問題。

本人正尋求派任或續任聯邦政府中之職務，而該等職務需接觸機密之國家安全資訊或特殊核子資訊或資料。基於安全認證程序之需要，本人特授權調查員、特別調查員或經授權進行本人背景調查之聯邦機關之正式委派人員取得下列有關本人心理衛生諮商情形之資訊。

受調查人員之狀況或治療內容是否可能對其判斷力或可靠度產生不利影響，尤其是在保護機密之國家安全資訊或特殊核子資訊或資料方面？

若然，請說明該等狀況之性質及不利影響或治療內容之範圍與持續期間。預後之情形如何？

本人理解依據本揭露授權書所揭露之資料，僅供聯邦政府爲本標準表格第 86 號所述目的之公務使用，且唯有於法律許可時，政府始得將其再度揭露。

本資料揭露授權書副本經本人簽署者，其效力與本人簽署之正本相同。本授權書自本人簽署日期或本人與聯邦政府關係終止日起，效期五年，以先到期者爲準。

簽署（請用墨水筆）	全名（打字或正楷書寫務必清楚）		簽註日期
別名			社會安全號碼
現址（含城市及街道名稱）	州名	郵遞區號	住宅電話（含區碼）

二、機密資訊保密合約

機密資訊保密合約

合約當事人： 及美利堅合眾國

（人員姓名—以正楷或打字書寫）

1. 爲受合法之約束，並基於本人獲准接觸機密資訊，本人特此同意接受本合約所載之義務。本合約中所稱之機密資訊，不問其標明爲機密資訊與否，均屬之，包括依行政命令令第 12958 號所定之標準或任何其他基於國家安全利益而禁止非法揭露資訊之行政命令或法令視爲機密之口頭通訊；以及符合行政命令第 12958 號第 1.1、1.2、1.3 項及第 1.4(e)款或任何其他基於國家安全利益而要求保護資訊之行政命令或法令所定之機密標準而正接受機密認定程序之非機密資訊。本人理解並接受，一旦獲准接觸機密資訊，即表示美國政府給予本人特殊之信任與託付。
2. 本人特此確認已接受對於機密資訊之性質與保護之安全教育，包括確認本人欲透露資訊之其他人員是否有接觸權限之必要程序，且本人明瞭該等程序。
3. 本人已明瞭，本人對於機密資訊如有不當揭露、不當持有或處理不週之情事，即可能對美國造成損害或無可彌補之傷害，抑或令外國因而獲利。本人特此同意，除有下列情形外，本人絕不向任何人透露機密資訊：(a)本人業已正式確認接收者經美國政府適當授權捌以接收該等資訊；或(b)本人業已獲得負責資訊保密或最後通過本人安全認證之美國政府部門或機關（以下稱「部門或機關」）之事前書面授權通知，許可本人揭露該等資訊。本人理解，若本人無法確認資訊之機密等及時，本人於揭露資訊前，應向獲授權之官員確認該等資訊非屬機密者，但接收資訊之對象有前開第(a)或(b)項之情形者，不在此限。本人進一步理解，本人有義務遵守禁止不當揭露機密資訊之法律與命令。
4. 本人已明瞭，若有違反本合約之情事，可能導致本人所擁有之安全認證資格遭終止；本人被解除要求須有該等安全認證資格之特殊信任及託付之職務；或聘僱關係或與通過本人安全認證之部門或機關間之其他關係

遭終止。此外，本人亦明瞭，本人若有任何未經授權揭露機密資訊之情事，則可能構成觸犯一項或多項美國刑法法規之情形，包括美國法典第 18 章第 641、793、794、798、*952 及 1924 條之規定、美國法典第 50 章第 783 條第(b)項之規定，以及 1982 年之情報人員身份保護法之規定。本人瞭解，本合約中並無任何規定構成美國政府對其追訴本人違法行爲之權利的拋棄。

5. 本人特此將一切因不合本合約條款規定之揭露、公佈或公開機密資訊所獲得、將獲得或可能獲得之權利金、報酬及津貼轉讓與美國政府。
6. 本人理解，美國政府得尋求任何可行之救濟方法以執行本合約，包括（但不限於）聲請法院之命令，以禁止違反本合約之資訊揭露行爲。
7. 本人理解，除有權責之官員或法院之終局裁判另有認定外，所有因本人簽署本合約而接觸獲得接觸之機密資訊，不問現在或將來，均係美國政府之財產，或爲美國政府所支配。本人同意，若有下列情形之一時，本人應將所有本人現正持有、可能持有或負責之機密資訊予以返還：(a)經美國政府授權之代表要求；(b)本人與通過本人安全認證或准許本人接觸機密資訊之部門或機關間之聘僱關係或其他關係終結；(c)本人之聘僱關係或其他必須接觸機密資訊之關係終結。本人理解，若本人經要求後仍未返還該等資料，則可能觸犯美國法典第 18 章第 793 條及/或第 1924 條之刑罰規定。
8. 本人理解，非經美國政府之授權代表以書面免除本人基於本合約之一切條件與義務，該等條件及義務於本人有權接觸機密資訊之期間及其後之時期，均繼續適用。
9. 本合約之個別條款均得與合約分離適用。若法院認定本合約之任何條條款不具執行力，本合約之其他條款仍應有完全之效力。
10. 前開之各種限制與下列法令所創設之雇員義務、權利或責任相符，並且未取代、牴觸或以他法更改之：行政命令第 12958 號、美國法典第 5 章第 7211 條（規範向國會所爲之揭露行爲）；經軍事密告者保護法修正之美國法典第 10 章第 1034 條（規範軍職人員向國會所爲之揭露行爲）；經密告者保護法修正之美國法典第 5 章第 2302 條第(b)項第(8)款（規範對於非法行爲、浪費、詐欺、濫用公共衛生或安全威脅之揭露行爲）；1982 年之情報人員身份保護法（美國法典第 50 章第 421 條以下）（規

範使政府秘密幹員曝光之揭露行爲）；以及其他避免可能危及國家安全之揭露行爲之法令，包括美國法典第 18 章第 641、793、794、798、952 及 1924 條之規定，以及 1950 年之顛覆活動法第 4 條第(b)項（美國法典第 50 章第 783 條第(b)項）之規定在內。前開所載之行政命令及法令所創設之定義、規定、義務、權利懲罰與責任均爲本合約之一部分，且規範本合約之履行。

11. 本人業已詳細閱讀本合約之內容，且本人之疑問均以獲得答覆。本人確認簡報官員業已將本合約中所提及之行政命令與法令及其施行細則（聯邦法令彙編第 32 章第 2003.20 條）提供與本人；職是，本人得選擇於此際閱讀其內容。

<table>
<tr><td>簽名</td><td>日期</td><td colspan="2">社會安全號碼
（參見下列公告之內容）</td></tr>
<tr><td colspan="4">單位（若係承包商、被授權人、受機關補助之人或代理人，請填寫名稱、地址及（如若可能）聯邦供應商代號）（以打字或正楷書寫）</td></tr>
<tr><td colspan="2">見證人</td><td colspan="2">承諾人</td></tr>
<tr><td colspan="2">本合約之簽署經下列簽名人見證</td><td colspan="2">下列簽名人代表美國政府接受本合約</td></tr>
<tr><td>簽名</td><td>日期</td><td>簽名</td><td>日期</td></tr>
<tr><td colspan="2">姓名及地址（以打字或正楷書寫）</td><td colspan="2">姓名及地址（以打字或正楷書寫）</td></tr>
<tr><td colspan="4">安全資訊簡報讀取確認欄</td></tr>
<tr><td colspan="4">本人茲確認下列事項：間諜活動法之規定及其他與保護機密資訊相關之聯邦刑法法規與行政命令均已提供本人；本人業已返還本人所保管之所有機密資訊；本人不會將機密資訊告知或傳遞與未經授權之人員或組織；本人會迅速將未經授權之人員查探機密資訊之企圖報告與聯邦調查局知悉；且本人（業已）（尚未）（請刪去不適用之文字）接受安全資訊簡報。</td></tr>
<tr><td colspan="3">雇員簽名</td><td>日期</td></tr>
<tr><td colspan="2">見證人簽名（以打字或正楷書寫）</td><td colspan="2">見證人簽名（以打字或正楷書寫）</td></tr>
</table>

公告：隱私法（美國法典第五章第 552a 條）要求聯邦機關於向個人請求提供資料時，告知該員是否有義務揭露該等資料；請求該等資料之法源爲何；以及該等資料之用途如何。職是，特此告知台端如下之事項：向台端要求社會安全號碼之法源爲行政命令第 9397 號；同時，台端之社會安全號碼將於發生下列必要情形之一時，用以確認台端之身份：(1)證實台端有接觸前開資訊之權限；或(2)認定台端接觸前開資訊之權限業已終止。台端雖無強制性之義務揭露其社會安全號碼，但若未揭露該等號碼，可能妨礙前述證實或認定工作之進行，抑或造成台端接觸機密之資格遭否決。
*不適用於簽署本合約之非政府人員

非公務機關（人員）安全認證

作業手冊（草案）

2004 年 01 月

－　目　　次　－

壹、名詞之定義

一、「安全認證」（security clearance）

泛指為維護國家機密不致外洩，所因而衍生必須針對人員、設施、資料、以及資訊傳播所進行之各項查核措施，凡是通過安全認證措施者，得依照安全認證之等級高低而獲得不同之權限，並得以接觸不同層級之重要國家機密文件、設施或儲藏位置。安全認證可以分階段、分等級、分項目、定期或不定期進行。不過不論查核的方式為何，必須注意的是，安全認證的通過並不代表該人員可以永久享有接觸重要國家機密文件或設施之權限，安全認證只有在進行查核的當時具有正確性，一旦查核過後，其正確性將隨時間增長而遞減。

二、「非公務機關（人員）」

所謂「非公務機關（人員）」係指除正式的官方機構與正式經過考試任用之公務員之外，所有那些雖不具官方位階、或者雖不具正式公務人員資格，但在進行工作或執行任務的過程中確有可能因此接觸國家機密的機關、企業、法人單位或者這些單位內的成員、甚至包括個人在內，將全部包括在本研究所定義的「非公務機關（人員）」的範圍之內，換言之，凡是公務機關（人員）以外的所有可以接觸到國家機密的機關（人員）通通涵蓋在本手冊建議規範的範圍之內。

三、「中央主管機關」

依據法令規定，有權進行安全認證並予受查核之非公務機關（人員）管制之部會署，簡稱「主管機關」或「權責機關」。

四、「國家機密」

所謂的「國家機密」乃是指「為確保國家安全或利益而有保密之必要，對政府機關持有或保管之資訊，經依國家機

密保護法核定機密等級者」。

五、「機密等級」

中央主管機關及執行機關按照「國家機密保護法」、「軍事機密與國防秘密種類範圍等級劃分準則」，將機密資料區分為「絕對機密」、「極機密」及「機密」三等級。

六、「絕對機密」

依照國家機密保護法，所謂「絕對機密」係指「洩漏後足以使國家安全或利益遭受非常重大損害之事項。」

七、「極機密」

係指「洩漏後足以使國家安全或利益遭受重大損害之事項」。

八、「機密」

係指「洩漏後足以使國家安全或利益遭受損害之事項」。

九、「軍事機密」

乃指「與軍事作戰具直接關連，為確保軍事安全或利益而有保密之必要，並經依法令核定機密等級之文書、圖畫、消息、電磁記錄或物品」

十、「國防秘密」

至於「國防秘密」則指「軍事機密以外，為確保國家安全或利益，而有保密之必要，由國防部主管並經依法令核定機密等級之文書、圖畫、消息、電磁記錄或物品」。

十一、「違常」

係指從事研究成果公開活動或其他故意或過失行為，致發生違法洩密或以合法掩護非法洩密或疑似洩密之情況。

貳、前言

在過去，台灣主要倚賴政府相關部門─特別是軍方─進行跟國家安全有關的政策與科技研究。民間部門－包括各種法人、智庫、甚或企業等等－很少有機會能夠參與這其中的過程。這種情況所造成的限制除了抵銷了這些民間部門所可能提供的創造力與改革動力，也讓民間部門無法在安全研究上做出有力的貢獻。

隨著時代的變遷，安全研究領域的參與門檻已經逐漸降低，許多非政府機關部門的智庫、法人機構或企業以及這些單位內的個人開始參與國防安全相關計畫，甚至是由政府部門主動邀請參與安全研究的相關計畫，並因此得以與聞國家安全機密。不過隨著參與的擴大，其他問題也逐漸浮上檯面，包括目前國內法令規章並不完備，各政府相關部門－特別是與國防安全相關之部門－對於所謂的「安全認證」的認識不若美國等先進國家，在執行過程上也往往不夠嚴謹。其結果是民間非公務機關或人員雖得以參與安全相關研究，但卻容易滋生弊端，更很可能在無意中導致國家機密外洩。

從政府的角度來看，為了保障國家安全以及全體人民的整體利益，有些機密資料（不論是來自政府機構或來自非政府機構）必須存在，而且必須嚴格保密，一旦這些資料外流，人民利益與國家生存就可能遭受極大的威脅。因此，進行安全認證以保護機密資料不致因為人為因素而外洩實有其必要。換言之，從正面的角度來看，安全認證的施行乃是希望任何個人在維持、追求其利益的過程中不去危害到全國人民的利益，更不至於因此威脅到國家安全。

參、權責機關與權責之劃分

當前我國安全認證制度的建立尚不夠完整與健全，就非公務機關（人員）部份並無明確之法源依據。但如依照可接觸「國家機密」、以及牽涉「國家安全」等之實質，政府部門對於本項研究所指稱之非公務機關（人員）仍有絕對之執行與管制權責。若按照「涉及國家安全或重大利益公務人員特殊查核辦法」之規定，當前負責執行公務機關（人員）安全認證之主管機關為法務部調查局，因此之故，非公務機關（人員）在同等範圍所受之管制以及主要管制單位應該以「事權統一」為主要之考量，仍以法務部調查局作為主要之權責機關。

在執行安全認證程序時，主管機關與受查核之機關（人員）應建立正確的權責劃分，即「**主管機關有權、非公務機關（人員）有責**」。非公務機關（人員）如果與公務機關（人員）身份有重疊的情況－比方說擔任政務官、國會議員或者國會助理等人員－政府部門當然有權力主動介入進行安全認證。但是對於不具備這些條件的非公務機關（人員），政府部門則可以扮演被動的角色。換言之，政府不必主動介入非公務機關（人員）的查核，反過來，應該由非公務機關（人員）負起主動之責任，依據政府所訂定的安全認證標準程序，詳實填具安全認證所規定之必要文件、以及相關準備（例如內部機密文件之分類、異地儲存重要資料與設備等），然後主動向政府部門提出申請安全認證，在通過查核之後，便可獲得正式參與未來與國家機密相關之研究等事務之資格。

當受查核的單位或人員已經依據標準作業程序提出申請並通過查核之後，主管機關必須轉化其原先之被動角色為主動，針對原先受查核之機關（人員）進行定期及不定期之再查核，受查核機關則轉化其原先主動的角色為被動，必須接受權責機關的查核，並善盡誠實義務，以確保其接觸國家

機密之資格能維持。

肆、非公務機關（人員）安全認證制度

民主國家中，人民有知的權利，但為了保障國家安全以及全體人民的整體利益，有些機密資料（不論是來自政府機構或來自非政府機構）必須存在，而且必須嚴格保密，一旦這些資料外流，人民利益與國家生存就可能遭受極大的威脅。因此，凡有接觸國家機密資料可能性之非公務機關（人員）政府部門均應貫徹執行安全認證制度，並建立通報系統，以防止保護機密資料外洩而危害國家安全。

針對非公務機關（人員）所進行之安全認證應包括：

一、 訂定機密等級之認定標準

凡中央主管機關即有接觸國家機密可能性之非公務機關均應依照「國家機密保護法」、「機密檔案管理辦法」及國防部「軍事機密與國防秘密種類範圍等級劃分準則」訂定機密等級之認定標準。

二、 安全認證

（一）人員安全認證

在既有之國家安全資料機密等級分類上之下，政府可統一規定人員安全認證規範、核發審查作業，以及與任何必要接觸機密資料的人員必需遵行之管制規範，這一規範統稱為「人員安全認證」。人員安全認證的資格審查為進行廣泛且詳細之人員安全背景調查，必要時並得實施測謊試驗。

安全認證應區分基本的等級，其分級應按人員所能接觸的機密等級為區分的標準，至少應包括以下項目：

五、反恐調查（Counter-Terrorist Check, CTC）－通

過這項調查的人士將可獲得接近那些可能遭受恐怖主義攻擊的政府建物或政府機構，但不包括那些受保護的機密文件。

六、安全調查（Security Check, SC）－凡是從事長期性工作，或者經常可以無限制接觸機密，抑或有可能接觸最高機密檔案或資料的人必須通過這項調查。一般來說，這項調查每十年重複進行一次。而如果是約聘人員則每五年必須重新調查一次。

七、進階調查（Developed Vetting）－從事那些最敏感任務或工作的人，包括可以無限制接觸最高機密資料的專任人員必須通過這項更高階的查核。進階調查乃是定期性的執行。

八、基本調查（Basic Check, BC）－泛指人員的前科、酗酒、品行、婚姻記錄等基本資料的調查；這項調查乃是上述三項查核程序的最基本前提。

（二）設施安全認證

「設施安全認證」乃是一種決定「某法人的工作環境與設備，是否具備接觸機密性資訊、或執行機密性合約資格」之判定。而設施安全認證的基本條件，乃是以法人必須接觸機密性資訊才能執行工作為基礎，而且該法人必須於本國法律規範下，於國內創立並實際存在。此外，法人也必須具備良好之商譽及法律紀錄可供查詢，不能有受外資擁有控制或影響。惟不論是國內法人或外資法人，任何法人的行為絕不能與國家利益有任何程度的牴觸。

（三）資訊安全認證

經過認證的法人或其他機關組織在進行與政府相關

的安全研究計畫時，必須指派資訊系統安全經理，以監督網路機密安全，並確認資訊系統符合安全要求，此項措施稱之為「資訊系統安全認證」。

（四）簽署安全保密協定

政府部門於資助非公務機關（人員）進行研究或委託辦理計畫時，應與計畫執行機關（或機關自行研究之研究人員）簽署安全保密協定。

三、 教育訓練

政府部門－包括資助、委辦計畫部門以及安全認證之權責機關－對於受委託、並有與聞國家機密可能性之非公務機關（人員）應定期舉辦有關**安全教育**與**保防知識**之相關講座與教育訓練，以提升接觸機密資料人員之安全概念。訓練課程之教材、師資應由政府部門主動提供。

四、 查驗安全保密措施

權責機關應定期或不定期查驗受委託執行安全研究計畫之非公務機關（及其內部人員）執行安全保密措施情形。

五、 建立「通報系統」

本通報系統由政府部門與受委託之非公務機關共同執行。執行步驟包括：

（一） 受委託執行計畫之非公務機關欲辦理成果公開活動時，應事先向資助機關或委託機關辦理申請並先行初審（自行研究計畫之研究人員直接向任職機關提出申請）；

（二） 資助機關或委託機關接受該機關之申請，並予核准；

（三） 非公務機關（人員）不得以「事後報備」方式辦理研究成果公開活動；

（四） 一旦發現洩密或疑似洩密情形，應立即採取補救措施，並將處理情形回報政府資助機關或委託研究機關；

（五） 從事辦理研究成果公開活動時，若有違常案件發生，政府資助機關或委託機關應即依法處理，並將全案處理結果送主管機關討論。經主管機關研判如屬「有危害國家安全之虞且屬重大者」，應繼續後續之處理程序並追究其相關刑事責任。

茲將政府針對非公務機關（人員）所進行安全認證制度詳述如下：

一、 訂定機密等級之認定標準

中央主管機關應參考「國家機密保護法」、「機密檔案管理辦法」，以及國防部「軍事機密與國防秘密種類範圍等級劃分準則」，依政策或業務需要將與國家安全有關資料訂定「絕對機密」、「極機密」及「機密」三個等級之認定標準。難以訂定標準者，於個別計畫認定時，詳加審查。

與國家安全有關資料並需訂定機密等級者，應包含以下項目：

（八） 軍事計畫、武器系統及其演練；

（九） 外國政府軍政、軍、經資訊；

（十） 情報活動、情報系統及其來源、方法、密碼等；

（十一） 外交關係、外國政府在國內活動資訊及機密來源；

（十二） 涉及國家安全相關之科技或經濟資訊；

（十三） 維護國家重要科技之計畫；

（十四） 涉及國家安全相關之計畫。

所有上述機密資料皆必須給予適當且足夠的保護措

施，使其能夠有效且合理防止遭受損失及破壞，或是被外人取得。這些機密資料保護包含以下三類：

（四） 口頭討論之防護：所有接觸機密資料之人員皆須警覺，並禁止在公共場合或大眾運輸工具，及未加防護措施之通訊媒介中，提及並討論機密文件資訊及內容。

（五） 周邊環境的防護：用於存放各類機密資料及文件資訊之措施，必須具備偵測及防止未經授權之機密資料存取動作。

（六） 緊急措施：發展一套保護機密文件及資訊之緊急應變程序，除考慮其適切性外，必須能做為各種緊急狀況發生時之反應參考。

二、 安全認證

（一）人員安全認證

在既有之國家安全資料機密等級分類上之下，政府可統一規定人員安全認證規範、核發審查作業，以及與任何必要接觸機密資料的人員必需遵行之管制規範，這一規範統稱為「人員安全認證」。人員安全認證的資格審查為進行廣泛且詳細之人員安全背景調查，必要時並得實施測謊試驗。所應填具之資料為**表一**。

人員安全認證的調查程度，依調查對象獲得授權接觸或執行的保密資訊層級而不同。其程序為，先進行一般之安全認證調查，若受調查對象能夠接觸的保密資訊密等越高，所需接受的調查也就越詳細，費時也更久。

為了避免各政府機關採取之調查措施重疊且耗時，

造成行政資源浪費，全國各政府機關應採行通用之相關安全認證最低範圍及標準，敘述如下：

甲、 人員安全調查的時間範圍：過去10年或年滿18歲後（以時間較短者為準），調查範圍可視需要擴大。

乙、 國家機關之查對：法務部調查局應對調查對象、其配偶/同居人進行調查，調查包括：指紋紀錄、與該人員有關之相關國家紀錄（如：國防部兵役資料、內政部警政署、出入境管理局等相關紀錄）

丙、 填報資料：需翔實填寫與國家安全相關的標準表格、檢附指紋卡等。

丁、 面談：受調查對象除要填寫問題表格外，尚須接受面談。面談係由受過訓練之安全調查人員或反情報人員進行，調查過程中，發生重大訊息或矛盾時，應進行額外之面談，另外，在政策許可下，得進行測謊。

戊、 安全認證中，必須查明下列有關受調查人的資訊：

i. 出生：出生日期地點與獨立的出生證明；

ii. 公民資格：調查對象需為中華民國公民（應取得公民資格之獨立證明、國外出生之近親，亦應有公民資格或法律地位之證明）；

iii. 教育狀況：由學術機構以封緘成績單之方式取得學位/文憑之獨立證明，或所有教育紀錄不再調查範圍內，需確認該調查對象有高中以上教育程度；

iv. 受雇情形：調查範圍內所有受雇情形。至少應包括最近兩年之紀錄。任職六個月以上之工作，應約談兩位上級或同事。（無六個月以上者，至少應約談一位主管或同事）超過60日以上之

失業期間，均應確認，如先前有關政府職務軍職等，亦應確認；

v. 證明人：需有四位（至少三位係由調查單位主動接觸），證明人應對調查對象在社會生活上有認識，所有證明人加起來的認識時間應涵蓋整個調查範圍；

vi. 鄰近地區：居住六個月以上者，應訪談最近五年內之鄰居。確認目前之居所，必要時得清查其租賃紀錄。無任何居所超過六個月者，應對其鄰居加以訪談；

vii. 信用狀況：過去七年內調查對象曾居住、受雇、就學達六個月之所有地點之財務、信用狀況確認；

viii. 地方機關之查對：查對調查範圍內曾居住、受雇、就學達六個月以上所有地點之相關警方紀錄。目前居所的紀錄查對；

ix. 公開紀錄：離婚、破產、其他民刑事訴訟之確認。

己、 調查結果得於各機關間相互移交，並應視為符合調查標準。調查結果每五年再重新確認即可中間不必重新調查。若有理由顯示該人員可能不符合調查標準，則需重新進行調查確認。通過初步安全認證的人員，將視其接觸保密資訊的密等而繼續不同程度的安全認證調查。

（二）設施安全認證

「設施安全認證」乃是一種決定「某法人的工作環境與設備，是否具備接觸機密性資訊、或執行機密性合約資格」之判定。設施安全認證是用以決定某法人的工作環境與設備，是否具備接觸機密性資訊或執行機密性合約之資格判定。此為政府單位與民間法人承包商間合作伙伴關係的基礎。

甲、　申請設施安全認證的法人：

以法人必須以接觸機密性資訊才能執行工作為基礎。而且法人必須於本國法律規範下，於國內創立並實際存在。法人必須具備良好之商譽及法律紀錄可供查詢，不能被外資擁有控制或影響。而外資法人安全認證，任何具有外資股份控制權及外資影響力之法人，皆須執行安全評估以降低安全上之風險。同時任何法人絕不能與國家利益有任何程度的牴觸。

乙、　設施安全認證的內容：

(1) 法人的工作環境與設備應提供存放機密文件於經過安全檢驗合格之容器、保險庫或密閉空間，並需要額外之防護措施。
(2) 限制性區域，工作期間如有必要於開放空間內處理機密資料，必須設置以限制區域以作為接觸機密文件之特定限制區。密閉區域，一律須加以控管，防止未經授權之進入及接近。
(3) 額外防護措施，如入侵偵測系統及警衛人員。
(4) 容器、櫥櫃、保險庫及密閉空間之鑰匙、掛鎖及號碼鎖之防護。
(5) 先進的接近控制系統及裝置，自動化的接近控制系統及電子、機械或電機裝置，將可作為取代控制進入限制性或密閉區域之警衛人員。

丙、 任何需要接觸、使用、儲存保密資訊或特殊器材、設施等，或因業務而需單獨進出管制區域之法人，都必須立即向主管機關申請設施安全認證。

丁、 提出申請時，必須註明法人名稱、設施位置、以及是否獲得其他單位之設施安全認證等。如先前未獲得其他設施安全認證，則必須提供標準安全工作之守則、安全措施以及建築物之藍圖等資訊。

戊、 設施安全認證過程如下：

i. 法人提供之資料應證明其安全設施與實行計畫符合國家利益，且未受到一定程度的外國影響或控制。評估的標準為：是否有遭到外國間諜威脅的可能？是否有未經授權之科技轉移？保密資訊的等級？是否遵守相關法令規範？若該法人受到外國勢力影響（如：所有權之轉讓、負債、單位高級主管之變更），必須在三十天內通知主管機關。

ii. 主管機關進行適當之安全認證。

iii. 法人之重要管理人員均需通過人員安全認證。

iv. 負責安全之人員必須為中華民國國公民。

v. 在整個調查完成之前的過渡時期，主管機關可先核發暫時之設施安全認證。

己、 一旦通過設施安全認證，該單位或人員必須經過主管機關核准才得以變更名稱、地點、安全計畫、設施藍圖等。並在進行變更 30 天前，將所有變更以書面通知主管機關，以便主管機關進行評估。主管機關會將評估結果以書面通知該單位。

庚、 法人除了應明確禁止員工在於安全維護裝置之場所與電話通路上討論保密資訊外，更應對工作場所進行管制。法人應建立並維護一可阻止及偵察非法入侵及保密資訊從其場庫辦公室被移動之系統。

辛、　所有進出工作場所之人員，必須接受隨身物品檢查。並需建立緊急狀況時保護保密資訊之程序。

壬、　對外收發紀錄：應保有收發資料之日期、密等等級、資料從何處收到或發往何地等紀錄，至少保留兩年。

癸、　保密資訊之傳送，應由工作場所內連續接收系統行之。並以連號號碼登載，影印號碼應放於極機密文件及所有相關處理文件上。如需於工作場所外傳送，則必須將保密資訊裝置於不透明材質之封袋中，並以兩層封存。封袋外僅標明接、送者之地址，不註明內含資訊之保密等級。收據應由收件人簽收，並保存兩年以上。

11、　極機密資料之傳送，必須先獲得主管機關許可。若由商業運輸業者代為傳送保密資訊，則運輸範圍僅限於本國境內，該運輸業者也必須是獲主管機關核准傳送保密資料者。若有必要，可使用專差、護衛，以保護傳送之保密資訊。

12、　儲存及儲存裝備：主管機關應將儲存保密資訊之容器、貯藏室、隔間材料、門鎖、鑰匙等器具設備建立並頒行統一標準、規格，並將經認可之製造商與儲存裝備列於中央信託局政府採購清單中。

13、　限制性區域：限制性區域需有明確範圍界定，但不一定要有硬體區隔。該區域內之所有工作人員均需注意是否有未經許可進入該區域的人士。

14、　密閉區域：因儲存的保密資訊其體積或本質特性，或因作業需要，必須建構一儲存保密資訊的密閉區域。建立密閉區域必須由主管安全機關核准，並依其要求之標準興建。密閉區域必須利用管制出入的器材，避免發生未獲授權者進出該區域的情況。在密閉區域內開啟任何儲存容器，均需先獲得主管安全機關之核准。

15、 儲存容器、密閉區域之門鎖、號碼鎖、鑰匙等應限定最少數需要者才知悉相關資訊，每月必須清查、每年需應新或輪替，管理人員如有更換，其管理之門鎖、鑰匙亦必須清查更換。

16、 管制出入器材：法人所建立的管制出入系統，必須可辨識進出管制區域或密閉區域之人員為何、並可立即判定該人員是否有權可進出該區域。該系統必須符合主管機關所頒佈的各項標準。

17、 若該法人或設施不再需要接觸、使用、儲存、再製、傳送、輸送或處理保密資料，或主管機關認為繼續授予該法人或設施此等認證，不符合國家安全利益。當設施安全認證遭到終止，主管機關應以書面通知該法人或設施。

（三）資訊安全認證

經過認證的法人或其他機關組織在進行與政府相關的安全研究計畫時，必須指派資訊系統安全經理，以監督網路機密安全，並確認資訊系統符合安全要求，此項措施稱之為「資訊系統安全認證」。

此外，網路安全整合趨勢已經無可避免，每個受資助或委託之非公務機關內部網路系統必須擬妥安全防護計畫，定期做資料備份與異地儲存。在此同時，面對不同、各具備之有管轄權的安全機構參與同一計畫時，應安排單一網路安全管理人員，以達到事權統一的效用、並對整體網路安全系統負責。網路安全管理人員本身也必須確認網路安全計畫之安全政策需求。

網路安全需求依實際需要而定，但必須具有以下基本條件：

（五） 對網路威脅、進行安全服務與機制的描述：
網路必須提供以下服務：使用控制、資料流程控制、資料分割、審核、通訊整合。
（六） 特殊網路安全需求：
網路各元件應有一致整體的安全規劃，網路內部連接之安全控制，資料傳輸的控制與防護，通訊協定與安全防護整合，必須有適當的防火牆（firewall）以控制人員使用及資料傳輸。
（七） 相容性：
連接新系統時必須有相容性，系統可支援區域性安全措施。
（八） 密碼傳輸或其他傳輸安全防護系統：
機密資料在網路中進行傳輸時，必須使用安全防護傳輸系統，或國家安全局認可之密碼編譯系統或其他保密設施，以保護資訊傳輸安全。

當資訊被歸類為機密資訊時，使用之軟體與硬體必須遵循機密等級之要求，同時在操作上也必須具備基本的操作認證技術。主管機關得要求接受查核之非公務機關必須具備以下任一種之操作認證技術：如「使用者之身分證明」、「密碼」、「代幣」、「生物測定」、「指紋辨識及智慧型卡片」等等。

（七） 簽署安全保密協定

政府部門於資助非公務機關（人員）進行研究或委託辦理計畫時，應與計畫執行機關或機關自行研究之研究人員簽署安全保密協定。機密資訊之保密協定可參附錄之範本。

三、 教育訓練

政府部門－包括資助、委辦計畫部門以及安全認證之權責機關－對於受委託、並有與聞國家機密可能性之非公務機關（人員）應定期舉辦有關**安全教育**與**保防知識**之相關講座與教育訓練，以提升接觸機密資料人員之安全概念。訓練課程之教材、師資應由政府部門主動提供；講員則應延聘國內知名學者或專家或政府單位實務經驗豐富之人員擔任。訓練內容應包括：設施安全綜合介紹、防禦安全、威脅的警覺、人員通報的責任、各人員之安全守則、複習簡報等。其中，負責設施安全的人員必須上設施介紹、設施安全維護與運作的課程，此等課程必須獲得安全認證後一年之內完成。

政府部門及主管機關應於每年十二月底前訂定次年之年度教育訓練計畫，並將預定開辦訓練課程公布於政府部門及主管機關網站，實際開辦之課程名稱及日期於開課前二個月公布，供各相關人員報名。

各相關人員每年參加訓練之時數，以下列為原則，如超出所列時數，可由教育訓練系統提供警示訊息供主管參核。

（一）辦理資訊業務人員：九十小時。
（二）非辦理資訊業務人員：六十小時。

各機關審查參訓名單之原則：

（一）　各機關審查參訓名單，以新進人員、將調任不同性質工作及業務有急迫性需求者優先推薦參訓。
（二）　各機關審查參訓名單應由訓練業務承辦人員檢核是否為列管不得參訓人員，將符合參訓人員名單排列優先順序，上網登錄於教育訓練系統且列印名冊，經機關首長或授權人員核准後，將名冊函送主管機關備查。
（三）　同一機關每個課程以三名為限，每人同一課程

二年內不得重覆報名。

四、 查驗安全保密措施

主管機關應成立執行查驗小組，每年針對政府部門所資助或委託與安全研究、國家機密相關之非公務機關（人員）採取辦理定期或不定期抽樣查驗至少一次，以決定該機關、人員、設施、資訊等安全認證是否持續有效，並確保國家機密資料之妥適運用與安全無虞。查驗結果應於每年十二月底前呈報主管機關與委託機關備查。

執行查驗小組實施檢查作業時，應就檢查情形詳予記錄，並應於作業完成後撰寫檢討報告，針對業務缺失提具興革建議，簽報機關首長核閱。前項有關紀錄及檢討報告等，均應指定單位妥為保管，以供權責機關實施外部稽核時之參考。

主管機關視受委託研究之非公務機關業務狀況，由稽核小組不定期實施外部稽核。其稽核作業程序如下：

（一） 受稽核機關實施檢查作業簡報。
（二） 實地稽核及文件審閱。
（三） 綜合座談。

執行查驗小組得調閱受查驗機關資訊作業有關資料，並徵詢作業人員之意見，受查驗機關並應配合提供。執行查驗小組成員因辦理稽核獲悉之機密性資料，應負保密責任。執行查驗小組於外部稽核作業完成後，應就稽核情形撰寫稽核檢討報告，簽報主管機關首長核閱。

外部稽核結果之運用乃為主管機關系統推動評估之參考。提出稽核結果報告送請各機關參考改進，並得視需要辦

理獎懲。

五、 建立並執行「通報系統」

主管機關一旦發現受資助或委託研究之非公務機關疑似洩密，或其他蓄意或無意洩漏、遺失、遭竊等情形（以上通稱洩密），應立即採取補救措施。補救措施除依「國家機密保護辦法」及國防部「軍事機密與國防秘密種類範圍等級劃分準則」相關規定辦理外，並應主管機關與非公務機關相互由建立通報系統，將洩密或違常情形、處理結果回報主管機關與委託機關。經主管機關研判如屬「有危害國家安全之虞且屬重大者」，應繼續後續之處理程序，並追究其相關刑事責任。。

執行「通報系統」時應注意以下各點：

（一） 聯繫有關單位採取適當補救措施，以減少因洩密所產生之損害。

（二） 確認原被洩漏之機密資料、將（或可能將）資料洩漏出去之人員及收到（或可能收到）第一手被洩漏機密資料之人員或機關。

（三） 尋回原被洩漏之機密資料及其複製品，使損害降至最低。並通知負有查處洩密責任之單位，調查洩密原因與責任。

（四） 研究改進機密資料維護措施，以防止再發生類似事件。

（五） 對於洩密人員，應依法追究其刑事責任或民事責任。若需提出訴訟，在訴訟期間應避免二度洩密或洩漏更多機密。

（六） 若受委託之非公務機關發生洩密情形應將處理結果回報政府委託機關；自行研究計畫研究人員應向自行研究機關報告。（洩密通報表格為「**表五、政府委託民營辦理計畫洩密通報表**」）

（七） 若有前述洩密等違常案件，受委託研究之非公務機關（人員）除依前述**依法處理**外，資助或委託機關應將全案處理結果（表格為「**表六、政府委託民營辦理計畫違常案件通報表**」）送主管機關討論。主管機關經研判如屬「有危害國家安全之虞且屬重大者」，應繼續後續之處理程序，並追究相關機關（人員）之刑事責任。

（八） 「有危害國家安全之虞且屬重大者」之判斷標準，可由下列三方向來研判：

甲、 對經濟發展之影響：

該機密資料若流出，足以影響我國相關產業之競爭力者。

乙、 對科技實力之影響

該機密資料若流出，足以喪失我國之在相關產業之國際領先地位者。

丙、 對其他之國家安全事項之影響

丁、 該機密資料足以影響軍事發展、外交利益、兩岸互動、社會安定及其他之國家安全者。

伍、非公務機關（人員）安全認證制度相關表格

表一、人員安全認證問卷

請台端確實遵循各項指示，以免台端之表格無法進行處理。並請務必簽署第九頁之聲明書與第十頁之資料揭露授權書及註明日期。若台端有任何疑問，請去電提供表格之單位查詢。

本表格之目的

中華民國政府進行各類背景調查及複查之目的在於確認軍職人員、國家安全職位之申請人或現職人員，不問其為政府之雇員或承包商、被授權人、證照持有人或受機關補助之人，均已通過必要之安全認證。我們主要依據取自本表之資料作為調查台端是否得以接觸機密資料或特殊核子資訊或資料之依據。當事人唯有決定應徵需要通過安全認證之職為時，才需填寫本表格。

台端提供我們所要求之資料均係出於自願，唯若台端未能提供我們要求完整資料，則我們或將無法完成對台端之調查，或不克及時完成該項調查。此等情形恐將影響台端之職務安置或安全認證之前景。

要求台端提供本表格所載資料之法源

視調查目的之不同而定，中華民國政府係依「國家安全法」、「國家機密保護辦法」、「法務部調查局組織條例」、「公務人員任用法」、「國防部從事及參與國防安全事務人員安全調查辦法」、「機密檔案管理辦法」、「國防部軍事機密與國防秘密種類範圍等級劃分準則」、「涉及國家安全或重大利益公務人員特殊查核辦法」、「行政院所屬各機關資訊業務整體委外作業實施辦法」、「政府資助敏感科技計畫安全管制作業手冊」

之授權而要求本表格之資料。

因他人可能與台端有雷同之姓名或出生年月日，故我們要求台端之身份證號碼以確保記錄之無誤。

調查之程序

國家安全職務之背景調查係為取得相關資料，俾便瞭解台端是否可靠、可信、品行端正及忠於中華民國。台端於本表格所提供之資料均將經由調查予以確認。若有解決爭議之必要時，調查所涵蓋之期間可能超過本表格所含涵蓋之時間。我們將與台端目前之雇主聯繫作為調查之一部分，即便台端先前於申請表或其他表格上表示相反之意思，亦同。

除本表格所載之問題外，我們亦將查詢特定人員對於安全規定之遵守狀況、誠實及正直之行為、易遭利用或脅迫之弱點、詐騙行為、欺瞞行為，以及可能顯示該員不可靠、無信用或不忠誠之任何其他行為、活動或交往情形。

對台端之面談

若干調查將包括與台端進行面談，作為調查程序之正常部分之一。此種方式提供台端更新澄清與更詳盡解釋台端之表格中所述資料之機會，而往往得以使對台端之調查於更短之時間內完成。一旦我們與台端聯絡後，則盡快進行面談是相當緊要的。延後面談之時間對我們處理台端之調查造成延宕，而拒絕面談則可能導致對台端所為調查遭延宕所取消之結果。

台端於前往接受面談時，將會被要求攜帶附相片之身分證明文件。此外，亦有可能要求台端攜帶其他文件以確認台端之身分。此類文件包括：任何合法姓名變更之記錄文件及/或出生證明書等。

我們亦可能要求台端攜帶與台端對本表格所示問題之回答資料或其他需特別留意之事項有關文書。此類事項包括：外僑登記、逾期未付之貸款或欠稅、破產、法院判決、出質情形或其他財務上之負擔、涉及子女監護或扶養之協議、贍養費或財產上之和解內容、遭逮捕、定罪、緩刑及/或假釋之情形。

本表格之結構

本表格分為兩部份。第一部份請交待背景資料，包括台端以往及目前之住居地、求學經過與工作經歷。第二部份則詢問台端之活動，例如被雇主辭退之事例、犯罪紀錄、服用禁藥及酗酒之情形。

於回答本表格之所有問題時，台端須切記由台端針對問題所提供之答案將與調查所獲致之資料一併加以考慮，俾達成妥善之決定。

填具本表格之說明

一、 請台端遵照分發表格人員之指示與其所提供之任何補充說明資料填寫本表。請台端清點需要遞交之表格份數，並以黑色墨水筆在遞交之表格正本及每份副本上簽署並註明日期。台端應保留一份完成後之表格副本作為記錄。

二、 請以黑色繕打或正楷清楚地書寫台端之答案（倘台端填寫之表格，字跡難以辨識，我們將無法受理）。我們亦可能要求台端以經核可之電子格式提供表格。

三、 台端需回答本表格上之所有問題。若無回答之必要或該問題不適用，請於表格上註明（例如，填入「無」或「不是用」）。若台端發現無法確定某日期時，請盡量填入約略之日期，並以填入「約計」或「約略」之方式註明此情形。

四、 若台端於簽署本表格後有變更其內容之情形，需由台端加註姓名字首縮寫及日期。於若干有限之情況下，機關得依台端之意思修改表格。

五、 台端於填寫表格時需利用下欄中所列之各縣市代碼（縮寫）。城市或外國之名稱則請勿縮寫。

六、 為加速對台端之調查，請填寫五碼之郵遞區號。提供本表格之單位會協助台端填寫郵遞區號。

七、 所有電話號碼均需包括區域號碼在內。

八、 本表格中所填入之日期均須以月/日/年或月/年之方式表示。請使用阿拉伯數字 1-12 表示各月份。例如，西元 1978 年 6 月 8 日，應以 6/8/78 加以表示。

九、 凡地址欄出現「城市（國家）」時，若該地址位於中華民國境外，則請於該欄位內亦填入國家名稱。

十、 若台端需要額外之填寫空間列出台端之居所或受雇/自雇/失業或就學記錄，則台端另需填具一份增補表格，及標準表格第 86A 號。若台端需要額外之瑱寫空間回答其他事項，則請使用空白紙張。台端所使用之每頁空白紙張，均須於頁首簽註台端之姓名及身份證號碼。

台端資格之最終決定

對於台端是否有接觸機密資訊之資格，係由要求對台端進行調查之相關政府機關做出最終之決定。於前述機關做出最終決定前，可能會給予台端親自解釋、辯駁或澄清任何資料之機會。

提供不實或虛偽陳述之處罰

依照中華民國法律規定，故意對重大事實為虛偽之陳述或為隱匿之行為，係屬重罪，得處十萬元以下之罰鍰，或科或併科五年以下之有期徒刑。此外，相關政府機關對於有重大變造或故意假造本表格之人員，通常會予以解雇、不予通過安全認證獲取消其資格；同時，此種情形將列入我們之永久記

錄，作為爾後職務安置之參考。基於台端被列入考量之工作具有敏感性，於認定台端是否通過安全認證時，台端之可信賴度乃至為重要之考慮因素。

若台端能誠實並完整地回答全部問題，則台端將有較佳之機會獲得工作或通過安全認證。台端將有恰當之時機就台端於本表格中所提供之任何資料加以說明，並使台端之解釋內容載入記錄。

資料之揭露

台端所提供之資料係用以調查台端是否識適任國家安全職務，依據「涉及國家安全或重大利益公務人員查核辦法」第十條，各機關辦理特殊查核之資料，由各機關依相關規定保密處理，並妥為保管，不得移作他用。故本表格之資料將受保護，不受未經授權之使用。

國家安全職務問卷調查表

第一部份		僅供調查機關使用				代碼			案號			
僅供機關使用												
調查類別		其他範圍		機密等級		存取		行動代號		行動日期	月	日	年
G 地理位置		H 職務				I 職銜						
官方人事檔案所在地				其他地址：					郵遞區號			
安全檔案所在				其他地址：					郵遞區號			
申請人	姓名及職銜		簽署		電話號碼(　　)		日期					
填寫本表格之人員應自下列問題開始回答												
1. 全名				2. 出生日期								
姓：	名：			月		日		年				
3. 出生地（若非於中華民國出生，請註明國名）				4. 身份證號碼								
5. 曾經使用過之其他名字 請台端將曾經使用過之其他名字及使用該名之期間填寫於下欄。（例如：娘家姓、前夫姓、本名、別名或綽號等）。請於娘家姓前加註。												
姓名 #1	自　月/年至月/年至			姓名 #3		自　月/年至月/年至						
姓名 #2	自　月/年至月/年至			姓名 #4		自　月/年至月/年至						
6. 其他個人資料	身高：（公分）			體重：（公斤）					性別：□女□男			
7. 電話號碼	公：（含區碼及分機） □日□夜（）			宅：（含區碼及分機） □日□夜（）								
8. 國籍(a)請參考右欄說明並於□內勾選適合台端之項目，依照其指示作答		我是中華民國出生之公民（請回答 b 和 d 項）							(b)娘家姓名			
		我是國外出生之中華民國公民（請回答 b 和 c 項）										
		我不是中華民國公民（請回答 b 和 e 項）										

<table>
<tr><td colspan="6">(c)中華民國籍：若台端係中華民國公民，但並非在中華民國出生，請提供下欄資料至少一項，以資證明。</td></tr>
<tr><td colspan="6">歸化證明書（在何處歸化）？</td></tr>
<tr><td>法院：</td><td colspan="2">縣市：</td><td colspan="2">證照號碼：</td><td>發證年月日：</td></tr>
<tr><td colspan="6">中華民國護照：</td></tr>
<tr><td colspan="2">現行護照抑或過期護照。</td><td colspan="2">護照號碼：</td><td colspan="2">發照年月日：</td></tr>
<tr><td colspan="3">(d)雙重國籍：若台端目前（或過去）擁有中華民國及另一國之雙重國籍，請將該國名填寫於右欄。</td><td colspan="3">國名：</td></tr>
<tr><td colspan="6">(e)外籍人士：若台端係外籍人士，請填寫下列資料：</td></tr>
<tr><td>台端入境中華民國地點：</td><td>縣市：</td><td>入境日期：</td><td>外僑居留證號碼：</td><td colspan="2">國籍：</td></tr>
<tr><td colspan="6">9. 住址：
請自現址(#1)開始，將過去七年之詳細住址由近而遠逐項填寫於下欄。台端須將所有時期之住址均列出，並請務必列出實際居住之地址：亦即，勿使用郵政信箱做為地址，莫使用永久地址作為就學期間之地址等。另請務必盡可能列出詳細之地址：例如，勿僅填寫台端服役之基地或船艦，而請一併列出營區編號或駐紮港口。台端得省略派駐時間少於 90 日之臨時性軍事任務地點（此際應填入永久住址），如若居住於海外，則應註明。
關於過去五年之住址方面，請列出一名證明台端居住過當地之人士，最好該名證明人目前仍居住在當地（切莫列出全然與過去五年期間無關之證明人，亦請勿以台端之配偶、前配偶或其他親戚作為證明人）。又關於過去五年之住址方面，若列舉之地址係「郵件候領處」、鄉間郵路或星號郵路，或難以確認之地點，請將該地址之方向與位置圖示附於附頁。</td></tr>
<tr><td>#1 現址：
起迄年月</td><td colspan="2">街道地址：　　號#</td><td>城市
（國家）</td><td colspan="2">郵遞區號</td></tr>
<tr><td>證明人姓名：</td><td>街道地址：　　號#</td><td colspan="2">城市
（國家）</td><td>郵遞區號</td><td>電話號碼：()</td></tr>
<tr><td>#2 住址：
起迄年月</td><td colspan="2">街道地址：　　號#</td><td>城市
（國家）</td><td colspan="2">郵遞區號</td></tr>
<tr><td>證明人姓名：</td><td>街道地址：　　號#</td><td colspan="2">城市
（國家）</td><td>郵遞區號</td><td>電話號碼：()</td></tr>
<tr><td>#3 住址：
起迄年月</td><td colspan="2">街道地址：　　號#</td><td>城市
（國家）</td><td colspan="2">郵遞區號</td></tr>
<tr><td>證明人姓名：</td><td>街道地址：　　號#</td><td colspan="2">城市
（國家）</td><td>郵遞區號</td><td>電話號碼：()</td></tr>
<tr><td>#4 住址：
起迄年月</td><td colspan="2">街道地址：　　號#</td><td>城市
（國家）</td><td colspan="2">郵遞區號</td></tr>
</table>

證明人姓名：	街道地址： 號#	城市（國家）		郵 遞 區號	電話號碼：()
#5 住址： 起迄年月	街道地址： 號#		城市（國家）	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）		郵 遞 區號	電話號碼：()

10. 學歷：

請將過去七年高中以上學歷由近(#1)而遠逐項填寫於下欄。請請列出專科或大學學位以上及其授與之日期。若台端離開最後一所就讀之學校已超過七年以上，請列出高中以上之最近學歷，而不問其就讀之時間為何：

關於下欄之「代碼」，使用說明如後：

2- 高級中學 2-專科/大學/軍事院校 3-職業/技術/商業學校

關於台端過去三年之學歷，請列舉一名證明台端就讀該校之人士（例如老師或同學等）。切莫列出全然與過去三年期間無關之證明人。關於函授學校及推廣教育課程，請填寫其紀錄保存之地址。

#1 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：()
#2 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：()
#3 起迄年月	代碼：	學校名稱：	學位/文憑/其他	授與之年月	
學校所在城市（國家）及街道地址：			州名	郵遞區號	
證明人姓名：	街道地址： 號#	城市（國家）	州名	郵 遞 區號	電話號碼：()

11. 請台端自現職(#1)開始，填寫過去七年之工作經歷。台端應詳列所有之全職工作、兼職工作、軍職、超過九十日之臨時軍事任務地點、自營業務、其他有給工作、以及全部失業時間。全部七年之期間均須無間斷加以敘明，但無庸填寫台端十六歲以前之受雇狀況。例外：請列出一切政府機關之文職工作經歷，而不問其是否發生於過去七年之期間內。

代碼：請使用下列「代碼」表明工作類別：
1-現役軍人　2-後備軍人　3-自營業務（填寫業務名稱及證明人姓名）　4-其他相關政府員工　5-縣市政府（非中央政府）員工　6-失業　　7-相關政府合約承攬人（請列出承攬人，而非相關政府機關名稱）
8- 其他

雇主/證明人姓名：請於本欄中填寫台端雇主之名稱或台端自營業務或失業之證明人姓名。若台端填入軍職時，請填入任職地點或駐紮港口及軍種。台端應使用不同欄位以反映軍事任職地點或駐紮港口之變動。

同一職務之早期經歷：若台端有為同一雇主於同一地點在不同期間工作之情形，請填寫此欄位。於第一個編號之欄位填入最近之受雇經歷後，請於其後之欄位填寫在同一地點之早期經歷。例如，台端若三度任職於台北市之 XY 配管工程公司，台端應將最近任職日期及相關資料填入第一欄，並將先前兩次任職之日期、職銜及主管依次填入下面適當之欄位。

#1 現職 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第一欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#2 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）

主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第二欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#3 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第三欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#4 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第四欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
#5 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第五欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	

#6 起迄年月	代碼	雇主姓名/證明人/軍職地點	職銜/階級		
雇主/證明人之街道地址		城市（國家）	州名	郵遞區號	電話號碼（）
工作地點之街道地址（與雇主街址不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
主管姓名及街道地址（與工作地點不同者）		城市（國家）	州名	郵遞區號	電話號碼（）
同一職務之早期經歷（第六欄）		起迄年月	職銜	主管	
		起迄年月	職銜	主管	
		起迄年月	職銜	主管	

12. 最瞭解台端之人士

列舉三位住在中華民國且最瞭解台端之人士。該等人士應為台端之好友、同儕、同事、大學室友等，且其綜合認識台端之時間應盡可能涵蓋過去七年。請勿列舉台端之配偶、前配偶或其他親戚，並盡量避免列舉出現於本表格其他欄位之人士。

#1 姓名	認識日期 起迄年月	電話號碼 □日□夜（）		
住家或工作地址		城市（國家）	州名	郵遞區號
#2 姓名	認識日期 起迄年月	電話號碼 □日□夜（）		
住家或工作地址		城市（國家）	州名	郵遞區號
#3 姓名	認識日期 起迄年月	電話號碼 □日□夜（）		
住家或工作地址		城市（國家）	州名	郵遞區號

13. 配偶

請勾選以下空格以表示台端之婚姻狀況，並於(a)項及/或(b)項提供關於台端配偶之資料。

□1- 從未結婚　□3- 分居　□5- 離婚
□2- 已婚　□4- 合法分居　□6- 鰥寡

(a)配偶　請填寫下列資料。

全名	出生日期	出生地（若非中華民國境內，請同時註明國家）	身份證號碼
其他姓名（娘家姓名、）曾使用過之夫姓等，及使用該名之時間		國籍	
結婚日期	結婚地點（若非中華民國，請同時註明國家）		州名

分居日期	如係合法分居，登記地點為何？城市（國家）		州名
配偶地址（與台端地址不同時填寫；）街、市及中華民國以外之國家		州名	郵遞區號

(b)前配偶　請填寫下列資料，如有需要，請續空白頁。

全名	出生日期	出生地（若非中華民國境內，請同時註明國家）	州名

國籍	結婚日期	結婚地點（若非中華民國，請同時註明國家）	州名

請勾選後填寫日期 □離婚　□鰥寡	月/日/年	如已離婚，登記地點為何？	州名

前配偶地址（街、市及中華民國以外之國家）	州名	郵遞區號	電話號碼 ()

14. 親戚及夥伴關係

請將台端每位存或歿之親戚全名、正確之稱謂代碼、及其他相關資料填入下欄：

1-母(1)　2-父(2)　3-繼母　4-繼父　5-養父母　6-（養）子女

7-配偶前婚子女 8-兄弟　9-姊妹　10-繼父（母）之子 11-繼父（母）之女

12-異父（母）兄弟 13-異父（母）姊妹 14-岳父 15-岳母 16-監護人

17-其他親戚*　18-伙伴　19-目前同居之成年人

*代碼 17（其他親戚）- 僅填入不包含於 1-16 之外國親戚，且與台端或台端之配偶於情感上或義務上有密切持續關係者。代碼 18（夥伴）- 僅填入台端或台端之配偶於情感上或義務上有密切持續關係者。

全名（若身故者，請勾選）左邊之空格		代碼	出生年月日	出生國	國籍	在世親戚目前街址及城市（國家）
		1				
		2				

15. 親戚及夥伴之國籍

若台端之母親、父親、姊妹、兄弟、子女、配偶或與台端間有類似配偶之關係者為非中華民國出生之中華民國公民或在本國居留之外國人，請於第一列填入該員與台端之關係（配偶、類似配偶、母親等）及該員之姓名與出生年月日（此項資料係用以詳細比對第 13 項及第 14 項之資料)。請於第二列填入該員之歸化證明或外僑居留證號碼。另請填入其他適當之資料。

#1 關係	姓名	出生年月日
證明書/居留證號碼	其他資料	
#2 關係	姓名	出生年月日
證明書/居留證號碼	其他資料	

16. 軍中經歷	是	否
(a)是否曾在中華民國軍中服務？		
(b)是否曾在中華民國商船服務？		

請將台端以往在軍中服務之全部經歷填入下列欄位，包括後備軍人。請從最近之經歷(#1)開始填寫。若服務有中斷之情形，請列出各個時期。

代碼：請於下列代碼中選擇一項表示台端服務之軍種：

2- 空軍 2-陸軍 3-海軍 4-海軍陸戰隊 5- 後備軍人

O/E：請勾選代表軍官之「O」欄或代表士兵之「E」欄。

身份：請在台端服役期間之適當欄位內打「X」以表示身份。若係後備軍人，則請勿打 X，請註明縣市。

國家：若台端所服務之對象非中華民國國軍，請填入台端所服務之國家名稱。

起迄年月	代碼	兵籍/證照號碼	O	E	身份			國家
					現役軍人	後備軍人	退役	

17. 國外經歷	是	否
(a)是否有在國外置產、經營事業或營利所？		
(b)目前或曾經受雇於外國政府、公司或機關或擔任其顧問？		
(c)除因中華民國官方業務外，是否曾於中華民國境內或境外與外國政府、外國政府機構（大使館或領事館）或其代表聯繫？（請勿列入例行性之簽證申請及出入境時之聯繫）		
(d)過去七年是否曾經使用外國政府核發之有效護照？		

若台端就(a)、(b)、(c)或(d)項回答「是」，請在以下空白處加以說明：填入日期、相關之公司及/或政府、及台端涉入情形之說明。

起迄年月	公司及/或政府	說明
起迄年月	公司及/或政府	說明

18. 曾經到過哪些國家

除依據政府命令所為之國外行程外，請列舉過去七年台端曾到過的國家，從最近者(#1)開始。（以受扶養人或承包商之身分所為之旅行亦需列入）

- 請使用下列代碼表示台端旅行之目的：1-公務　2-娛樂　3-求學　4-其他
- 請勿將第 9、10 及 11 項提過之國家列入。

#1 起迄年月	代碼	國家	#3 起迄年月	代碼	國家
#2 起迄年月	代碼	國家	#4 起迄年月	代碼	國家

本表格第一部份到此結束。若台端為作答第一部份而使用到續頁或空白頁，請將上述問題之題號填入右欄空白中。	

第二部份	僅供官方使用

19. 軍中紀錄 台端是否曾自軍中不光榮退伍？若「是」，請於下列欄位列出退伍日期及退伍類別	是	否

月/年	退伍類別

20. 醫療紀錄 過去七年中，台端是否曾向心理醫療專業人員（精神科醫師、心理醫師、諮詢師等）求診，或向其他醫療專業人員因心理狀況之問題而求診？	是	否

若台端之答案為「是」，請於下欄中填寫治療日期及治療師或醫師之姓名與地址，但求診之內容僅涉及婚姻、家庭或節哀諮詢，而以台端之暴力行為無關時，不在此限。

起迄年月	治療師或醫師之姓名/地址	縣市	郵遞區號

21. 離職紀錄 台端過去七年是否發生下列情事？若「是」，請自最近發生者開始向前追溯，提供遭解雇、辭職或離職之日期，及其他相關資料。	是	否

請選擇下列代碼並敘明停職理由：

1-被解雇　2-被告知遭解雇後辭職　3-因被指控行為不當經雙方協議離職　4-因被指控績效不彰經雙方協議離職　5-因情勢不利之其他理由離職

起迄年月	代碼	敘明理由	雇主姓名及地址（若非中華民國境內，請同時註明城市/國家）	縣市	郵遞區號

22. 違警紀錄 請於本項中填入台端之相關資料，而不問其資料是否已「封存」或因其他原因自法庭紀錄中消去。	是	否
(a)台端是否曾經被控或被判以重罪？（包括根據軍法所為者）		
(b)台端是否曾經被控或被判以違反槍砲彈藥管制法之罪？		

(c)台端目前是否有任何刑事案件繫屬中？		
(d)台端是否曾經被控或被判以與酗酒或服用禁藥有關之罪？		
(e)過去七年中，台端是否曾經接受軍法審判？（包括非司法、艦長懲戒權等）		
(f)過去七年中，台端是否曾經因違反任何未列入上述(a)(b)(c)(d)(e)項之罪名，被逮捕、控告或定罪？（交通罰鍰在台幣 3000 元以下者無庸列舉，但其違規情事與酗酒或服用禁藥有關者，不在此限）		

若針對上述(a)(b)(c)(d)(e)或(f)項答「是」，請在下列空格中說明。請勿於「罪名」欄內填入特定之刑法典，但請列舉實際之罪名或違法事項（例如：縱火罪、竊盜罪等）。

月/年	罪名	處分行動	執法單位/法院（若非中華民國境內，請同時註明城市/國家）	縣市	郵遞區號

23. 禁藥之服用及毒品相關活動

下列問題與非法服用禁藥及毒品相關活動有關。台端須完整而誠實地回答問題，否則將可能成為影響聘任決定之不利理由，但台端之回答內容及其衍生資料均不會於往後之刑事程序中作為對台端不利之證據。

(a)台端自 16 歲迄今，獲於過去七中，以較短之期間為準，是否曾非法使用任何禁藥，如大麻、古柯鹼、純古柯鹼、大麻膏、麻醉品（鴉片、嗎啡、可待因、海洛因等）、安非他命、鎮靜劑類（巴比妥酸鹽、安眠酮、鎮靜劑等）、迷幻藥（麥角二乙基酸胺、天使粉等）或處方藥？

(b)台端是否曾於受雇為執法人員、檢察官或法庭職員期間、持有安全認證資格期間，或擔任直接而立及對公共安全有影響之職務期間，有非法使用禁藥之情形？

(c)過去七年中，台端是否曾為圖利自己或他人而涉及任何麻醉品、鎮靜劑、興奮劑、迷幻藥或大麻煙之非法購買、製造、運輸、生產、轉運、運送、收受或販賣？

若台端就以上(a)或(b)項回答「是」，請列舉日期、服用之禁藥及/或處方藥名稱，及各項藥物服用之次數。

起迄年月	服用之禁藥及/處方藥	服用次數

24. 酒精性飲料之服用 過去七年中，台端是否曾因服用酒精性飲料（例如烈酒、啤酒、葡萄酒）而導致任何與酒精有關之治療或諮詢（例如酗酒、或酒精中毒等原因）？	是	否

若台端之答案為「是」，請於下欄內填寫治療日期及諮詢師或醫師之姓名與地址，但請勿重複上述第 21 題之回答內容。

起迄年月	諮詢師或醫師之姓名/地址	縣市代碼	郵遞區號

25. 接受調查紀錄	是	否

(a)中華民國政府是否曾對台端進行背景調查/或通過台端之安全認證？若回答「是」，請註明進行/通過調查之機關名稱。若回答「是」，但卻無法確定調查機關及/或個人機密等級，請分別選擇調查機關或個人機密等級「其他」項之代碼，並將「不知道」或「不記得」填入「其他機關」項下。若答「否」，或不知道或不記得是否曾經接受調查或通過安全認證，請勾選「否」。							
機密等級代號 1-機密　2-極機密　3-絕對機密　4-其他							
月/年	機關名稱	機密等級代碼	月/年	機關名稱		機密等級代碼	
(b)就台端所知，以往台端之機密等級或調閱權限是否曾經被拒、被中止或遭撤銷，或台端曾被政府機關拒絕錄用？若答「是」，請提供被拒日期與機關名稱。 註記：行政上之降低或終止安全認證等級非此處所謂之撤銷。						是	否
月/年	被拒之機關部會		月/年	被拒之機關部會			
26. 財務狀況 (a)過去七年中，台端是否曾依法聲請破產？						是	否
(b) 過去七年中，台端是否曾有任何薪資遭扣押或財產被收回之情形？							
(c) 過去七年中，台端是否曾因未繳納稅捐或給付其他債務而有財產遭到質權處分之情事？							
(d) 過去七年中，台端是否曾有未支付法院不利判決金額之情形？							
若台端就以上(a)(b)(c)(d)項回答「是」，請提供以下資料：							
月/年	訴訟列別	金額	訴訟當事人姓名	受理案件法院或機關名稱/地址		縣市	郵遞區號
28. 債務問題 (a)過去七年中，台端是否曾有任何債務欠達 180 日之情形？						是	否
(b)台端目前是否有積欠任何債務達 90 日之情形？							
若台端就以上(a)(b)項回答「是」，請提供以下資料：							
發生日期	清償日期	金額	貸款或債務類別及帳號	貸方或債權人姓名/地址		縣市	郵遞區號
29 公開之民事法庭程序 過去七年中，台端是否曾係任何本表格未舉列之公開民事法庭程序之當事人						是	否
若回答「是」，請於下欄提供有關該公開民事法庭程序之資料：							
月/年	程序類別	程序結	當事人姓名	法院（若非中華民國境內，請		縣	郵

		果		同時註明城市及郡縣/國家）	市代碼	遞區號
30. 參加社團經歷					是	否
(a)台端是否曾經是以暴力推翻中華民國政府為目的且因此從事非法活動之組織幹部或成員，或為其效力，且明知該組織係以推動是類活動為其成立之宗旨？						
(b) 台端是否蓄意從事以武力推翻中華民國政府之任何行動或活動？						
若台端就以上(a)(b)項回答「是」，請於下列空白處敘明：						
使用續頁之說明						
第 9、10、11 項之答案欄不敷使用時，請利用空白頁繼續作答。其餘項目如有任何補充資料，請一律使用下列空白繼續作答。若下列空白亦不敷使用，請使用空白紙繼續作答；惟每頁首應註明台端之姓名及身份證號碼，並於各答案前標明題號。						
為求正確與完整，請台端將本表格第一、第二及附件部分填寫完畢後，再將所有答案檢查一遍，然後在下列切結書及資訊揭露授權書上簽署並註明日期。						
切結書 本人於本表格及附件之陳述乃秉持堅定之信仰與忠實之信念，盡個人所知作真實、完整而正確之紀錄。本人理解，明知且故意在本表格作虛偽不實之陳述得處以徒刑，或課或併課罰金。						
簽署（請使用墨水筆書寫）					日期	

個人資料揭露授權書

請詳細閱讀本件個人資料揭露授權書，並請以墨水簽署及註明日期

本人授權任何調查員、特別調查員或其他相關政府機關正式委派人員對本人之背景資料進行調查，並向個人、學校、公寓管理員、雇主、刑事司法機關、徵信機構消費者報導機構、討債公司、零售商或其他消息提供者取得有關本人活動之任何資訊。本項資訊取得包括（但不限於）本人求學經過、搬遷歷史、學業成績、工作表現、出勤狀況、受訓情形、工作經歷、犯罪紀錄、財務及信用狀況。本人授權相關政府機關對本人進行調查，並

將本人背景調查紀錄提供申請機關，作為核發機密資料調閱證之審查依據。

本人理解，對金融或貸款機構、醫療機構、醫院、醫療專業人員及其他資訊提供者而言，另行揭露特定項目的資料乃屬必要，本人亦可能於稍後成為此項揭露之聯繫對象。有關心理治療或諮商特定項目的資料揭露方面，針對與工作有關之特定問題，得徵詢醫師或治療師之意見。

依照涉及國家安全或重大利益公務人員特殊查核辦法，本人進一步授權調查員、特別調查員或相關政府機關、法務部調查局、國安局、國防部正式委派人員，及其他任何經授權之相關政府機關向刑事司法機關調閱本人之犯罪紀錄，據以判定本人接觸機密資料及/或接受派任或續任國家安全機密職務是否適當。本人理解，依法本人得申請事項紀錄之副本，加以保留。

本人授權本人紀錄之監管者及其他有關本人資料之提供者，於調查員、特別調查員或經授權之上述相關政府機關正式委派人員提出申請時，得揭露是等資料，縱使先前有相反之約定者亦在所不問。

本人理解個人紀錄監管者及資料提供者揭露之資料，僅供相關政府為本標準表格所述目的之公務使用，且唯有於法律許可時，政府始得將其再度揭露。

本資料授權書副本經本人簽署者，其效力與本人簽署之正本相同。本授權書自本人簽署日期或本人與中華民國政府關係終止日起，效期五年，以先到期者為準。

（若台端針對第廿一題回答「是」，請閱讀本授權書次頁，並請簽名及簽註日期。）

簽署（請用墨水筆）	全名（打字或正楷書寫務必清楚）	簽註日期
別名	身份證號碼	
現址（含縣市及街道名稱）	郵遞區號	住宅電話（含區碼）

個人醫療資料揭露授權書

填寫本授權書之說明

本揭露授權書之目的係使調查員得以詢問台端之醫療人員下列三項有關台端心理衛生諮商情形之問題。台端對於本授權書之簽署將僅授權該等醫療人員回答下列問題。

本人正尋求派任或續任中華民國政府中之職務，而該等職務需接觸機密之國家安全資訊或特殊核子資訊或資料。基於安全認證程序之需要，本人特授權調查員、特別調查員或經授權進行本人背景調查之相關政府機關之正式委派人員取得下列有關本人心理衛生諮商情形之資訊。

受調查人員之狀況或治療內容是否可能對其判斷力或可靠度產生不利影響，尤其是在保護機密之國家安全資訊或特殊核子資訊或資料方面？

若然，請說明該等狀況之性質及不利影響或治療內容之範圍與持續期間。預後之情形如何？

本人理解依據本揭露授權書所揭露之資料，僅供中華民國政府為本標準表格所述目的之公務使用，且唯有於法律許可時，政府始得將其再度揭露。

本資料揭露授權書副本經本人簽署者，其效力與本人簽署之正本相同。本授權書自本人簽署日期或本人與中華民國政府關係終止日起，效期五年，以先到期者為準。

簽署（請用墨水筆）	全名（打字或正楷書寫務必清楚）	簽註日期
別名	身份證號碼	
現址（含縣市及街道名稱）	郵遞區號	住宅電話（含區碼）

表二、機密資訊保密合約

機密資訊保密合約

合約當事人：　　及中華民國
（人員姓名—以正楷或打字書寫）

12. 為受合法之約束，並基於本人獲准接觸機密資訊，本人特此同意接受本合約所載之義務。本合約中所稱之機密資訊，不問其標明為機密資訊與否，均屬之，包括依「國家機密保護法」、「軍事機密與國防秘密種類範圍等級劃分準則」或任何其他基於國家安全利益而要求保護資訊之行政命令或法令所定之機密標準而正接受機密認定程序之非機密資訊。本人理解並接受，一旦獲准接觸機密資訊，即表示美中華民國政府給予本人特殊之信任與託付。
13. 本人特此確認已接受對於機密資訊之性質與保護之安全教育，包括確認本人欲透露資訊之其他人員是否有接觸權限之必要程序，且本人明瞭該等程序。
14. 本人已明瞭，本人對於機密資訊如有不當揭露、不當持有或處理不週之情事，即可能對中華民國造成損害或無可彌補之傷害，抑或令外國因而獲利。本人特此同意，除有下列情形外，本人絕不向任何人透露機密資訊：(a)本人業已正式確認接收者經中華民國政府適當授權以接收該等資訊；或(b)本人業已獲得負責資訊保密或最後通過本人安全認證之中華民國政府部門或機關（以下稱「部門或機關」）之事前書面授權通知，許可本人揭露該等資訊。本人理解，若本人無法確認資訊之機密等及時，本人於揭露資訊前，應向獲授權之官員確認該等資訊非屬機密者，但接收資訊之對象有前開第(a)或(b)項之情形者，不在此限。本人進一步理解，本人有義務遵守禁止不當揭露機密資訊之法律與命令。
15. 本人已明瞭，若有違反本合約之情事，可能導致本人所擁有之安全認證資格遭終止；本人被解除要求須有該等安全認證資格之特殊信任及託付之職務；或聘僱關係或與通過本人安全認證之部門或機關間之其他關係遭終止。此外，本人亦明瞭，本人若有任何未經授權揭露機密資訊之情事，則可能構成觸犯一項或多項中華民國刑法法規之情形，包括之規定。本人瞭解，本合約中並無任何規定構成中華民國政府對其追訴本人違法行為之權利的拋棄。
16. 本人特此將一切因不合本合約條款規定之揭露、公佈或公開機密資訊所獲得、將獲得或可能獲得之權利金、報酬及津貼轉讓與中華民國政府。
17. 本人理解，中華民國政府得尋求任何可行之救濟方法以執行本合約，包

括（但不限於）聲請法院之命令，以禁止違反本合約之資訊揭露行為。

18. 本人理解，除有權責之官員＼或法院之終局裁判另有認定外，所有因本人簽署本合約而接觸獲得接觸之機密資訊，不問現在或將來，均係中華民國政府之財產，或為中華民國政府所支配。本人同意，若有下列情形之一時，本人應將所有本人現正持有、可能持有或負責之機密資訊予以返還：(a)經中華民國政府授權之代表要求；(b)本人與通過本人安全認證或准許本人接觸機密資訊之部門或機關間之聘僱關係或其他關係終結；(c)本人之聘僱關係或其他必須接觸機密資訊之關係終結。本人理解，若本人經要求後仍未返還該等資料，則可能觸犯中華民國法律，須負起相關刑責。
19. 本人理解，非經中華民國政府之授權代表以書面免除本人基於本合約之一切條件與義務，該等條件及義務於本人有權接觸機密資訊之期間及其後之時期，均繼續適用。
20. 本合約之個別條款均得與合約分離適用。若法院認定本合約之任何條款不具執行力，本合約之其他條款仍應有完全之效力。
21. 前開之各種限制與下列法令所創設之雇員義務、權利或責任相符，並且未取代、牴觸或以他法更改之：「國家安全法」、「國家機密保護辦法」、「公務人員任用法」、「國防部從事及參與國防安全事務人員安全調查辦法」、「涉及國家安全或重大利益公務人員特殊查核辦法」之規定在內。前開所載法令所創設之定義、規定、義務、權利懲罰與責任均為本合約之一部分，且規範本合約之履行。
22. 本人業已詳細閱讀本合約之內容，且本人之疑問均以獲得答覆。本人確認簡報官員業已將本合約中所提及法令及其施行細則提供與本人；職是，本人得選擇於此際閱讀其內容。

<table>
<tr><td>簽名</td><td>日期</td><td colspan="2">身份證號碼
（參見下列公告之內容）</td></tr>
<tr><td colspan="4">單位（若係承包商、被授權人、受機關補助之人或代理人，請填寫名稱、地址）（以打字或正楷書寫）</td></tr>
<tr><td colspan="2">見證人</td><td colspan="2">承諾人</td></tr>
<tr><td colspan="2">本合約之簽署經下列簽名人見證</td><td colspan="2">下列簽名人代表中華民國政府接受本合約</td></tr>
<tr><td>簽名</td><td>日期</td><td>簽名</td><td>日期</td></tr>
<tr><td colspan="2">姓名及地址（以打字或正楷書寫）</td><td colspan="2">姓名及地址（以打字或正楷書寫）</td></tr>
<tr><td colspan="4">安全資訊簡報讀取確認欄</td></tr>
</table>

<table>
<tr><td colspan="3">本人茲確認下列事項：與保護機密資訊相關之法規與行政命令均已提供本人；本人業已返還本人所保管之所有機密資訊；本人不會將機密資訊告知或傳遞與未經授權之人員或組織；本人會迅速將未經授權之人員查探機密資訊之企圖報告法務部調查局及其他主管機關知悉：且本人（業已）（尚未）（請刪去不適用之文字）接受安全資訊簡報。</td></tr>
<tr><td colspan="2">雇員簽名</td><td>日期</td></tr>
<tr><td>見證人簽名（以打字或正楷書寫）</td><td colspan="2">見證人簽名（以打字或正楷書寫）</td></tr>
<tr><td colspan="3">公告：依據「涉及國家安全或重大利益公務人員特殊查核辦法」，特此告知台端如下之事項：向台端要求身份證號碼之法源為；同時，台端之身份證號碼將於發生下列必要情形之一時，用以確認台端之身份：(1)證實台端有接觸前開資訊之權限；或(2)認定台端接觸前開資訊之權限業已終止。台端雖無強制性之義務揭露身份證號碼，但若未揭露該等號碼，可能妨礙前述證實或認定工作之進行，抑或造成台端接觸機密之資格遭否決。</td></tr>
<tr><td colspan="3">*不適用於簽署本合約之非政府人員</td></tr>
</table>

表三、資訊安全認證表

1 資訊安全政策

查 核 項 目	是	否
1.1 管理階層是否瞭解資訊安全目的並予支持？		
1.2 貴機關之資訊安全政策文件是否由管理階層核准並正式發布且轉知所有員工？		
1.3 貴機關是否訂有資訊安全政策的說明文件及資料(如作業程序、資訊安全控管文件、使用者應遵守的安全規則)？		
1.4 資訊安全政策文件是否包括資訊安全定義、目標、涵蓋範圍、實施內容、執行組織、權責分工、員工責任、事件通報程序、處理流程等？		
1.5 資訊安全政策文件是否就一般使用人員與專責人員之權責分項說明？		
1.6 是否指定專人或專責單位進行資訊安全政策的維護及檢討工作？		
1.7 資訊安全政策是否定期評估，並作必要調整？		
1.8 是否定期對單位人員及資訊設備進行安全評估，以確定其是否遵守機關資訊安全政策及相關規定？		
1.9 是否訂有違反資訊安全規定之處理程序？		
1.10 與外單位簽訂資料存取之契約中是否包含資料保護、服務水準、智慧財產權、事故發生處理方式等條款？		
1.11 委外契約中有關安全需求內容是否包含法律需求(如電腦處理個人資料保護法)、界定雙方有關人員權責、使用何種實體與邏輯安全控管措施、對委外廠商稽核權、得依實際需要隨時修改安全控管措施及作業程序等？		

2 建立資訊安全組織

查 核 項 目	是	否
2.1 是否指定高級主管人員或成立跨部門組織負責推動、協調及監督資訊安全管理事項？		
2.2 是否指定專人或專責單位負責規劃、執行與控管資訊安全工作？		
2.3 是否指定單位辦理風險評估、安全分級、系統安全控管措施？		
2.4 是否訂定規範員工的資訊安全作業程序與權責(含經管使用設備及作業須知)？		
2.5 是否訂定各項資訊設備的安全作業程序？		
2.6 是否訂定有關資訊安全狀況授權處理層級？		
2.7 是否對資訊計畫內容進行資訊安全政策符合性檢查？		
2.8 單位內因業務需要開放給外單位(含其他機關、上下游業者、顧問、維護廠商、委外承包商、臨僱人員)使用之資訊，其存取權限是否嚴加控管？		
2.9 單位內開放給外單位作資料存取是否辦理風險評估？		
2.10 單位內開放給外單位作資料存取是否訂定控管程序？		
2.11 單位內開放給外單位作資料存取於契約中是否訂定雙方權利義務及違約處分方式？		

3 人員安全與管理

查　核　項　目	是	否
3.1 對人員之進用及調派，是否作適當之安全評估？		
3.2 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有妥適分工，分散權責？		
3.3 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否實施人員輪調？		
3.4 對於可存取機密性、敏感性資訊或系統之員工以及配賦系統存取特別權限之員工是否有建立人力備援制度？		
3.5 針對人員之調動、離職或退休，是否立即取消其各項識別碼、通行碼？		
3.6 是否對員工品德、行為、家庭狀況等加以考核？		
3.7 員工是否瞭解單位之資訊安全政策？		
3.8 是否依員工職務層級進行適當的資訊安全講習？		
3.9 是否隨時公告資訊安全相關訊息？		
3.10 下班後員工是否將經辦之機密性或敏感性資料，妥善收藏？		
3.11 是否對員工的私人資訊設備作必要之安全控管程序？		
3.12 單位是否派員參與外界舉辦相關訓練、研討會、產品展示會？		

4 資產分類與控管

查　核　項　目	是	否
4.1 重要的資產(含資訊、軟體、實體)是否均指定專人負責？		
4.2 是否建置資產清冊且隨時更新？		
4.3 資訊是否分級(區分機密性、敏感性及一般性)？是否建立資訊安全等級之分類標準？		
4.4 是否配合資訊分級，建立一套符合需要的資訊保護措施？		
4.5 系統文件、顯示螢幕、儲存媒體、電子訊息及檔案資料等是否作安全等級分類？		
4.6 對於安全等級要求高的各類資訊，是否標示清楚？		

5 實體及環境安全管理

查　核　項　目	是	否
5.1 資訊設備之設置是否作安全上之考量？		
5.2 機密性工作站是否專人管理？		
5.3 需特別保護之設備是否與一般設備區隔？		
5.4 是否檢查及評估火、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等加諸於設備之危害？		
5.5 電腦作業區(含機房)是否落實執行禁止抽煙及飲用食物？		
5.6 電源之供應及備援電源是否作安全上考量？		
5.7 通訊線路及電纜線是否作安全保護措施？		
5.8 設備之維護是否由授權之維護人員執行？		
5.9 攜帶型的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)並落實執行？		
5.10 設備報廢前是否先將機密性、敏感性資料及有版權軟體移除？		
5.11 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？		
5.12 電腦機房內是否嚴禁存放易燃物及未經核准之電器或其他物品？		
5.13 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？		
5.14 電腦機房操作人員是否熟悉自動滅火系統操作方法及滅火機位置？		
5.15 各項安全設備是否定期檢查？員工有否施予適當的安全設備使用訓練？		
5.16 是否制訂資訊安全緊急應變處理程序？有否定期演練及測試？		
5.17 公文及磁片長時間不使用及下班後是否妥為存放？機密性、敏感性資訊是否妥為收存？		
5.18 棄置之手寫或影印公文廢紙及已過保存期限之公文，若為機密性、敏感性者是否予以銷毀？		
5.19 個人電腦及終端機不使用時是否有關機、登出、設定螢幕密碼或是以其他控制措施進行保護？		
5.20 對於資訊財產攜出辦公處所，是否訂有安全之攜出管理規則？		

6 通訊與操作管理

查　核　項　目	是	否
6.1 資訊處理設備，是否訂有操作程序及管理責任？		
6.2 是否建立系統變更之程序？		
6.3 是否訂定電腦當機及服務中斷後之緊急處理程序？ 6.4 是否訂有資訊安全事件通報程序並確實依規定通報？		
6.5 資訊安全事件處理的過程是否均留有完整記錄？		
6.6 對安全要求高的資訊業務是否將資訊安全管理及執行的責任分散？		
6.7 業務系統之使用、資料建檔、系統操作、網路管理、行政管理、系統發展維護、變更管理、安全管理等工作是否授權分由不同的人員執行？		
6.8 系統開發及正式作業是否在不同的處理器、不同的系統環境處理？		
6.9 系統開發及正式作業是否使用不同的登入程序？		
6.10 是否與業者簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款？		
6.11 資訊委外服務契約是否包含對於機密性、敏感性資料之雙方權責及作業程序？		
6.12 伺服器及個人電腦是否採行必要的事前預防及保護措施？		
6.13 是否遵守軟體授權規定，禁止使用未取得授權的軟體？		
6.14 是否全面使用防毒軟體並即時更新病毒碼？		
6.15 是否即時公告有關病毒最新資訊？		
6.16 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？		
6.17 是否對單位員工辦理資訊安全宣導講習(含防毒、備份及一般機密保護規定)？		
6.18 對於外來及內容不確定的磁片在使用前，是否先作電腦病毒掃瞄？		
6.19 是否對重要的資料及軟體定期作備份處理？		
6.20 備份資料是否異地存放?存放處所環境是否合於電腦機房安全標準？		
6.21 重要資料的備份是否保留三代以上？		
6.22 是否定期測試備份資料以確保備份資料之可用性？		
6.23 是否檢查更正作業妥適與否？確保更正作業未破壞系統原有的安控措施及更正作業係依正當的授權程序辦理。		
6.24 是否定期檢討電腦網路安全控管事項之執行？		
6.25 是否使用網路防火牆(Fire Wall)？		
6.26 是否定期檢測網路運作環境之安全漏洞？		
6.27 有關電腦網路安全之事項是否隨時公告？		
6.28 對於敏感性資訊之傳送是否採取資料加密等保護措施？		
6.29 媒體儲存的資料不再繼續使用時是否將儲存的內容消除？		
6.30 儲存媒體是否依保存規格要求存放在安全的環境？		
6.31 內含機密性或敏感性資料的媒體報廢時是否指定專人處理？		
6.32 敏感性資料報廢時是否紀錄處理時機、方式、人員？		

6.33 輸出及輸入機密性、敏感性資料是否有處理程序及標示？		
6.34 收受機密性、敏感性資料是否有正式收受紀錄？		
6.35 機密性、敏感性資料在儲存媒體上是否明確標示資料機密等級？		
6.36 系統文件發送對象是否經系統負責人的授權？		
6.37 系統文件是否有適當的存取保護措施？		
6.38 對於資料及軟體之交換使用是否均有相關文件？		
6.39 重要電腦資料媒體(含報表)是否有專人負責運送並記錄運送時間及內容？		
6.40 儲存機密及敏感性資料的電腦媒體是否採取特別的安全保護措施(如使用加密技術)？		
6.41 採行電子交換之資料交換是否視資料之安全等級採行帳號密碼管制、電子資料加密或電子簽章認證等保護措施？		
6.42 是否要求員工接收電子郵件後立即自郵件伺服器中刪除？		
6.43 敏感性、機密性資料的處理過程是否有嚴密的安全保護機制(如數位簽章、認證及加解密等)？		

7 存取控制

查 核 項 目	是	否
7.1 是否訂有資訊存取控制政策及相關說明文件？		
7.2 資訊存取控制政策是否符合資料保護等相關法令與契約規定？		
7.3 資訊存取控制政策是否依工作性質與職務分別訂定？		
7.4 是否將資訊存取說明文件列入員工手冊？		
7.5 對於多人使用之資訊系統，是否建立使用者註冊管理程序及紀錄？		
7.6 使用者及外單位人員是否取得正式存取授權？		
7.7 是否依個別應用系統安全需求制定安全等級與分類？		
7.8 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？		
7.9 資訊系統與服務是否儘量避免使用共同帳號？		
7.10 使用者存取權限的檢視，是否訂有嚴格管制程序？		
7.11 是否保留與隨時更新使用者註冊資料？		
7.12 是否定期檢查並刪除重覆或閒置的使用者帳號？		
7.13 是否嚴格管制使用者初次登入電腦系統後必須立即更改預設之密碼？		
7.14 對於忘記密碼之處理，是否有嚴格的身份確認程序？		
7.15 預設之密碼是否以規定之安全程序轉交於使用者，使用者取得密碼確認無誤後回應系統管理者？		
7.16 是否定期複檢(建議每六個月一次)或在變更權限後立即稽核？		
7.17 密碼長度是否超過七個字元？		
7.18 密碼是否規定需有大小寫字母、數字及符號組成？		
7.19 密碼輸入錯誤，是否訂有三次以下之限制？		
7.20 是否避免使用與個人有關資料（如生日、身份證字號、單位簡稱、電話號碼等）		

當做密碼？		
7.21 是否依照規定的期限或使用的次數變更密碼？		
7.22 是否於不使用時用上鎖或密碼等管制措施不讓電腦或終端機遭非法使用？		
7.23 應用系統是否具有作業結束後或在一定期間未操作時即自動登出之保護機制？		
7.24 是否有界定網域的範圍與在該網域上可利用的網路連線服務？		
7.25 是否建立完整的網路服務使用授權程序？		
7.26 是否規劃建置使用者連線使用資訊系統的方式(如專線或固定號碼撥接)？		
7.27 是否規劃運作將特定輸出入埠(port)之使用者自動連線到指定的應用系統或安全閘道(Security Gateway)做認證或其他安全辨識的工作再進入系統？		
7.28 是否依環境或業務需要，於網路防火牆作適當之設定？		
7.29 是否依業務性質或任務分配來建置邏輯性網域的存取權限機制(如虛擬私有網路 VPN)？		
7.30 對外連線是否有使用密碼技術(Cryptographic based technique)、硬體符記(Hardware token)、挑戰/回應(Challenge/Response)協定或透過檢查專線用戶位址的設備等鑑別方法以找出連線作業的來源？		
7.31 對外連線是否有建置回撥(Dial-back)作業程序與控管措施及相關測試？		
7.32 網路中繼節點設備是否列入管制與鑑別的範疇並有適當的鑑別方法？		
7.33 是否有製訂遠端維護用輸出入埠的存取作業規範並確實遵行(如用鑰匙鎖住，軟硬體維護支援人員須通過查驗或稽核始能進行)？		
7.34 是否依據服務性質區隔出獨立的邏輯網域，每個網域都有既定的防護措施並有通訊閘道管制過濾網域間資料的存取(如網路防火牆)？		
7.35 是否管制使用者的連線功能(如網路通訊閘道所設定的規則)？		
7.36 是否針對電子郵件、單雙向檔案傳輸、互動式存取與存取時段做通盤連線控管考量？		
7.37 是否設有檢測連線的來源位址與目的位址網路路由之控管措施？		
7.38 提供網路服務的供應廠商是否對網路中繼設備的特性與安全政策提供清楚的說明與設定方式？		
7.39 是否限制登入失敗次數的上限(建議三次)並中斷連線？		
7.40 是否限制登入失敗次數超過上限時需經過一段時間或重新取得授權後才可再登入？		
7.41 是否限制登入作業，在一定期間未操作時，即予中斷連線？		
7.42 對於異常的登入程序，是否留有紀錄(LOG FILE)，並有專人定期檢視？		
7.43 是否於登入作業完成後顯示前一次登入的日期與時間，或提供登入失敗的詳細資料？		
7.44 使用者是否均有專屬的識別碼？		
7.45 是否採用適當的加解密與生物測定技術提供身份辨別(Identification)鑑別		
7.46 密碼是否分由不同單位分配與保管？		

7.47 是否將輸入的密碼顯示在螢幕上？		
7.48 是否將密碼檔與應用系統的資料檔分開儲存？		
7.49 密碼檔是否以單向加密演算法(One-way encryption algorithm)儲存？		
7.50 軟體安裝完畢後是否立即更新廠商所預設之密碼？		
7.51 是否必須經過身份認定程序才能使用系統公用程式？		
7.52 是否將系統公用程式與應用程式隔離存放？		
7.53 是否訂定系統公用程式授權程序？		
7.54 是否訂定系統公用程式授權等級？		
7.55 是否訂定系統公用程式使用期限？ 7.56 是否保存系統公用程式使用紀錄？		
7.57 是否對風險性高的應用程式限制其連線作業需求？		
7.58 是否依據使用者身分控制應用程式的存取？		
7.59 是否指定專人管理應用程式原始碼、資料庫及執行檔？		
7.60 是否將應用程式原始碼、資料庫及執行檔分別存放？		
7.61 是否將開發中及正式作業之應用程式及資料庫分開存放及處理？		
7.62 是否將程式目錄清單、資料及相關電子檔作備份並異地存放？		
7.63 是否保有應用系統各種更新版本？		
7.64 機密及敏感性資料的處理是否於獨立或專屬的電腦作業環境中執行？		
7.65 例外事件及資訊安全事件是否建立紀錄？		
7.66 事件之記錄內容是否包括使用者識別碼、登入登出系統之日期時間、電腦的識別資料或其網址及事件描述等事項？		
7.67 對於系統存取異常時，是否留有紀錄並作必要處置？		
7.68 是否查核系統存取特別權限的帳號使用及配置情形？		
7.69 是否追蹤特定的系統存取？		
7.70 敏感性資料的存取情形是否留有紀錄？		

8 系統開發與維護

查　核　項　目	是	否
8.1 應用系統在規劃分析時是否將安全需求納入考量？		
8.2 安全控管方式是否採用系統自動控管及人工控管兩種方式處理？		
8.3 對高敏感性的資料在傳輸或儲存過程中是否使用加密技術？		
8.4 應用程式執行碼更新作業是否限定只能由授權的管理人員才可執行？		
8.5 有無建立應用程式執行碼的更新紀錄？		
8.6 系統變更後是否立即更新系統文件？		
8.7 版本更新是否保留舊版軟體及系統文件？		
8.8 是否避免以真實資料進行測試？如須用真實資料是否於事前將足以辨識個人身份的資料去除？		

8.9 開發、測試與正式作業是否分開使用不同主機？		
8.10 系統變更後其相關控管措施與程序是否檢查仍然有效？		
8.11 系統變更後，是否主動公告異動的範圍、時間、可能的影響？		
8.12 修改套裝軟體是否確認有無涉及廠商的版權問題？		
8.13 系統上線前是否檢查程式碼有無後門或木馬程式？		
8.14 系統安裝後是否管制程式碼？		
8.15 委外開發合約中是否對著作權之歸屬訂有規範內容？		
8.16 訂約時是否簽訂履行條款與相關罰則？		
8.17 是否定期對使用軟體實施病毒偵測？		

9 永續經營管理

查 核 項 目	是	否
9.1 是否已擬訂關鍵性業務及其風險評估、衝擊影響、優先順序？		
9.2 是否檢討業務停頓的企業損失和備援措施？		
9.3 是否指定適當層級主管負責永續經營政策之執行與協調？		
9.4 是否分析造成業務停擺的可能危機及損失？		
9.5 是否定期作風險評估並調整永續經營政策？		
9.6 永續經營計畫是否配合業務、組織及人員之變更而更新？		
9.7 是否建立資訊安全事件之通報作業程序及應變措施？		
9.8 是否訂有緊急應變計畫？		
9.9 緊急應變程序是否涵蓋有往來外單位之應變規劃？		
9.10 緊急應變程序是否設有對外發言的處理機制？是否結合相關單位及地方警消單位？		
9.11 緊急應變程序是否有異地場所、設備、處理程序及時限？		
9.12 緊急應變計畫是否定期演練與修正？		
9.13 緊急應變之作業程序與流程是否書面化？		
9.14 緊急應變計畫是否納入內部教育訓練？		
9.15 緊急應變計畫復原程序是否測試無誤？		
9.16 永續經營管理是否保持人員異動的取代更替？		
9.17 永續經營管理是否隨法令更新？		

10 內部稽查及其他

查 核 項 目	是	否
10.1 是否定期稽查資訊安全事項辦理情形？		
10.2 稽查範圍是否涵括資訊系統、供應商、資訊資產負責人、使用者和管理階層？		
10.3 是否訂有資訊安全作業稽查計畫(含稽查內容、範圍、程序、人員)，並公布？		
10.4 稽查人員是否經過訓練並作事前工作分配？		
10.5 稽查時是否需要額外的資源支援？		
10.6 稽查時的存取行為是否經過監控與記錄？		
10.7 稽查結果是否製成文件？		
10.8 稽查結果是否包括背景描述、稽查項目、過程、結果、改進建議等內容？		
10.9 是否清查過系統內與資訊安全相關的記錄檔案？10.10 與資訊安全相關的記錄檔案是否訂有保存規範？		
10.11 是否定期審閱資訊安全相關的記錄檔案？		
10.12 是否專人負責管理與資訊安全相關的記錄檔案？		
10.13 與資訊安全相關的記錄檔案是否足以追蹤駭客入侵的證據？		
10.14 是否使用合法軟體？		
10.15 是否訂有軟體採購作業程序？		
10.16 是否擬訂合法使用軟體規範及違規罰則，並作宣導？		
10.17 是否妥善保存授權證明、原版程式、使用手冊？		
10.18 對於以使用者人數為基礎的授權合約是否確實履行使用人數限制？		
10.19 是否確定個人電腦中只載入合法軟體？		
10.20 是否使用適當稽查軟體工具檢查所有個人電腦內使用之軟體？		
10.21 是否訂定軟體使用記錄和資料的儲存、處理和報廢的規則？		
10.22 是否訂定軟體使用記錄和資料的保存時限？		
10.23 是否建立軟體目錄？		
10.24 是否即時辦理軟體異動登記？		
10.25 是否指派專人負責有關個人資料保護法規之蒐集、公告、實施作為？		
10.26 是否依照「電腦處理個人資料保護法」規定辦理？		

表四、政府委託民營辦理計畫洩密通報表

填表日期：_____年____月____日

政府委託民營辦理法人（含自行研究計畫研究人員）、委託辦理之政府機關（含自行研究機關）及中央主管機關於洩密情形處理後，應填寫本通報表並函知相關機關（詳手冊陸、六、（四）之 7.）。

一、計畫名稱：_____

計畫編號：_____

二、通報基本資料（若有”□可能或□確定”之選項，請勾選” ☑”其一）

（一）填表人姓名：_____

服務單位名稱：_____

聯絡電話：_____

（二）機密資料洩漏之時間（□可能或□確定）為：_____

_____

發現機密資料洩漏之時間：_____

填表人得知機密資料洩漏之時間：_____

（三）機密資料洩漏之場合（□可能或□確定）為：_____

_____

_____

（四）發現機密資料已洩漏之人員：

姓名：_____

服務單位名稱：_____

聯絡電話：_____

（五）機密資料洩漏之可能地點：_____

發現機密資料洩漏之地點：_____

（六）機密資料（□可能或□確定）洩漏予何人（單位）：

_____

（七）洩漏之機密資料機密等級：（請勾選” ☑”，可複選）

□機密 □極機密 □絕對機密

三、請詳述為何會洩漏機密資料：

四、請詳述洩漏之機密資料內容：

五、請詳述本洩密事件之嚴重性（對經濟發展、對科技實力及對其他國家安全事項等之影響）：

六、請詳述洩密事件發生後本機關之處理過程：

七、請詳述洩密事件發生後之保密改進措施：

填表者簽章：_____ 日期：_____

表五、政府委託民營辦理計畫違常案件通報表

填表日期：_____年____月____日

政府委託民營辦理法人（含自行研究機關）於違常案件處理後，應填寫本通報表送主管機關討論。

一、違常案件基本資料：

1.計畫名稱：_____

2.計畫編號：_____

3.洩漏之機密資料機密等級：(請勾選" ☑"，可複選)

□機密 □極機密 □絕對機密

4.委託機關：_____

5.中央主管機關：_____

6.填表人姓名：_____

服務單位名稱：_____

聯絡電話：_____

二、洩密發生經過（相關機關、人、事、時、地）

三、請詳述洩漏之機密資料內容：

四、請詳述本洩密事件之嚴重性（對經濟發展、對科技實力及對其他國家安全事項等之影響）：

五、請分別詳述洩密機關與政府委託機關於洩密事件發生後之處理過程：

六、請分別詳述洩密機關與政府委託機關於洩密事件發生後之保密改進措施：

填表者簽章：_____ 日期：_____

表六、設施安全認證表

設施安全認證表

法人名稱：
營利事業登記證號碼：
設施名稱：
設施性質：
設施地址：
電話：
傳真：
接觸使用保密資訊之等級：□絕對機密 □極機密 □機密
是否獲得其他單位之設施安全認證？□否 □是 名稱：
認證機關：

查核項目	是	否	狀況描述／備註
法人經營安全			
1．該法人是否曾經違反任何法令而遭起訴？			
2．承上題，如回答是，請舉出遭起訴之理由。			
3．該法人是否曾申請設施安全認證遭拒？			
4．承上題，如回答是，請列舉遭拒之原因。			
5．該法人之外資百分比			
6．經營高層（經理以上）外籍人士之比例			
7．公司經理級以上之員工名單（需註明姓名、地址、身份證號碼、國籍、其他兼職等）			
8．法人經營高層是否通過人員安全認證？			
9．接觸保密資訊之人員是否通過人員安全認證？			
10．法人財務是否健全？			

建物實體安全認證			
1．設施藍圖規劃是否符合建築安全法規？			
2．消防設備是否配備足夠？			
3．高樓層是否具備自動灑水系統？			
4．建物是否經過耐震考驗？			
5．建物主牆厚度是否足以承受高溫？			
6．建物是否具有良好排水系統，足以防範水災？			
7．是否提供足夠之避難與安全規劃？			
8．其中之工作人員是否具有足夠之安全與操作知識？			
9．工作人員是否定期接受安全教育？			
門禁措施查核			
1．是否聘請專業保全人員			
2．是否裝置保全防盜系統			
3．是否配置人員出入辨識（含刷卡、指紋辨識、聲控或者瞳孔辨識等）系統			
4．是否配置監視器錄影系統			
5．是否定期舉辦無預警門禁突破演練			
6．是否定期或不定期與辦保全人員、總機人員 清潔人員對於資料保密之教育訓練			
7．所有出入紀錄應保存三年以上			
儲存機密資料之場所與容器安全			
1．安全程序計畫			
2．儲存機密資料之空間與容器是否通過國家檢驗？是否防火、防水、耐震			
3．是否定期檢查所有鎖具之安全、鑰匙是否有妥善之保管方式？			
需繳交之附件：			
公司或法人登記證明影本			
經理級以上之人員名單及資料			
法人之年報、公司營運報告			

股東大會紀錄與財報			
建物藍圖			
設施安全維護計畫			

行政院國家科學委員會補助專題研究計畫■ 成 果 報 告
□期中進度報告

非公務機關（人員）安全查核制度

計畫類別：□ 個別型計畫　　□ 整合型計畫　□ 其他補助計畫
計畫編號：NSC 92－2745－P－009－001－
執行期間：92 年 8 月 1 日至 92 年 11 月 30 日

計畫主持人：交通大學電信工程系教授　闕河鳴
共同主持人：交通大學電機與控制工程學系教授　楊谷洋
　　國防大學軍事學院教授　廖宏祥
計畫參與人員：

成果報告類型(依經費核定清單規定繳交)：□精簡報告　■完整報告

本成果報告包括以下應繳交之附件：
■赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：交通大學電信工程系

中　華　民　國　九　十　二　年　十　二　月　五　日

赴國外出差（研習）心得報告

報告撰寫人：張棋炘

一、 國外出差行程安排：

本次出國預定目的地爲美國華府，總行程時間含括飛行時間共計七天整（十一月十九日至十一月廿五日）。不過由於飛機飛行時間延誤，以致於被迫停留於紐約甘乃迪機場住宿一晚，實際停留華府時間乃因此縮減爲三天（十一月廿一日至時一月廿三日），住宿地點則爲華府 Dupont Circle 附近之 Radison Barcelo 旅館。

就本次差旅行程目的而言，由於本次行程安排較爲匆促，並無法順利就美國從事安全查核之相關官方人員進行會面安排，所以此行的目的乃主要爲前往美國國會圖書館進行資料蒐集，特別是針對「設施安全查核」（Facility Clearance）層面的資料蒐集。。

二、 資料蒐集情形：

在抵達華府當日下午，隨即利用住宿旅館所提供之旅遊資訊，確認國會圖書館之所在位址。並於廿一日（五）、廿二日（六）進行爲期兩天的資料訪查。

美國國會圖書館藏書之豐富爲舉世聞名，佔地遼闊，主體共分爲三大建物，分別是 Jefferson Building、Adams Building 以及 Madison Building。進入國會圖書館便即可感受其對全世界所有人（包括研究者與觀光客）開放的便利服務，不過伴隨著這項便利服務的同時，美國國會圖書館對於進入的人員卻也採取了相當高程度的安全查核措施，包括研究者與觀光客的基本區別、進入建物過程的安全檢查以及任何欲進入圖書室之前的事前咨詢服務。

比較令人意外的是，在經過兩天的查訪之後，從國會圖書館當中確實可以搜尋到相當豐富的有關「安全查核」方面的資料，但是這些資料卻幾

乎都集中在「人員安全查核」以及「資訊安全查核」兩個層面，在「設施安全查核」方面可以說是付之闕如。不論是電子格式的資料或者是圖書期刊方面的資料都是如此，對此行的主要目的可以說是一個相當大的挫折。

經過與國會圖書館方面的人員進行諮詢與雙重確認之後，確定國會圖書館目前所蒐錄的資料當中，並沒有包括所謂的「設施安全查核」資料。雖然透過國會圖書館電腦查詢到部分設施安全查核資料檢查表，不過這些資料表幾乎都隸屬於美國軍方單位，而且由於其可檢索期限都已經過期，也都已經被美國軍方單位移除。最後國會圖書館的館員還是建議本人利用網路搜尋引擎（如 Google 等）以確認是否有可行的其他途徑來檢索可能的設施安全查核資料。

三、 結論

此行的主要目的可以說並沒有順利達成，不過從另外一個角度來看，這也顯示出「設施安全查核」即使是在規範相當完善的美國也還是相當新的一個項目，也顯示非從事此一領域的人員對這個項目依然相當的陌生。據此，我們可以說，台灣在這方面如果能夠對此一項目投注更多的研究、並具體實行，對於未來引進更多非公務機關及人員從事與國家安全相關之研究必能提供相當的助力。