法務部廉政署
「世界主要國家之國家安全及國家機密維護法令與措施比較分析」
委辦計畫案

研究成果報告書

財團法人資訊工業策進會

日期：102 年 07 月

目錄

表目錄

圖目錄

法務部廉政署「世界主要國家之國家安全及國家機密維護法令與措施比較分析」委辦計畫案基本資料表

表 1：法務部廉政署「世界主要國家之國家安全及國家機密維護法令與措施比較分析」委辦計畫案基本資料表（本表年份為民國）

契約期限	**101 年 8 月 14 日至 102 年 8 月 13 日止**
契約金額	**新台幣 1,050,000 元整（含稅）**

一、期中報告、期末報告（含研究成果報告）

■ 執行成果詳閱本計畫期中報告、期末研究報告

NO	履約項目	契約規格要求	本所執行成果	審查會議來函	審查會議結論	本所印製交付
1	繳交期中報告	(1) **101 年 12 月 28 日前**，提出期中報告初稿 **1 式 15 份**。 (2) 依廉政署審查意見及所訂期限內補充、修正及說明，**經廉政署**	**101 年 12 月 12 日**以（101）資法字第 1011006775 號函，檢送期中報告初稿 **1 式 15 份**。	101 年 12 月 20 日廉政字第 10100107720 號函，於 101 年 12 月 25 日完成期中審查會議。	廉政署 101 年 12 月 26 日廉政字第 10107006200 號函指示：依本次會議審查委員意見（含書面審查	**102 年 1 月 4 日**以（101）資法字第 1011007411 號函，**印製交付期中報告定稿 1 式 6 份**。

		審查通過後 10 日內（自審查會議之日或書面發文日起算），**印製交付期中報告定稿 1 式 6 份**。			意見），先行修正期中報告後，於 102 年 1 月 4 日（星期五）前將修正定稿版（1 式 6 份）函送廉政署署，辦理後續事宜。	
2	繳交期末報告（含研究成果報告）	(1) **102 年 8 月 13 日前**，提出期末報告**初稿 1 式 15 份**送廉政署審查。 (2) 經廉政署**審查通過後 10 日內**（自審查會議之日或書面發文日起算），**印製交付研究成**	**102 年 7 月 29 日**以（102）資法字第 1021003693 號函，檢送期末研究報告**初稿 1 式 15 份**。	102 年 8 月 12 日廉政字第 10207003010 號函，於 102 年 8 月 12 日完成期末報告審查會議。	廉政署 102 年 9 月 9 日廉政字第 10207004150 號函指示，依委員意見修正及回應說明後，並依本案契約第 5 條第（一）款第 3 目，	**102 年 9 月 16 日**以（102）資法字第 1021004570 號函，**印製交付期末研究報告定稿 1 式 50 份及電子檔光碟 2 片**。

		果報告書1式50份及製作報告書電子檔光碟2片。			**機關發文日10日內**，辦理後續履約及第3期款驗收等事宜。	

二、專題分析報告及廉政署指定重要議題分析報告

■ 執行成果詳閱期末報告上冊「附錄一、計畫成果 - 專題分析報告及重要議題分析報告」。

NO	履約項目	契約規格要求	本所執行成果	本所交付初稿日期	廉政署審認日期
3	專題分析報告	「議價條件」單第2點，每篇字數**至少需達5,000字以上。無單獨印製紙本需求。**	‧報告題目：公務機關電子機密資訊系統面對內部威脅之作法。 ‧報告字數：**12,156字**。	101年12月6日，(101)資法字第1011006681號函，檢附**報告紙本一式10份**。	102年1月30日，前廉政署胡專員Email審認通知。
			‧報告題目：為維護國家安全並因應資通安全政策之資訊業務採購評選廠商標準—以廠商人力來源之背景安	101年12月6日，(101)資法字第1011006681號函，檢附**報告紙本一式10份**。	102年1月30日，前廉政署胡專員Email審認通知。

			全查核為核心。 ·報告字數：**6,741 字**。		
			·報告題目：智慧電網安全維護報告。 ·報告字數：**14,478 字**。	102 年 3 月 1 日，(102)資法字第 1021000788 號函，檢附**報告紙本一式 2 份**。	102 年 5 月 14 日，前廉政署胡專員 Email 審認通知。
			·報告題目：涉密公務人員退離職後之保密。 ·報告字數：**10,672 字**。	102 年 5 月 29 日（102）資法字第 1021002546 號函，檢附**報告紙本一式 2 份**。	102 年 7 月 16 日，前廉政署胡專員 Email 審認通知。
			·報告題目：機關安全維護之研析－以實體設施及人員安全維護為核心。	102 年 6 月 24 日（102）資法字第 1021003001 號函，檢附**報告紙本一式 2 份**。	102 年 7 月 16 日，前廉政署胡專員 Email 審認通知。

			·報告字數：**17,095 字**。		
4	重要議題分析報告	(1) 依廉政署指定及審認，撰寫重要議題分析報告至少 2 篇。 (2) 「議價條件」單第 2 點，每篇字數**至少需達 5,000 字以上**。**無單獨印製紙本需求**。	·報告題目：論機關公務機密之保護-以因應個人資料保護法之修正為中心。 ·報告字數：**11,246 字**。	102 年 3 月 1 日，(102)資法字第 1021000788 號函，檢附**報告紙本一式 2 份。**	102 年 5 月 14 日，前廉政署胡專員 Email 審認通知。
			·報告題目：「論我國公務機關解決公務機密核密等級與解密程序爭議之思考 – 以美國國防部與美國國土安全部公務機密管理機制為例」。 ·報告字數：**15,016 字**。	102 年 5 月 15 日，(102)資法字第 1021002299 號函，檢附**報告紙本一式 2 份**。	102 年 7 月 3 日，前廉政署胡專員 Email 審認通知。
三、舉辦焦點座談 ■ 執行成果詳閱期末報告上冊「附錄二、計畫成果 - 公務機關機密與機敏資訊維護焦點座談」。					

NO	履約項目	契約規格要求	本所執行成果
5	舉辦焦點座談	「議價條件」單第 3 點，本活動均須於活動前 2 月提送廉政署審認確定後，方得辦理： (1) 辦理時間：於**期末報告完成前舉辦 1 場**焦點座談。 (2) 參與對象：邀請與國家安全及機密維護議題相關之政府機關、專家學者代表出席與談，**至少 6 人以上**（不含廉政署出席人員）。 (3) 活動規模：焦點座談之活動規模，**至少應達 3 小時以上，討論議題至少 2 項以上**。	(1) **102 年 5 月 20 日**，假資策會科法所行遠講堂舉辦 1 場「**公務機關機密與機敏資訊維護焦點座談會**」。 (2) 邀請**8 位**[1]政府機關、專家學者代表出席與談。 (3) 焦點座談活動時間為**下午 2 點至 5 點（3 小時）**；討論議題為 **2**： A) 公務機關機敏資訊之安全維護。 B) 密等核定與解密適當性之查核或檢核機制。
四、編撰維護雙週報 ■ 執行成果詳閱期末報告下冊「附錄三、計畫成果 - 資訊雙週報」。			
NO	履約項目	契約規格要求	本所執行成果

[1]行政院勞工委員會政風室王偉松主任、法務部法律事務司李世德科長、國家通訊傳播委員會政風室李志強科長、臺灣大學電機工程系暨研究所蔡志宏教授、世新大學法學院段重民教授、中正大學財經法律學系黃俊杰教授、中原大學法學院陳櫻琴教授、高雄大學政治法律學系楊戊龍教授。

5	編撰維護雙週報	(1) 依本計畫需求書所列範圍[2]，篩選維護政策有關重要資訊（含譯稿），摘譯成中文，定期編輯重要國際維護訊息週報雙週報（**每期 1,000 字以上**）。 (2) 資料來源應隨譯文詳附於後，每期內容至少包含 10 則資訊譯稿量（各種類別至少 1 則，各則內容須通過機關審核認可）。另針對機關指定之重要事件發展，應予以後續追蹤。 (3) 依「維護雙週報履約管制表」表定管制時間繳交，最終期雙週報應於 **102 年 8 月 14 日**完成繳交。 (4) 需求書第參條第三項要求以「**電子郵件方式**」更新。	(1) 資策會科技法律研究所（下稱本所）依左列第（1）點要求，定期編輯重要國際維護訊息週報雙週報，平均**每期譯稿 9,000 字以上**。 (2) 本所依左列第（2）點要求，每期均提供 10 則資訊譯稿量，**平均一個主題即含 2 則資訊譯稿**，並依廉政署審查意見，完成修正、追蹤及意見回覆。 (3) 本所依左列第（3）點要求，於 **102 年 6 月 21 日**完成最終期雙週報繳交。 (4) **配合廉政署指示，繳交各季雙週報彙編紙本：** A) 第 1 季雙週報彙編：第 1~6 期，共 206 頁，印製 15 冊。 B) 第 2 季雙週報彙編：第 7~12 期，共 219 頁，印製 15 冊。

[2]蒐集世界主要國家及機構近 3 年國家安全（含機關安全）及機密維護之網路及平面資訊，對象包括美、日、南韓、新加坡、澳洲、英、歐盟、中國、OECD、APEC 等主要國家及國際組織相關機構。計畫主題應涵蓋國家安全、國家機密維護、機關安全維護、機關公務機密維護、資（通）訊安全等相關類別或主題。

			C) 第 3 季雙週報彙編：第 13~20 期，共 278 頁，印製 15 冊。 D) 第 4 季雙週報彙編：第 21~26 期，共 252 頁，印製 15 冊。

資料來源：本計畫整理

中文摘要

近來伴隨資通訊技術的進步，新型態恐怖攻擊手法不斷推陳出新，資安攻擊事件頻傳，再加上人民知的權利與機密保護的界線漸進模糊，洩密與安全事件迭起，實已嚴重危及國家（公務）機密之保護與國家（機關）安全及之利益。法務部廉政署依其法定業務執掌，為即時掌握世界主要國家及機構有關國家（機關）安全，及國家（公務）機密維護最新法令措施與因應作法之發展趨勢，以資料蒐集為研究方法，建立國家（機關）安全，及機密維護資料庫為目的，委託財團法人資訊工業策進會科技法律研究所(下稱本所)執行「世界主要國家之國家安全及國家機密維護法令與措施比較分析」委辦計畫案。

本計畫以「國家安全」、「國家機密維護」、「機關安全維護」、「公務機密維護」，及「資通（訊）安全政策」5 大議題為主軸，從法律面、制度面，與技術面等 3 大構面進行資料蒐集與議題歸納整理，篩選具參考價值之法令政策或因應措施等資訊加以編譯，更進一步選擇國際或國內特別關注之事件類型或議題做為專題進行研究，配合訪談其他公務機關了解國內法制和因應作法,並透過舉辦焦點座談會,邀請專家，進行法制措施與政策作法的比較分析，提出具體業務之發展趨勢與政策建議。

本計畫執行團隊發現，國家安全、機關安全、國家機密維護、公務機密維護與資通訊安全政策 5 大研究議題就像是一個五角形的蜘蛛網路，各個議題是單獨的點，而各議題間

又可以資通訊技術作為連結。表面上各議題看起來似乎可各自成立,但卻又彼此受到影響與牽制,無法僅規制單一議題，即可達成完全的解決方案，即所謂牽一髮而動全身。資通訊技術導入業務與服務的運作，帶動政府與民間企業的電子化，固然使效率提升，但同時也因為涉及國家（機關）安全與機密維護的人員與事務的繁雜與大幅增多，風險因此而加乘。不過,就如連結縱線的蜘蛛網路,對於安全與機密資訊維護，也可藉由橫線的資通訊科技技術，發現弱點與風險因子，而加以防範與加強防護。

本計畫建議我國政府如欲建構完善、細緻、具前瞻性的整體安全維護策略架構，實應對特定議題採取長期監測性的觀察、研究與分析，進行有效的總體規劃，方能提供資源之整合及跨部會協調，也藉由議題的歸納研析，俾利主管機關得以統一解釋與進行權責分配，並得辦理監督國家之整體性政策、措施與作法等工作。目前立即可行之作法，則建議從整頓現行法制架構著手，蒐集並整合所有政府機關相關之行政規則及行政指導文件，檢討相關之法律、法規命令、解釋性規定及裁量基準，是否已落實明確性原則而無賦予各機關過度的裁量空間,並參考先進國家所開放之政策、制度文件，與相關作法，集中現行各安全維護議題之主管機關的能量，力行跨部會合作，建構我國之安全維護政策框架。

關鍵詞：國家安全、國家機密維護、機關安全維護、公務機密維護，及資通訊安全政策

Abstract

With the progressive development of the ICT, multiplying the new forms of terrorist attack and APT（Advanced Persistent Threat）. The gradually fading and blurring boundaries between the freedom of information and the protection of the classified information also worsen the situations of leaks and security breach, which has really become serious threat to the protection of classified information and official secrets, and put the interests of national security at risk.

In order to understand the national security, security of the agencies, protection of classified information, protection of official secrets and ICT security policy, related legislation, policies and practices of other countries, “Agency Against Corruption （AAC）” delegated the “Institute for Information Industry（III） Science & Technology Law Institute （STLI）” to execute “ The Comparative Legal Studies on the Protection of National Security and Classified Information” Project.

This project was conducted under five major themes, including "national security", "security of the agencies", "protection of classified information", "protection of official secrets" and "ICT security policy" as the research spindle and exams each themes in legal, institutional and technical aspects.

After closely and carefully reviewing the literatures with

the content of legislature, policies and practice of other countries, the research team then translates and edits the content to buildup the Literature Database.

In furtherance, the research team selects important issues or incidents as the topics of seven Special Reports and conducts comprehensive analysis and comparison of the legislations, policies and practices of other countries, holds one “Protection and Safeguarding the Security of Official Secrets and Sensitive Information” Symposium, by inviting experts in the government agencies to put forward viable and important legal and policy recommendations.

During the research, the research team finds these five research themes are just like a five pentagonal spider web, each theme seems can be standing alone; instead, with the introduction of the ICT into the everyday business practice and services of the government agencies, each theme is actually relates to and depends on one another. Due to the characteristics of the ICT, the complex personnel and activities might increase the level of the venerability; however, the application of the ICT can be the tool to fight against the security threats, to hold each other to be a strong web. It is the same case in the co-operation among the five themes; all themes have to work together and work balancedly to reach the ultimate goal of the protection of national security and classified information.

In order to construct a complete, detailed, and

forward-looking, but does not cause excessive burdensome protective security policy framework, in the long term approach, it is recommended to select critical issues based on priority, and take in-depth research and analysis to do effective and overall planning in the resource integration and inter-ministerial coordination. Provided, to carry out the consistent interpretation of codes and regulations, allocation of the rights and responsibilities, and conduct supervision of the country integration and inter-ministerial coordination to fulfill the ultimate goal to have consistent internal security and the classified information protection policy framework.

In the short-term, it is recommended to review the existing legal framework, proceed from the collection and organization of the relevant official documents, including laws and regulations, orders and administrative rules, guidance and standards; then to further exam whether the agency has been properly authorized with plenty of room for discretion; in conclude, the Government shall gather the strength of the intelligence and security related authorities, implement the inter-ministerial cooperation, with the goal to build our country's protective security policy frameworks with reference to the public policy and practices of advanced countries.

Keyword： National Security, Security of the Agencies, Protection of Classified Information, Protection of Official Secrets, and ICT Security Policy

壹、計畫緣起

自美國 911 事件之後，各國恐怖爆炸攻擊事件頻傳，利用資通訊科技之攻擊手法不斷推陳出新，國家、機關與人員安全遂受高度重視，各國政府紛紛構思強化相關的安全政策與因應作法，積極防範恐怖主義的蔓延與恐怖事件的發生，我國的安全政策也面臨恐怖主義的新威脅，實有重新檢視的必要。

復因政府機關業務的運作與服務的提供，使得政府機關成為掌握全國最完整、多元與龐大的資訊來源，政府機關於一方面為龐大與種類繁多資訊的產製與處理者，另一方面也擔負著維護與管理的責任。隨著資通訊技術導入政府機關，政府業務的電子化，使得涉及的業務、事務、人員與系統設備等的維護管理責任，更形交錯綜雜。再加上言論自由與機密保護，知的權利與界線漸進模糊，洩密及資安事件迭有發生，對於資訊的安全與機密的維護，實已嚴重危及國家安全與機關安全及其利益。

法務部廉政署為即時掌握世界主要國家有關國家（機關）安全，及機密維護的最新法令措施與因應作法之發展趨勢，作為推動國家（機關）安全及機密維護法令與措施之參考，委託財團法人資訊工業策進會（下稱本會）執行「世界主要國家之國家安全及國家機密維護法令與措施比較分析」委辦計畫案（下稱本計畫）。

貳、計畫目的

瞭解世界主要國家及機構（包括：美、日、南韓、新加坡、澳洲、英、歐盟、中國、OECD、APEC 等主要國家及國際組織相關機構），近 3 年有關國家安全（含機關安全）及機密維護相關法令與措施之發展趨勢。透過資料收集研究之方法，系統性、持續性蒐集有關國家安全、國家機密維護、機關安全維護、公務機密維護及資通（訊）安全政策之相關資料，以建立公務機密維護及機關安全維護之資料庫。

另配合委託機關之需求，經由專題分析報告與指定重要議題分析報告對於國際或國內特別關注之事件類型或議題進行深度研究與探討，並以舉辦焦點座談方式廣徵各界意見，針對公務機密維護及機關安全維護之法制及實務現況提出全面評析與探討，期對維護業務提出具體之政策評估與建議。

參、研究方法與進度說明

本計畫研究範圍以國家安全、國家機密維護、機關安全維護、機關公務機密維護、資通訊安全等 5 大議題為主軸，從法律面、制度面，與技術面就國家安全及國家機密相關法令及資訊進行資料蒐集，而後進行資料之比較分析，並配合委託單位之需求，就國內目前相關政策或法制規範待討論之處，舉辦焦點座談會，並參酌與會專家之各項建議，綜整政策與策略方向。

一、研究範圍

（一）國家安全

包括國土安全層次之反恐政策或措施；國家元首、外國元首及使館安全措施；危及社會經濟穩定、金融秩序、生態環境、資源安全、重大爆炸事件、疾病蔓延及跨國重大經濟犯罪等天然、人為及科技之災害等相關資訊。

（二）國家機密維護

包括竊取國家機密事件始末及洩密管道；軍事、國防機密資訊之維護措施；政府通信、資訊保密技術、設備或設施；為確保涉及國家安全或利益之機敏資料之措施等相關資訊。

（三）機關安全維護

包括危害機關或關鍵基礎設施之爆炸、破壞事件；偶突發意外事故、機關首長安全、重大陳抗事件；選舉或重大節慶期間之安全維護等相關資訊。

（四）公務機密維護

包括重大洩密案件、機敏資料、資（通）訊設備維護措施等相關資訊。

（五）資通訊安全政策

包括駭客網路攻擊事件及其發展趨勢（如社交工程、封包攻擊...等）、資安及通訊洩密事件、網路安全設備、最新病毒資訊、資訊網路安全政策、最新資訊安全認證、防火牆及措施等相關資訊。

二、研究方法

本計畫之研究方法以各國資料蒐集為主要基礎，將與議題相關之資訊進行內容之分類篩選與歸納整理，編撰國際維護訊息雙週報；檢視與選擇特別受到國際或國內關切的議題做為專題，進行國外與國內法制與作法資料蒐集與比較分析，並提出建議或可行作法以供參考。另外，針對目前政府機關所遭遇之機密維護議題，以舉辦焦點座談等方式進行研究，最後，針對我國國家（機關）安全、國家（公務）機密維護、資通訊安全政策，提出趨勢發展的政

策建議或可行的作法。詳細內容將分述於下列說明：

（一）國際維護訊息雙週報（請參見附錄三、計畫成果 - 資訊雙週報）

蒐集世界主要國家、機構及國際組織（例如：美、日、南韓、新加坡、澳洲、英、歐盟等）近 3 年有關國家安全（含機關安全）及機密維護相關法令與措施之網路及平面資訊，摘譯與編輯為每期 10 篇共 26 期（260 篇）之國際維護訊息雙週報。

資訊的蒐集主要分為含法制作法的最新新聞資訊與各國法令措施或具體政策兩類。新聞事件提供對於最新事件的趨勢與因應作法的掌握，介紹事件發生的背景、相關事實、法制或因應作法，以及評論；另一則以國家（機關）安全、國家（公務）機密維護、資通訊安全政策議題為主，將主要國家已經具體成形之法令措施或具體政策的文件，提供較為完整與詳細的內容。另針對機關指定之重要事件發展，予以後續追蹤。每則國際維護訊息雙週報內容需通過機關審核認可，並於每季提交季報。

表 2：資訊雙週報新聞所涉政策或法律議題歸納表

計畫主題類別	所涉 政策或法律 議題
國家安全	（1）反恐及國家安全法規、行政命令、政策、戰略之發布、檢視與修正 ● 資訊雙週報期數：02-06、05-01、06-01、06-02、06-03、07-03、08-02、08-01、08-03、09-01、10-01、10-02、11-01、12-01、12-02、13-01、14-01、15-01、15-03、16-01、17-01、17-02、18-01、18-02、19-01、19-02、20-01、20-02、21-01、21-02、22-02、23-01、23-02、24-01、24-02、26-01 （2）國家安全團隊之設置 ● 資訊雙週報期數：11-02、25-02、 （3）本國及跨國反生物武器威脅監測策略 ● 資訊雙週報期數：02-02、02-04、08-06、 （4）政府擬定「極端氣候之防災管理政策」，並與私人企業、人民共同進行極端氣候災害應對及演習 ● 資訊雙週報期數：02-10、03-05、04-09、

	（5）全國性緊急事故警報系統之設置 ● 資訊雙週報期數：07-02 （6）國土安全之跨境合作政策 ● 資訊雙週報期數：03-07、04-10、
國家機密維護	（1）國家機密維護專責部門之建立 ● 資訊雙週報期數：09-03 （2）國家機密維護之跨境合作政策 ● 資訊雙週報期數：10-03、11-03 （3）軍事人員使用智慧行動裝置之管理政策 ● 資訊雙週報期數：01-04、03-10 （4）情報人員將不得以匿名之方式接受媒體訪問並提出評論 ● 資訊雙週報期數：01-09 （5）就涉及國家機密之訴訟案件，擬以「不公開審理」之方式進行 ● 資訊雙週報期數：01-01、23-03、24-03 （6）「未經授權揭露國家機密資料」事件之應變政策

	● 資訊雙週報期數：03-03、08-08、12-03、26-03、 （7）「未經授權揭露國家機密資料」事件衍生爭議： （A）其訴訟應由普通法院或軍事法院審理？ ●資訊雙週報期數：05-08、 （B）「未經授權揭露」（Unauthorized Disclosures of Classified Information）與「揭弊者」（Whistleblower）之爭 ●資訊雙週報期數：04-07、07-04、07-08、07-09、08-04、09-02、18-05、19-03、20-03、22-03 （8）國家機密維護法規、行政命令、政策之發布、檢視與修正 ● 資訊雙週報期數：13-03、14-03、15-04、16-04、17-03、18-04、19-04、20-04、21-04、21-05、22-04、23-04、24-04、25-01、25-04、26-04
機關安全維護	（1）整合區域性的機關維安監控系統

	● 資訊雙週報期數：01-02、 （2）關鍵基礎設施業務運作之持續性 ● 資訊雙週報期數：13-05、16-02、18-03、20-06、24-05、26-05 （3）機關整體安全應變政策或計畫 （A）政策、計畫之訂定、檢視及修正 ● 資訊雙週報期數：05-02、06-01、06-07、07-06、07-07、09-04、09-05、09-06、10-04、10-06、11-05、11-07、11-08、12-05、14-06、15-06、21-07、22-06、23-07、25-05 （B）機關安全維護意識教育及稽核 ● 資訊雙週報期數：07-01、10-05、12-06、12-07、25-06 （C）對「人員之身分辨識、背景查核」之管理 ● 資訊雙週報期數：01-08、17-05、17-06、18-07、19-06、22-01、26-06 （D）對「建築物主體及周邊硬體設施」之風險評估、維安管理

	● 資訊雙週報期數：02-01、03-06、04-01、07-05、13-06、14-07、23-06、24-06、26-07 （E）對機關內部「紙本檔案、電子檔案安全」之管理 ● 資訊雙週報期數：15-07、16-07、26-06、26-07、 （F）機關間之合作協力、資源共享 ● 資訊雙週報期數：08-05、13-04、14-05、15-05、16-05、17-04、18-06、19-05、20-05、21-06、22-05、23-05
公務機密維護	（1）公務機密維護法規、行政命令、政策之發布、檢視與修正 ● 資訊雙週報期數：08-07、10-08、12-08、12-09、13-08、13-09、14-08、14-09、15-08、16-08、16-09、17-07、17-08、18-08、18-09、19-07、19-08、20-07、21-08、22-07、23-08、23-09、24-07、24-08、25-08、26-08、 （2）公務人員攜帶自有裝置之管理政策 ● 資訊雙週報期數：02-03、22-09

	（3）涉及個人資料之公務機密資料保護 ● 資訊雙週報期數：06-08、09-07、10-07、21-09、22-08、25-07、26-07、 （4）機密之分級，不凌駕法律之上、可受法院審視 ● 資訊雙週報期數：13-07、14-04、19-09、 （5）公務機密維護之跨境合作政策 ● 資訊雙週報期數：16-06 （6）跨政府組織擬統一各會員國國內內部公務檔案安全規則 ● 資訊雙週報期數：05-09
資通（訊）安全政策	（1）政府機關擬就官方網站、資訊系統、適用資安標準進行管理、更新 ● 資訊雙週報期數：01-07、03-02、10-10、20-09 （2）政府機關擬單獨、或與私人企業機構合作，進行網路監控 ● 資訊雙週報期數：01-05、01-10、02-05、05-05、05-10、13-02、14-02、15-02、15-09、17-09、25-03、26-02

	（3）政府機關跨部會、或與私人企業機構合作，共同執行網路安全防禦與資料保護 ● 資訊雙週報期數：02-07、02-09、03-04、21-10、 （4）政府機關跨部會、或與私人企業機構合作，進行網路安全威脅應對及演習 ● 資訊雙週報期數：04-03、05-06、06-06、06-10、11-09 （5）進行全面的國家資通（訊）安全性檢視 ● 資訊雙週報期數：03-08、04-02、07-10、07-11、08-09、09-10、10-09、13-10、14-10、23-10、24-10、25-10、26-10 （6）資通（訊）安全法規、行政命令、政策之發布、檢視與修正 ● 資訊雙週報期數：01-03、03-01、03-09、04-05、04-06、05-03、06-09、09-08、11-10、12-10、15-10、16-10、17-10、18-10、20-10、22-10、24-09、26-09

資料來源：本計畫整理

（二）專題分析報告及重要議題分析報告（請參見附錄一、計畫成果 - 專題分析報告及重要議題分析報告）

以國家（機關）安全、國家（公務）機密維護、資通訊安全政策為主議題，檢視與選擇特別受到國際或國內關切的子議題，撰寫共 5 篇專題分析報告，及 2 篇重要議題分析報告。

專題分析報告題目、大綱、訪談題綱由研究團隊與諮詢顧問做初步研究後提出，經機關核可後進行訪談，以獲得國內政府機關不對外公開的機制或作法，研究團隊就國內外資料與訪談內容，進行蒐集與比較分析，提出結論與建議，並需通過機關審核認可。

表 3：專題分析報告及重要議題分析報告主題表（本表年份為民國）

編號	主題	交付日期	審認日期
專題分析報告 5 篇			
1	公務機關電子機密資訊系統面對內部威脅之作法	101/12/06	102/01/30
2	為維護國家安全並因應資通安全政策之資訊業務採購評選廠商標準 – 廠商人力來源之背景安全	101/12/06	102/01/30

編號	主題	交付日期	審認日期
	查核為核心		
3	智慧電網安全維護報告	102/03/01	102/05/14
4	涉密公務人員退離職後之保密	102/05/29	102/07/16
5	機關安全維護之研析－以實體設施及人員安全維護為核心	102/06/24	102/07/16
重要議題分析報告 2 篇			
1	論機關公務機密之保護-以因應個人資料保護法之修正為中心【焦點 1】	102/03/01	102/05/14
2	「論我國公務機關解決公務機密核密等級與解密程序爭議之思考 – 以美國國防部與美國國土安全部公務機密管理機制為例」【焦點 2】	102/05/15	102/07/03

資料來源：本計畫整理

（三）「公務機關機密與機敏資訊維護」焦點座談會

（請參見附錄二、計畫成果 - 公務機關機密與機敏資訊維護焦點座談會）

本計畫於 2013 年 5 月 20 日於本所行遠講

堂，以「公務機關機敏資訊之安全維護」及「密等核定與解密適當性之查核或檢核機制」2 項議題為主題，邀請國家安全及機密維護議題相關之政府機關、專家學者代表，針對前揭議題進行深入討論與建言，並因應政府機關實務作業需求，檢視現行公務機關機密與機敏資訊的維護分級系統與相應的分級處理程序、安全維護措施與其他配套措施，以建立符合我國國情、完善機密維護保護法規、措施與機制，提升行政機關對資訊敏感度判斷的能力、減少不必要維護成本的支出。

焦點座談會的舉辦，配合重要議題分析報告議題的撰寫，產出「公務機關機敏資訊之安全維護」及「密等核定與解密適當性之查核或檢核機制」兩份簡報，與座談會會議紀錄 2 份。

*焦點座談會專家學者名單、簡報及專家學者建言之紀錄，請詳閱附錄二、計畫成果 - 公務機關機密與機敏資訊維護焦點座談會。

三、進度說明

表 4：計畫執行進度表（本表年份為民國）

時程 工作內容	101 年 08 月	101 年 09 月	101 年 10 月	101 年 11 月	101 年 12 月	102 年 01 月	102 年 02 月	102 年 03 月	102 年 04 月	102 年 05 月	102 年 06 月	102 年 07 月	102 年 08 月
26 期資訊雙週報	完成	完成	完成	完成	完成	完成	完成	完成	完成	完成	完成		

時程 工作內容	101年08月	101年09月	101年10月	101年11月	101年12月	102年01月	102年02月	102年03月	102年04月	102年05月	102年06月	102年07月	102年08月
	1期	2期	2期	2期	3期	2期	2期	3期	4期	3期	2期		
5篇專題分析報告及2篇重要議題分析報告					完成2篇			完成2篇		完成2篇	完成1篇		
期中報告					完成								
1場焦點座談會										完成			
期末報告												完成	

資料來源：本計畫製作

四、研究限制

本計畫執行於研究方法係因部分國家或國際組織在安全因素的考量下，不公開或僅公開部分資訊，對於細部的相關資訊並不予以公開，或是以遲延公開或部份公開的方式提供，以防有心人士掌握細膩的法制與防護作法，進行系統性與組織性的蒐集、比對或資料探勘，對其國家或機關安全及機密維護造成莫大威脅。各國對於資料的開放態度與安全考量，客觀面上本難就各個議題臚列而進行平行比較，對於本計畫資料的蒐集造成一定程度的影響。

衡酌各國政府結構、文化歷史背景及政策發展基礎的差異，對於未來欲強化或偏重之面向不盡相同，較難歸納整理出一共通的策略。

再加上研究議題的特性，雖看似各自獨立，但彼此間

實際上卻相互交接牽連之影響，亦涉及不同之機關之權責，使得研究議題更形複雜。不過，這反而突顯出安全與機密保護議題，亟需全面規劃之需求。

故執行團隊對於較為成熟的政策或公開的法制資料，已盡力取得與掌握充分；相對於新興待解決之議題，資料之取得面向則偏向政策與法制趨勢，以及以各界對於新興議題的評論或建議為多。

肆、各國國家安全及機密維護法令與措施之整理與分析

為能有效掌握各國有關國家安全及機密維護之政策、措施及法令之現行作法、趨勢及未來方向，本計畫以各世界主要國家、機構及國際組織之新聞、專論、最新版官方制度文件等網路與平面資訊進行研究、歸納及分析。惟囿限於各國或國際組織對於安全性之考量及資訊公開透明度的斟酌，客觀面上難以就每一議題臚列數國進行平行比較；再者，衡酌各國政府結構、背景及政策發展的基礎上均有所不同，對於未來欲強化之面向亦不盡相同。是以，以下就不同子議題下，經酌選後挑出最具前瞻性、代表性、資訊公開最完整性之國家進行深入介紹。

一、國家安全

因科技技術的發達，世界各國的政治、經濟、文化、環境各領域均緊密串聯，牽一髮而動全身，國家利益及國家安全之形貌不斷變化；另外，利用網路進行之跨國型組織犯罪或恐怖攻擊活動日益嚴重，故各國無不致力於精確描繪出未來將面臨的挑戰及可能之因應措施。再者，近年全球氣候變遷快速而引發許多天災，進而釀成人禍，為穩定民生及因應災變，各國亦陸續的強化關鍵基礎建設並制訂防災政策，因應會帶來大規模損害的天災。

（一）國家安全策略

澳洲在 2013 年 1 月發布共 58 頁的國家安全策略文件，全名為「強大與安全：澳洲國家安全策略（Strong and Secure： A Strategy for Australia's National Security）」。因應亞洲世紀（Asian Century）的崛起，針對亞洲區域劇烈的經濟與安全趨勢改變，就其伴隨而生的風險與挑戰，本文件提出了相應的國家安全策略。

「澳洲國家安全策略」主要是以「2008 年澳洲國家安全聲明（2008 National Security Statement）」為基礎，安全聲明除了係澳洲作為國家安全風險政策之導引，對於現今及未來澳洲所面臨的挑戰與威脅，也描繪出許多面向，包含區域不穩定因素、可能涉及澳洲國家利益之衝突與高壓情勢、惡意網路活動威脅、恐怖主義所帶來的負面效應、間諜活動對於澳洲國家安全所產生的影響、大規模毀滅性武器過濾需求，以及境內或境外嚴重的組織性犯罪問題等。

而 2013 年的「國家安全策略」則描繪出澳洲在未來五年於國家安全面上應著重的四個主要目標，首先，是保護並強化澳洲主權完整性；第二，確保人口的安全性與流通性；第三，確保和維護國家資產和關鍵基礎建設，如醫護設施、補給供應鏈、智慧財產、資通訊科

技、通訊網路和自然資源資產等；第四，推動有利的國際環境以強化國家利益與價值。結構上，首先提及四大主要目標；接著描述策略環境的演進，包含澳洲持續面對的重要國家安全挑戰和必須掌握的機會；進而說明現今國家安全的基礎建設及所帶來的影響；最後則對已預見的挑戰和機會，對戰略展望提出檢視，包括在亞洲世紀中，地緣政治環境的轉變及所生影響。澳洲的國家安全措施將依亞洲區域的變革性來改變戰略。

同時，「澳洲國家安全策略」特別強調保衛邊境安全的實體力量，直接指名國防武力和情報基礎建設的重要性，但並非意謂著將拋棄軟性力量（Soft Power）在國安政策的角色，爰此，澳洲總理已計畫於 2014 年成立「國家網路安全中心（Australian Cyber Security Centre）」，藉此強化澳洲網路安全技術實力。

*請參見附錄三、計畫成果 - 資訊雙週報第 12-02、15-03、17-02、18-02、19-02、20-02、21-02、23-01、24-01、25-01、26-01 期。

（二）恐怖攻擊之預防與應變

美國近 10 年來不斷遭遇各種恐怖攻擊並造成大量的人口傷亡，從 2001 年至 2011 年共有 207 件恐怖攻擊事件，最常使用的是炸藥和

燃燒裝置,除 2001 年的 911 恐怖攻擊事件外，2013 年所發生的波士頓馬拉松爆炸事件是人員傷亡最多的一次。

故有專家倡導應用「無人機」進行預防與應變，可有效減少恐怖攻擊所帶來的人身傷亡或是恐怖攻擊事件發生的機率，包括進行偵測危險物、替深入救難人員無法進入的區域提供立即可使用的衛星訊號及通訊設備。對此提議，美國參議院司法委員會於 2013 年 4 月 23 日召開了聽證會，題目為「無人機的戰爭：憲法與反恐主義之關係」。反對意見表示，無人機的使用方式，可能會形成過度監控而侵害人民隱私；贊成意見則認為無人機能有效的預防和減緩恐怖攻擊，對於國家安全之維護具相當大之優勢。

*請參見附錄三、計畫成果 - 資訊雙週報第 22-02、23-02、24-02 期。

（三）防災管理政策

鑑於全球暖化導致世界各地自然災害損害程度日趨嚴重，各國均投注相當心力規劃防災管理政策與應變計畫，因我國位於東亞區域，故以下將以鄰近之日、韓兩國之防災政策進行介紹：

1.日本

日本於 1961 年制定的「災害對策基本法（災害対策基本法）」，旨在促進全面性的防災行政體系，規定政府應每年將防災相關計畫與措施概況向國會報告。2012 年由國會所提出的「防災白皮書（防災白書）」，詳實記載了前年度（2011 年）東日本 311 震災事件中的災害處置措施，又適逢災害對策基本法實施的第 50 周年，決定擬定更完善的災害對策以構築健全的日本環境。

在 2011 年東日本 311 震災當中，發生屋舍傾毀、人員傷亡、土地液化及核能輻射外洩等嚴重問題。針對受災區的重建，日本透過法律之制定，由地方政府聯合中央政府與民間團體力量，採取災害復原措施，主要有三大方向：復興特別區域制度、重建輔助金制度與公司和事業者重生支援機構之設立。

於復興特別區域制度部分，為使災害區域迅速復原，針對區域特殊性採取相配的處置措施並減輕地方政府的負擔及加速其應變能力，於地方事務、稅務、財政與金融等各方面，採取「一站式（ワンストップ）」的統一適用架構。依「東日本大震災復興特別區域法（東日本大震災復興特別区域法）」，得使一部或全部屬於災害地區的地方政府得

以災害復原為目的，彈性採取合適作法。此外，另設置了「國家與地區協議會（「国と地方の協議会）」，在「東日本大震災復興特別區域法」施行之後，倘地方政府基於實際需求而有新提案，可與協議會達成協議，以擴充、追加新的規定，諸如為支援創造就業機會而採取特別的稅務措施。

於重建輔助金制度部分，「東日本大震災復興特別區域法」創設了市區重建的補助金制度，使提供重建所需設備設施的基礎事業得向復興廳提出廣泛的重建輔助金交付計畫，便能獲得補助，毋須個別向地方政府的主管部、局提出申請。

就公司與事業者重生支援機構之設立部分，為解決震災中公司與事業者二重債務的問題，2011 年底以「株式会社東日本大震災事業者再生支援機構法（株式会社東日本大震災事業者再生支援機構法/原文與譯文同）」（特別法）為法源基礎，設立了「東日本大震災事業者重生支援機構（原文與譯文同）」，用以維持受災區的經濟活動，協同金融機關、地方政府，對在震災中受損而負擔鉅額債務的事業者，透過債權買收、出資與派遣專家等措施，給予支援，助其減輕負擔。

基於 2011 年東日本震災的教訓，促使日本重

新檢討「災害對策基本法（災害対策基本法）」。其修正概要重點如下：（1）強化對於大規模區域災害的防禦：包含災害發生時，積極蒐集資訊、傳遞資訊以及資訊之共有；關於地方政府相關的支援業務等規範，擴充至都道府縣的規範層級，並在國家層級訂定因應規範；此外，強化各地方政府間的互相支援措施。（2）新增改善大規模區域災害發生時的受災者處置方式：包含創設救援物資能確實供給予受災地區的機制，並且創設受災者跨地區收容、安置的程序。（3）藉由教訓傳承、防災教育強化與多元主體參與等方法，提升地區防災力。（4）修正國家・地方政府防災會議與災害對策本部之角色劃分。

*請參見附錄三、計畫成果 - 資訊雙週報 07-03、08-02、09-01~21-01 期。

2.韓國

「韓國國家災害管理署（National Disaster Management Institute）防災規劃部」於 2012 年提出極端氣候之防災管理政策，透過政策之發布與夏季災害緊急應變系統相結合，以期大幅降低人民之傷亡。極端氣候之防災管理政策主要有三項內容：大幅降低人民生命損失和社會不便、建置位於第一線且具預測

功能的救災管理中心系統及設置緊急支援措施以迅速恢復受災民眾的日常生活。

（1）大幅降低人民生命損失和社會不便

韓國政府希望透過擴大觀察山體滑坡（走山、土石流）和地質脆弱地區，進行現場管控並即時疏散危險地區之居民；並加強防洪措施、易淹水區域預知管理、配搭防洪資訊傳輸至交通號誌（VMS 系統）（Variable Message Signs System）及強化供電系統等方式，使極端氣候所可造成之社會經濟損失和人民生命財產損害降至最低。

（2）建置位於第一線並具預測功能之救災管理中心系統

透過「韓國國家緊急應變管理局（National Emergency Management Agency）」之災情分析判斷系統、全國性的監視器（Closed-Circuit Television, 簡稱 CCTV）系統、安裝於各橋樑之洪水監控系統、災難視訊資訊系統，判斷降雨、分析河川氾濫狀況、城市淹水情形，提前預測風險，並將風險監測之結果，通知相關機構。同時智慧型手機用

戶可以透過「國家災害安全中心」APP 軟體之服務，將 CBS（Cell Broadcast Service）災難廣播和 DMB（Digital Multimedia Broadcasting）災害警報廣播網路之訊息分享至推特（Twitter）或社交服務（Social Networking Services, 簡稱 SNS）等社交網路平台，亦得使國家救災機構之災難管理，進行雙向的即時災害資訊共享。

（3）設置緊急支援措施、迅速恢復受災民眾以往的生活

韓國制訂迅速恢復人民受災損害之緊急救援政策，災區之救災物資應達足夠數量，臨時避難所也從過去的學校和官署延伸到行政機關、政府資助的研究機構或教育機構。另外，對受災民眾迅速提撥財政預算預備金，作為風災水災損害之災後修復費用。

*請參見附錄三、計畫成果 - 資訊雙週報第 03-05、04-09 期。

我國與韓國就極端氣候面對之可能災害相似，多為土石流及洪泛，故相關政策擬定趨勢相當類似，除可參酌韓國之相關作法外，「歐盟面對極端氣候之應變策略套案（EU

Adaptation Strategy Package）」[3]或追蹤其他相關國際組織之研究，協助我國防災與應變政策之制訂。

二、國家機密維護

國家機密維護之議題一直以來均為各國政府重點關注的對象，相關的規範與機制亦與時俱進進行修正變更。近年來，美國不斷發生重大的機密公開揭露事件，例如維基解密（Wiki Leaks）曼寧（Bradley Manning）案、國安局的稜鏡（Prism）計畫史諾登（Andrew Snowden）案等，消息來源均係來自於政府機關內部人員，引發一連串的爭議與反思。因此，為達成國家安全之目的，美國不斷地強化內部控管國家機密資訊的能力，值得做為我國之借鏡。

（一）國家機密維護之管控機制

為加強政府機關內部國家機密資訊的保存及管控制度，「美國國土安全部（Department of Homeland Security, DHS）」於 2004 年發布「保護國家機密之責任及其處理、儲存指令（Protection of Classified National Security Information： Accountability, Control, and Storage）」，規範國土安全部內部國家機密計畫的安全維護要求。其適用的對象包括所有依據

[3]European Commission，EU Adaptation Strategy Package，Retrieved from http://ec.europa.eu/clima/policies/adaptation/what/documentation_en.htm (last accessed Sept. 02, 2013).

契約永久或暫時隸屬國土安全部，或與美國國土安全部相關及派遣人員；本指令亦適用於被允許存取機密資料之非聯邦政府官員。

針對國土安全部內部人員之責任劃分，該指令特別就「資深行政官員（Senior Agency Official, SAO）」、行政安全部門長官、組織成員中之主席、組織成員之安全官/安全聯絡官、監督人員和管理人員、以及所有國土安全局個人等 6 大類別進行規範與說明。除相關部門長官、主席等管理人員需依職權確保和提倡組織成員遵守規定外，所有人員皆負有保護機密資訊免於未經授權而被揭露的責任。

除了國土安全部內部人員之權責劃分外，該指令亦特別針對國家機密之處理和儲存面向進行規範，然這僅為最低標準，組織成員可選用更嚴謹之標準後，依相關程序向國土安全部部長呈報。

另外，參議院提出「2013 年度情報授權法（The Intelligence Authorization for Fiscal Year 2013）」法案，禁止媒體向情報機構人員蒐集並公開介紹「背景」或「不列入正式紀錄」之資訊。縱使媒體已獲得相關機密，亦受此限制；同時禁止擁有讀取最高機密權限的前公務人員在離職三年內與媒體任何具拘束力之協議（包含正式及非正式）；賦予情報機構取消洩

密者因服務政府部門而享有的福利，例如取消退休金之發放。又，法案將使司法部更易對記者發出偵查洩密的傳票，擴大傳喚與刑事追訴的權力。

*請參見附錄三、計畫成果 - 資訊雙週報 01-09、13-03、14-03、16-04、17-03、18-04、19-04、20-04、21-04、22-04、23-04、24-04、25-04、26-04 期。

（二）能獲悉國家機密職位的考核標準

白宮於2013年1月25日發布總統備忘錄，要求特定部門對於具「國家安全敏感性（National Security Sensitive）」的職位提出考核標準及解雇規範。

備忘錄的新規則允許聯邦機構不經上訴即可解僱職務範圍涉及國家安全的員工，且適用對象不限於已通過安全查核的人員，聯邦機構可自行指定將來可能需要具備安全查核通過資格的職位（敏感性職位）。惟政府若廣泛的行使指定權利，可能造成員工根本不知道其職位已被指定屬於「敏感」的職位的狀況，爾後如果員工後來被所屬機構認定沒有擔任該職務的資格，也無從提出上訴進行救濟。

揭弊者（Whistleblower）倡導組織認為，

新規則或許可以成為遏止公務員洩露情資的有效措施，但亦會對維持政府透明度和防範貪腐的機制造成傷害，蓋政府人員若能遭機關自行決定是否開除，且無法向中立的上訴機構提起上訴，會降低揭露政府不法或貪腐行為的意願，以國家安全為名的這頂大帽子實乃過度限縮了法律所賦予機構人員的權利。此一爭論反映出保護機密和捍衛民主（如政府施政透明度和揭弊者的權利）間的緊張關係。

*請參見附錄三、計畫成果 - 資訊雙週報第 07-08、07-09、19-03、20-03、21-03 期。

（三）公務機關面對內部威脅之作法

鑑於電子化政府政策之推動，資通訊技術導入公務機關的業務運作，以及對於電子資料庫之應用與仰賴日益加深，公務機關所持有或擁有之大量資訊（包含具機密性或敏感性之資訊），可能成為有心人士或其他國家情報機構覬覦的目標。

根據網路入侵案件的統計分析，約有 8 成的資安事件與內部人員有關，其原因可能歸咎於資安人才與預算不足、系統權限與身份識別控管機制不完善、委外開發維護及品質管理問題、人員資安意識不足以及機關橫向聯繫機制尚待建立等，內部威脅（Insider Threat）的議

題近來受到高度重視。

觀察現行資通安全政策對於外部駭客攻擊的威脅較具完備防禦配套措施，相較之下對於可能使用（Access）公務機關資訊系統之個人或廠商之規範相對的缺乏。

參照美國為因應維基解密事件，建構了一連串監控內部威脅的政策、法制與配套標機制，並對現行制度與措施進行全面檢討。首先於 2011 年發布第 13587 號行政命令，並依該號命令發布「國家內部威脅政策和機關內部威脅方案的最低標準（National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs）」總統備忘錄。各部會與機關也開始強化內部威脅的防範措施，例如國防部開發自動偵測內部威脅的辨識系統、商務部（Department of Commerce）國家標準與技術中心（National Institute of Standards and Technology, NIST）與司法部（Department of Justice）聯邦調查局（Federal Bureau of Investigation, FBI）也訂立內部威脅指引，提供企業與機關單位遵循；Carnegie Mellon University 的電腦緊急應變團隊（Computer Emergency Readiness Team）也受情報機構委託，進行對內部威脅之研究。

據此，為落實對內部威脅的防範，機關內

部人員與委外廠商都應進行一定的安全查核程序，並透過科技技術進行監管，例如利用系統監控人員的異常行為（短時間內大量下載檔案或轉出信件、消費力顯著提高或情緒異常低落或起伏極大）等取得潛在威脅的證據，便能進一步確認內部威脅是否有可能發生。而相關制度宜有一統一綱要後由各機關因應自身特性加以建置，並要求全國公務機關一起合作落實。例如，可先採取全國統一的公文系統、統一公務機密的分類，如此便能確保各機關間的保密措施位於統一水平，不會有因資訊傳遞致保密措施不足的機關而提升外洩的風險。

*請參見附錄一、計畫成果 - 專題分析報告（一）公務機關電子機密資訊系統面對內部威脅之作法。

（四）未經授權公開揭露國家機密與解密間之關係

美國自 1940 年起由羅斯福總統開啟以行政命令來建立政府核定機密標準的先例，現今核密與解密的依據為第 13526 號行政命令，一旦按命令之標準將某資訊列為機密，則未經授權的揭露將被視為危害國家安全；反之，當某些資訊公開揭露亦不影響國家安全時，則應立即解密（Declassification），解密後得對外公開。

然而，實務上不乏機關內部人員，尤其是機關首長或高階官員，在未經合法授權下，以對政府有利為由向媒體或不明第三人任意洩漏（Leak）機密資訊。根據「美國國會研究服務處（Congressional Research Service/CRS）」在 2013 年 1 月提出的研究報告指出，未經授權洩露機密資訊的行為，理論上不應該影響資訊的機密等級，然而目前官方的政策是卻傾向將未經授權公開揭露機密資訊的行為視為「立即解密行為（Instant Declassification）」或「有高層授權揭露」。

惟第 13526 號行政命令雖規定「機密資訊不會因相同或相關連之資訊未經授權揭露而自動解密」，似乎假定核密機關除了依法公開或因緊急事故揭露機密資訊（此時的揭露必須符合核密機關之程序，如限於必要知悉者及必要之資訊，且揭露效果不等於解密）外，不會有其他公開揭露之情事，因此並未處理到前開情形，亦即實質上等同授權揭露時之法律效果為何。另外命令亦未明確賦予機關自由裁量權，得在合法解密前便釋出機密資訊予公眾。

針對政府官員任意洩漏機密資訊、尤其是口頭散播給記者的行為，美國政府將之視為跨機關的內部威脅。2012 年 12 月白宮發布「國家內部威脅政策及行政機關內部威脅計畫基

準（National Insider Threat Policy and Minimum Standard for Executive Branch Insider Threat Programs）」，指導各機關如何保護機密資訊免於受內部官員在未經授權情況下對外揭露。另國會通過效力為期一年的「2013 年度情報授權法（The Intelligence Authorization for Fiscal Year 2013）」，針對聯邦政府官員的揭密行為進行相應的規範措施。

*請參見附錄三、計畫成果 - 資訊雙週報第 01-09、03-03、06-04、08-04、09-02、11-08、18-05、22-03 期。

三、機關安全維護

機關安全維護著重於實體設施及出入人員之安全性，確保政府業務和基礎建設能正常運作以維民生秩序、國家資產不受破壞及機關人員、訪客或洽公民眾的人身安全。天災與人禍均足影響機關之安全性，宜建立相關之預防與應變計畫，又近年恐怖組織活動頻繁，各國政府對此嚴陣以待，英、澳兩國所釋出之相關資訊相當完整充分，足值借鑑。

（一）機關安全維護政策

1.澳洲

澳洲司法部（Australia Government

Attorney-General's Department)於 2012 年 12 月發布最新版本的「防護性安全政策架構（Protective Security Policy Framework，簡稱 PSPF）」，架構設計成四個層次，由高而低為：政府業務安全性指令、核心政策與強制性要求、議定書/標準與指引、機關特定的政策與程序。

最上層以「政府業務安全性指令(Directive on the Security of Government Business)」做為安全政策架構的基石，闡明政府對於機關本身與委外廠商安全防護工作的要求；第二層進一步明定「核心政策與強制性要求（Core Policies/Mandatory Requirements）」，核心政策三大面向為人員安全、資訊安全及實體安全；第三層係為遵循核心政策與強制性要求，訂定了細緻化、具體化之「實施指引、安全防護措施及風險管理之範本及相關適用標準（Protocols/Standards & Guidelines）」，提供各機關一致性的作法，使跨部門業務之執行和資訊共享更加順暢。第四層則為「機關特定的政策與程序（Agency-Specific Policy & Procedures）」，要求各機關應依業務需求與自身特性，制定專屬的安全維護政策和程序，同時也能補充和支持其他機關的營運和操作程序。

*請參見附錄三、計畫成果 - 資訊雙週報第05-01、05-05、06-01、07-01、09-05、10-05、11-06、12-06、13-05、14-06、15-06、16-06、17-05、18-07、24-09、25-05 期。

2.英國

近年隨著全球氣候變遷，自然災害所造成之影響開始波及國家的正常運作。2012 年英國因受豪雨、暴洪和暴雪侵襲損害慘重，導致水電無法正常供應以及交通中斷、受阻。是以，如何有效透過國家關鍵基礎設施之串連，能即時應變天災之影響並維持國家運作，此為一相當重要之議題。

英國為促使關鍵基礎設施之所有者和經營者、緊急救援人員、企業集團、監管機構和政府機關等能共同攜手合作，進而提升關鍵基礎設施和基本服務之應變能力，英國政府遂於 2011 年出版「維持國家運作：自然災害和國家關鍵基礎設施（Keeping the Country Running：Natural Hazards and Infrastructure）」指南，希望藉此提供改善重要國家關鍵基礎設施安全及必要服務恢復力之指引方向。

該指南主要提供之建議分成 6 大面向：對自然災害之風險識別和評估、恢復力標準、業務連續性和公司治理、給經濟管制機關之指

導、資訊共享和了解當地該建設的依賴性。值得注意的是，該指令特別提出資訊分享之目的係為使公、私部門間之資訊能於適當及需要的時機，及時的交換情報以利有效的進行緊急應變措施。故該指令闡明，規劃民間緊急應變計畫時，必須了解關鍵基礎設施於其所在區域內提供之必要服務及人民對其之依賴度、設施功能因天災而瓦解會帶來怎樣的風險和影響程度、以及事故發生能得到哪些援助（例如水災侵襲時能請消防人員協助抽水）。

*請參見附錄三、計畫成果 - 資訊雙週報第07-06、07-07、08-05、10-04、11-05、12-05、13-04、14-05、15-05、16-05、17-04、18-06、19-05、20-05、21-06、22-05、23-05、24-05期。

（二）機關實體安全維護

恐怖主義對英國是相當真實而且嚴重的威脅，除了以暴力攻擊或破壞資通訊系統引發大規模事故、對機關(構)向來會造成立即性、長期性的嚴重損害和信用破壞外，也包括對特定政商人物的人身威脅。故英國政府發布適用於公私部門的反恐指導文件「防止恐怖主義-第三版（Protecting Against Terrorism-Third

Edition）」（下稱「本文件」），指導機關（構）如何從人員人身安危保障、營運穩定性、信譽維護及成本考量四大面向上進行衡平考量，達成僅需面對合乎比例風險之目標。另外英國政府設計了「看守人指示計畫（Project ARGUS）」，模擬恐怖攻擊事件，企業可以申請參加，透過實際應變演練瞭解自身的安全計畫是否完善、人員的訓練是否充分。

本文件所指導之安全計畫為層級式結構，基本元素為：資訊（盤點、弱點檢測與風險評估）、防護措施、應變計畫及安全文化。安全計畫仰賴公正的評估，故過去的失敗紀錄應忠實的呈現作為基礎。又安全計畫的建構需以風險評估為基礎，因能投注之成本和資源具有限性，故應投注於最需要關注的風險來源並劃分類型和等級。

至於防護措施部分，本文件認為完整的防禦體系必須包含實體安全、資訊安全及人員安全 3 大防禦措施，依評估狀況均衡的投入人力與預算，措施的手段與威脅的損害必須符合比例原則，且投入的成本必須低於資產的價值，並強調預防勝於治療的概念。實體安全防禦措施目標在預防及有效降低實體攻擊（如炸藥）所造成的損害，具體作法如設置阻車地柱/檢查哨、獨立隔離的包裹收發室、使用監視器

（CCTV）系統等；資訊安全防禦措施的目標則是確保資訊的安全使用、儲存與傳輸，而最需要注意的元素是「人」，蓋現今機關（構）多將資訊安全委外處理，故對於委外廠商的管控需特別注意，另外內部人員多半欠缺資安意識而常因過失而丟失或洩漏資訊；另人員安全防禦措施的目標是透過有效管理減少引狼入室的可能性、確保合法權限不被濫用，且同時不得影響例行業務的運作，亦需避免員工覺得不被信任而對機關（構）離心。

應變計畫的大方向可分為企業營運持續計畫、緊急聯絡計畫及緊急疏散計畫。首先，確保遭遇攻擊或重大災害時能在第一時間內恢復正常運作，並以順暢的內、外部通訊，有效分派人力與任務並能及時聯絡緊急應變服務廠商、總部和能給予支援的政府機關；且對新聞媒體也應有聯絡窗口以利第一時間發布官方回應避免不必要的社會觀感誤解或商譽損失。另，疏散計畫最大挑戰點是要預先決定哪裡是安全的避難地點及疏散動線、以及對於特殊身份者如身體殘缺者或孕婦的照護需求和特別疏散安排。

末者，本文件強調應建立機關（構）全體人員的安全意識，對例行性業務需抱持一定警覺心，重視組織所訂定的安全維護政策和計畫，

不讓政策宣導僅成為空泛的口號。安全文化的建立有五大要素：與基層員工的溝通、管理階層的支持、中階主管的聯繫溝通能力、員工訓練/諮商/輔導與安全熱線。

*請參見附錄三、計畫成果 - 資訊雙週報09-06、10-06、11-07、12-07、13-06、14-07、15-07、16-07、17-06、19-06、20-06、21-07、22-06、23-06、24-06、25-06、26-06 期。

四、公務機密維護

除卻攸關國家安全與國家利益之國家機密外，政府為進行重大政策或計畫的推動、維持金融市場或社會秩序、及商業談判或磋商等活動或各機關（單位）因其業務特性而持有某些不宜對外公開或特定時點前不宜公開之敏感性資訊，對此機關必須負起妥善管理與保密的義務，同時亦需考量作業效率、維護成本與人力負擔之衡平性。各國已注意到並不適宜將劃入「敏感性資訊」區塊之資料通盤以同一位階之「公務機密」去作處置，應按資訊之敏感性程度、價值及特性建構分類分級的金字塔結構，配以相應嚴謹度的管理及安全維護機制。另對於洩漏公務機密之人員，若欲給予制裁，應有明確清楚之法令規範，定明違犯行為、構成要件與法律責任，方能達到震懾及事後明確究責之效果。

（一）機敏性資料之分類分級與安全維護措施

英國將機敏性資訊（包含國家機密、公務機密與敏感性資訊）分為5階，除卻前3階的國家機密外，另將敏感性資訊劃分成「限閱級（Restricted）」與「防護級（Protect）」，稱為「政府防護標記系統（The Protective Marking System）」，並按3大關鍵要素「人員、標準程序、技術」[4]規劃管理與安全維護措施，英國由資訊專員辦公室（Information Commissioner's Office）負責執掌機關資訊安全事項，發布相關的指引文件，具體指示每一級資訊的標示標準、法遵義務與違犯責任。

*請參見附錄一、計畫成果 - 重要議題分析報告（一）論公務機密之保護 – 以因應個人資料保護法為中心。

北愛爾蘭亦將國家機密分為三級，其餘的敏感性資訊分為「限閱級（Restricted）」與「敏感性（Sensitive）」兩級，由「北愛爾蘭地區就業與學習部（Department for Employment and Learning, DEL）」於2009年發布供內部人員遵守之「保護標誌和檔案安全維護指導方針（Guidelines for Staff in the Department for

[4]人員：鑑別資訊價值的能力培養、資安維護職場文化的建立；標準程序：標準作業及流程的徹底落實、明確責任劃分與定期稽核；隨時更新安全技術與設備設施。

Employment and Learning - Protective Markings and Document Security）」，設計不同的保護處理程序，按資料敏感性等級限制閱覽權限與流通範圍，另外，資料敏感程度性會隨時間變化而有所變動，人員組成也會流動，因此規定需定期就資料內容與閱覽權限檢視、查核以利變更。

*請參見附錄三、計畫成果 - 資訊雙週報第 12-09、13-09、14-09、15-08、16-09、17-08、18-09、19-09 期。

紐西蘭亦於 2011 年提出「紐西蘭公務機密保護指引（Guidelines for Protection of Official Information）」。該指引除強調應依資料類型選擇適當的分類、等級的重要性外，同時強調在處理與傳送敏感性資料時，須就資料類型與分類等級使用嚴謹度不同的作法。

指引指出，若使用電子儲存的方式儲存限制、敏感、或保密性資料時，除需注意內部的使用存取權限設定外，亦需特別注意防範外部人員透過不法手段方式存取內部資料。就電子資料之銷毀需採不可回復性之辦法。而傳遞紙本資料時，除需標示該資料之分類等級外，亦需清楚標示退件住址。

*請參見附錄三、計畫成果 - 資訊雙週報第 23-09、24-08、25-08、26-08 期。

（二）公務機密維護與為公共利益揭露之衡平

由於政府高官多因其職務而持有相當份量之公務機密，而不時會有以為政府之利益口頭洩漏予媒體或其他第三人，造成社會紛擾與動盪，是以，為避免因不法揭露公務資訊或文件對國家安全產生危害或侵擾公務機關正常運作，各國對此均欲以法規範進行有效之管制，惟從另一角度觀之，亦不希望過度管制而扼殺為民喉舌者揭發政府不法行為的意願。

1.新加坡

新加坡於 2010 年 5 月通過「公務機密法（Official Secrets Act）」規範所有攸關公務資訊傳送、接收等事項，並於 2011 年 1 月 2 日正式施行，又於 2012 年 11 月 30 日進行修正。其內容包含對從事間諜活動之罰則規定、禁止使用照相機的場合及違犯的法律責任、資訊非法傳遞的構成要件、未經授權使用制服、報告之竄改/偽造/冒名和提供錯誤文件之效果、與外國間諜聯繫構成不法的犯罪證據、干預警察機關或軍隊之效果、獲得產出資訊的權限、非法提供資訊可能致生的犯罪行為、藏匿犯罪嫌疑人的效果、攻擊與搧動行為的從事等。

另外，治安法庭法官如因口頭誓言或已證實之資訊而確信有相當理由懷疑新加坡公務機密法之罪名成立或有違犯之虞時，法官得核發搜索令授權警察機關，或有行使武力必要時，亦得授權由軍隊指揮官指派之軍隊陪同警察人員，在任何時間進入搜索令明定之場所，進行地域及出入人士的搜索，並得扣押與留置任何照片、圖畫、計畫、模型、文章、筆記或文件，或是任何可能作為已成立或即將違犯新加坡公務機密法所規定相關犯罪的證據。同時，警察機關亦得扣押或留置在該場所之人身上所找到、任何警察均會合理懷疑係與涉犯公務機密法之罪有關的所有物品。

*請參見附錄三、計畫成果 - 資訊雙週報第12-08~14-08、16-08、17-07、18-08、19-07、20-07、21-08、22-07、23-08、24-07 期。

2.美國

有時政府機關會以其立於高位之便利，假借機密之名，掩蓋政府的非法、濫權或怠惰職務的行為，縱有知情而欲為民喉舌的內部人員，也會因擔心遭到報復或飯碗不保而噤聲。因此，美國國會曾訂定「揭弊者保護法（Whistleblower Protection Act）」，鼓勵揭露

政府機關或不肖官員的非法行徑，但該法並無法提供情報機構的員工相關的法律上保護。為彌補此一缺口，美國總統歐巴馬於2012 年 10 月 10 日發布「第 19 號總統政策指令（Presidential Policy Directive 19）」，提供接觸機密資訊揭弊者的保護（Protecting Whistleblowers with Access to Classified Information）。

指令主要在禁止政府機關對在「受保護下揭露（Protected Disclosure）非法活動或浪費、詐欺、和濫用行為」的情報機構人員（Intelligence Community Employee）進行報復，同時奠定政府相關責任的框架-內部申訴的審查程序。但前開指令並不保護未經授權即向公部門管道以外的媒體或公眾揭露機密資訊的情形。又本指令並不會抵觸「揭弊者保護法」現有的權利規範。

該指令受到支持揭弊組織的肯定，雖然認為指令並沒有解決所有問題，但至少是一個填補缺口的開始。不過，雖情報機構人員依指令享有特定言論自由、並在揭弊時無須擔心遭到報復，指令仍無法取代國會以立法的方式對國家安全情報揭弊者、第三方執行者與其他員工提供法律上的權利保障。

*請參見附錄三、計畫成果 - 資訊雙週報第

04-07、07-08、07-09 期。

五、資通（訊）安全政策

電子化時代的來臨，意味著公、私部門的資訊處理不再是以紙本為主，而是在電腦系統及通訊網路中流通，因此，竊取機密或癱瘓、中斷機關（構）的功能和運作不再需要透過實體攻擊，可以僅透過虛擬的網路環境進行攻擊；另外，電子商務的崛起不僅改變商家和消費者間的關係，也使得交易資訊、私人財務狀況等高度隱私資訊很可能因為網路之不安全而遭到竊取、進而引發大規模的網路詐欺、身份竊盜等電腦犯罪。是以，創造安全的資通訊環境乃政府首當其衝之任務。

（一）資通訊安全法案

新加坡政府於 2012 年 11 月表示，全世界的網路攻擊頻率、速度和複雜性與日俱增，且時常毫無預警的出現，故必須採取迅速和有效的行動，來防止網路威脅危及關鍵資訊基礎設施。為此，新加坡政府修正「電腦濫用法（Computer Misuse Act）」，修正內容將迫使境內企業在特定情況採取必要行動，防止對電腦系統的網路攻擊。

依「電腦濫用法修正法案」之規定，賦予新加坡內政部長（Minister of Home Affairs）極大的權力，得以遏止、偵測或打擊對國家安全、

重要基礎服務（Essential Service）或國防及外交關係之威脅為由，要求任何組織及自然人採取相關措施或遵守相關規定（包含可行性措施種類的例示規定），藉此預防、偵測或打擊任何型態的電腦威脅。政府可能課予企業提供相關資訊予政府之義務，例如企業電腦系統的設計細節或安全性、系統上即時資訊（Real-Time Information）紀錄或曾發生的入侵系統事件的細節資訊。

此外，修正法案中也重新定義「重要基礎服務（Essential Service）」，只要直接關係到資通訊基礎設施、銀行與金融業、公營事業、大眾運輸、陸路交通基礎設施、航空、海運或公眾重要基礎設施或緊急救助服務，例如警察、民防或醫療衛生服務均包含在重要基礎服務範圍內。

關於罰則部分，若不遵守新加坡內政部長依據該修正法案所為之命令，或妨礙他人遵守任何命令且無正當合理之事由（Reasonable Excuse）時，將可能面臨長達 10 年的監禁和高達50,000新加坡幣的罰款(約117萬台幣)。

*請參見附錄三、計畫成果 - 資訊雙週報第 16-10、18-10、20-10、21-10 期。

（二）關鍵基礎建設之網路安全問題

美國總統歐巴馬於 2013 年 2 月 12 日簽署「改善關鍵基礎設施的網路安全總統行政命令（Executive Order on Improving Critical Infrastructure Cybersecurity）」，期藉由增加自願性的非機密性資訊分享，與民間企業合作，共同對抗網路威脅和強化關鍵基礎設施之網路安全。

合作方式主要係以「國防產業基礎資訊分享計畫（Defense Industrial Base Information Sharing Program）」為基礎，開放其他部門參與，並由「國家標準與技術局（National Institute of Standards and Technology, NIST）」主導「網路安全架構（Cybersecurity Framework）」之發展。

在維護網路安全的同時，機關必須將隱私與公民自由保護措施納入活動當中，並檢視現行的網路安全規範。政府機關必須針對活動進行例行性的隱私與公民自由衝擊評估，且公開評估結果。法令主管機關則應依據網路安全架構，評估網路安全法令之妥適性，配合向所轄產業進行諮詢後，確認現有規定是否需要變更或廢止。並宜鼓勵獨立之法令主管機關於職權範圍內權衡網路架構之要求，考量應採取之優先事項以減輕關鍵基礎設施所面臨的網路風

險。

*請參見附錄三、計畫成果 - 資訊雙週報第 15-10、17-10、23-10、25-10、26-10 期。

（三）智慧電網

「智慧電網（Smart Grid）」係指在傳統電網上建設高速通訊網路，透過資訊處理技術，降低用電量及提供高效率電力供應，同時兼具自我監控、診斷及修復功能，並能減少 CO_2 排放、抑制尖峰負載及節約能源。美國、歐盟、日本、韓國、中國大陸均積極推出建置智慧電網相關政策。

美國每年都會因為天災造成的大停電，除卻天災之外，恐怖攻擊、網路攻擊、熱浪和老化的電網等人禍也會造成電力供給的極度不穩定。為因應前開威脅，各機關紛紛自行建置「微型電網（Microgrids）」，微型複製大型商用電網，從多個來源產生和傳輸能源。美國國防部、衛生相關的機關和「美國聯邦航空管理局（Federal Aviation Administration）」等關鍵設施上投資，企圖使電力供給具可靠性和獨立性。平時微型電網與當地的商業電網互相串聯與運作，不過當商業電網無法運作時，微型電網便會斷開連接，以自身的設施接續運行。

因停電期間所可能遭受的經濟損失，政府機關對於微型電網的需求不斷增加，民間機構也逐漸思考獨立電網的可能性。然而，微型電網並不適用於每一個聯邦機構，但對於重要建設和校園，如政府機關的資料中心，必須具備能執行關鍵功能而不允許中斷的電力，在發生災害時仍能持續運作。

然而由於智慧電網需利用通訊網路，接連不斷的威脅事件陸續增加，「美國國土安全部（Department of Homeland Security, DHS）」已經向工業系統連接到電網的公用事業發出警告。另為保護智慧電網免於遭受網路攻擊，「美國國家安全局（National Security Agency, NSA）」建立「完美公民（Perfect Citizen）計畫」，以保護關鍵公用事業敏感控制系統為目標，搜尋公用事業的電腦資訊系統間與電子產品設備介面間的弱點，並提出解決與修補弱點的方案。

該計畫受國防部和情報機構的支持，但執行方式卻受到些許爭議。蓋美國國家安全局為國防部五角大廈的手足，負責蒐集和分析外國通訊和捍衛美國政府的通訊和電腦網路，並不負責監控國內間諜活動，所以若欲裝置感應器將會涉及隱私權保護之敏感議題。國會與避免政府控制網路的網路隱私倡議者（Internet

Privacy Advocate）認為，不宜將私人企業所擁有的網路系統視為「關鍵基礎設施」而使其遭受侵入性的數位監測。

對此疑慮，美國國家安全局聲明，「完美公民計畫」定位為「純粹的弱點評估和能力開發，而不涉及監測（Monitor）通訊，或放置感應器（Sensor）至公用事業的系統上」，強調將嚴格遵守美國法規範的精神和條文，否認有任何非法或侵入性的活動。另有非政府組織表示該計畫應於執行前，先進行「隱私衝擊評估（Privacy Impact Assessment, PIA）」。

*請參見附錄三、計畫成果 - 資訊雙週報第 13-02、14-02、15-02、16-02、18-03 期。

伍、重要政策建議

本計畫之緣起係為瞭解世界各國機密維護政策之發展趨勢，掌握世界主要國家之最新國家安全及機密維護政策、法令與措施，除以國家安全、國家機密維護、公務機密維護、機關安全維護及資通(訊)安全政策等五大方向進行資料(含重大新聞、官方資料及相關評論等）蒐集以建立豐富之資料庫外，另就特定議題以專題分析報告之形式進行比較分析，期能作為擬定政策、法規、行政規則及相關措施之參據及考量，並提供我國政府機關可繼續延伸關注之方向與關切之焦點。

惟查國家機密與公務機密維護兩大議題有密切之攸關且議題屬性類似，實難明確區隔加以分論，爰謹將此兩議題合併討論、分析與提出建議，合先敘明。

一、國家安全方面

本計畫「國家安全」主題所涉範圍包括：國土安全層次之反恐政策或措施；國家元首、外國元首及使館安全措施；危及社會經濟穩定、金融秩序、生態環境、資源安全、重大爆炸事件、疾病蔓延及跨國重大經濟犯罪等天然、人為及科技之災害等相關資訊。

國家正常運作的前提，乃民生秩序、金融秩序及政府之運作具不受任何因素動盪的穩定性。對於整體國家安全之政策或戰略，政府首應依國家所在區域、外交關係及國際經濟趨勢進行風險分析，找出關鍵風險領域，方能進一

步打造國家安全的基礎，保護並強化國家的主權。

為達此目標，各國如英國、美國、澳洲，近來關心之主要議題聚焦於反恐活動、關鍵基礎建設之應變與恢復力、打擊網路犯罪，促進國內公私部門之資訊共享環境與國際間的結盟合作以建立安全友善的網路空間，與因應全球氣候異常變遷規劃完善的防災政策。

（一）反恐政策、措施

我國於國土安全層次之反恐政策、措施，查有外交部 2002 年研擬之「中華民國依據聯合國安理會 1373 號決議文執行反恐怖主義行動之相關作為」[5]、行政院反恐怖行動管控辦公室（現行政院國土安全辦公室）於 2004 年 11 月 16 日規劃訂頒之「我國反恐怖行動組織架構及運作機制」[6]、法務部研擬並經行政院於 2007 年 3 月 23 日院臺管字第 0960083701 號函送「反恐怖行動法」之「反恐怖行動法草案」[7]、國軍依國安會「國內重大緊急突發（危機）

[5]外交部（2002 年，3 月 29 日）。*中華民國依據聯合國安理會一三七三號決議文執行反恐怖主義行動之相關作為*。取自 http://www.mofa.gov.tw/webapp/public/Attachment/471315182571.pdf（最後瀏覽日：2013 年 11 月 8 日）。

[6]法務部調查局（2013 年，4 月 22 日）。*法務部調查局反恐機制及運作現況專案報告第貳大點*。取自 http://npl.ly.gov.tw/do/www/FileViewer?id=3594（最後瀏覽日：2013 年 11 月 12 日）。

[7]法務部（2007 年，3 月 23 日）。*反恐怖行動法草案*。取自 http://www.moj.gov.tw/ct.asp?xItem=27404&ctNode=27518&mp=001（最後瀏覽日：2013 年 11 月 8 日）。

事件處理機制」及行政院「中央反恐應變中心作業要點」[8]，另有其他散諸於我國其他法律之規範[9]。

查近年英國[10]、法國[11]與澳洲[12]均於 2012 年積極的對於其反恐政策、法規、具體措施及指導文件進行檢視修正和制訂，確認能有效發揮反恐效果；另外巴基斯坦亦為有效預防、阻止恐怖活動，已提出反恐法案交由國會審議。另美國關注的議題之一為「生化威脅」及，於 2012 發布「國家生物監測策略（National Strategy for Counter Biological Threats）」文件，強化對於生物攻擊或生化武器的應變能力，國土安全部亦投入大量預算進行生化攻擊監測系統的研發。

相較國際間對日趨複雜的恐怖行動，積極進行政策、法規、具體措施及指導文件之制訂和修正，我國因國情及較少觸及恐怖行動相關案件，反恐意識較為薄弱，相關規範較為零散；然我國仍有受恐怖攻擊之虞，例如今（2013）年發生的行李炸彈案件[13]，一旦發生爆炸案件

[8]國防部（2013 年，10 月）‧*中華民國 102 年國防報告書 2013 第二篇第四章第八節第二點、(一）部分*‧取自 http://2011mndreport.mnd.gov.tw/m/part16.html（最後瀏覽日：2013 年 11 月 12 日）。

[9]如通訊保障及監察法第 8、9 條，入出國及移民法第 7、36 條，國家安全法等。

[10]英國部分請參見本報告第肆大點、三、(二）部分。

[11]法國反恐法案請參見本報告附錄三、計畫成果 - 資訊雙週報第 08-03 期。

[12]澳洲部分請參見本報告第肆大點、一、(一）部分。

[13]蘋果日報（2013 年，4 月 13 日）‧*行李炸彈連環放 襲高鐵嚇立委 點名馬英九*‧

恐將嚴重影響民眾人身安全，造成實體建設的崩壞及功能運作之嚴重阻礙或中斷。

我國現有之反恐機制係採行政、國安雙軌一體制；行政體系負責應變計畫擬訂、政策審議協調和指揮，此部分係由行政院設置「行政院國土安全政策會報」[14]及「國土安全辦公室」[15]；實際執行面係由各部會編成 9 個反恐怖攻擊應變組[16]，因應不同類型的恐怖攻擊；國安體系則負責反恐情報的蒐整、研判及國際合作，此部分係由國安會成立「反恐怖情勢綜合研判小組」，國家安全局設置「反恐怖情勢研判小組」。

取自 http://www.appledaily.com.tw/appledaily/article/headline/20130413/34949308/（最後瀏覽日：2013 年 11 月 13 日）。

[14]立法院（2010 年）。*立法院公報第 99 卷第 47 期委員會紀錄*。取自 http://lis.ly.gov.tw/lgcgi/lgttsimgpdftxt?d0cfc6c6d0cfcbc8d0cfcec4cfcdcdccc4cfcdcccb（最後瀏覽日：2013 年 11 月 13 日）。「行政院國土安全政策會報」歷經 2 次更名，第一次更名為 2005 年 1 月 31 日，行政院將反恐怖行動小組，修正為「反恐怖行動政策會報」；第二次更名為 2007 年 12 月 21 日，行政院將「行政院反恐怖行動政策會報設置要點」修正為「行政院國土安全政策會報設置要點」。

[15]行政院（2013 年，7 月 8 日）。*行政院處務規程第七條第十一款、第十八條*。取自 http://www.laws.taipei.gov.tw/taipei/lawsystem/lawsearchresult02.jsp?LawID=A040020000000900-20130708&K1=%E5%9C%8B%E5%9C%9F%E5%AE%89%E5%85%A8%E8%BE%A6%E5%85%AC%E5%AE%A4&K2=&st1=%20or%20&K3=&st2=%20or%20&year1=-1&month1=1&day1=1&year2=-1&month2=12&day2=31&Srange=&no=&wd=&kwd=&ltype1=&ltype2=&cltype1=1&cltype2=1&cltype3=1&cltype4=1&lcode=&RealID=（最後瀏覽日：2013 年 11 月 12 日）。

[16]黃正芳（2012 年，2 月 10 日）。建構我國國土安全五大應變體系國土安全網之探討。*國防雜誌第二十七卷*（第二期），3-26。取自 http://www.mnd.gov.tw/Upload/201203/003-026%20part2.pdf（最後瀏覽日：2013 年 11 月 13 日）。目前共有暴力、生物、毒化物、輻射物、重大交通設施、重大經建設施、資通安全、其他、海事反恐怖攻擊之反恐怖攻擊應變組。

從前述我國組織及所依據之組織法規，較難以釐清其業務分工與權責劃分，當恐怖攻擊案件發生時，跨部會的協調應變時間恐遲延，難即時、加以統一指揮。

是以，我國反恐政策、措施可參酌前述英國、法國、澳洲、美國、巴基斯坦之國家經驗：

1.積極建構並完備國土安全層次之反恐政策、措施，整合我國現行相關法律規範，並就「恐怖行動、組織、團體及份子」明確定義，因無論是實體環境的恐怖攻擊或虛擬環境的資訊攻擊，均宜清楚意識並建立「反恐」之概念，以避免因立法不夠周全而致生侵害人權之疑慮。

2.考量單一專責機關、統一指揮職權之明確化，如此能免除權責界定之疑慮，亦能統合反恐之資源，或可整合納入國家安全之災害緊急應變體系範疇，以統籌、擬定及推動前、後端預警和快速應變威脅之步驟、機制。

3.強化反恐怖活動情資之交換及國際合作，以利取得預防恐怖攻擊活動的先機。

（二）關鍵基礎建設之應變與恢復力政策、措施[17]

世界各國對於關鍵基礎建設（Critical Infrastructure，簡稱 CI）之定義因國情有所不相同，但大多係指水、電、能源、交通、金融與中央政府等領域，若當中其一領域之運作受嚴重干擾或中斷，將造成極巨大之損害。

我國對關鍵基礎設施定義為「國家公有或私有、實體或虛擬的資產、生產系統以及網絡，因人為破壞或自然災害受損，因而有影響政府及社會功能運作、造成人民傷亡或財產損失、引起經濟衰退、環境改變或其他足使國家安全或利益遭受損害之虞者」；關鍵基礎設施之判定準則為：（一）足以直接或間造成大規模人口影響者、（二）足以直接或間造成經濟損失者、（三）足以直接或間影響其他關鍵基礎設施營運之能力者；並將關鍵基礎設施分為八個部門（Sector），依照設施防護優先順序排列如下：（一）能源（Energy）、（二）水資源（Water）、（三）資通訊（Information and Telecommunication）、（四）交通（Transportation）、（五）銀行與金融（Banking and Finance）、（六）緊急救援與醫院（Emergency Services and

[17]細部資料請參見本報告附錄三、計畫成果 - 資訊雙週報第 08-05、10-04、11-05、12-05、13-04、14-05、15-05、16-05、17-04、18-06、19-05、20-05、21-06、22-05、23-05、24-05 期。

Emergency Services）、（七）中央政府及主要都會（Government）、（八）高科技園區（Hi -Tech Industrial Parks）[18]。

而我國就關鍵基礎建設應變與恢復力之政策、措施、研究常與反恐及防災政策相涉，查有災害防救法、國家災害防救科技中心協助行政院國土安全辦公室於 2009 年至 2011 年推動之「國家關鍵基礎設施安全防護計畫」；惟我國現行（2013 年）法令尚無關鍵基礎設施安全防護相關規範，但已有行政院國土安全辦公室初步草擬[19]之「國家關鍵基礎設施辦法（或法）草案」[20]及立法院賴士葆委員等 27 人提案第 10511 號之「關鍵基礎設施安全防護條例草案」[21]二立法草案種版本。

相較於我國目前仍處立法探討階段，部分

[18]國家災害防救科技中心（2012 年，4 月）。*關鍵基礎設施災害脆弱度評估與風險管理：災害衝擊評估方法 I*，105-113。取自 http://astdr.colife.org.tw/file_download.aspx?auto_id=68&pid=71（最後瀏覽日：2013 年 11 月 13 日）。

[19]自由時報（2013 年，4 月 22 日）。*政院將提關鍵基礎設施防護草案*。取自 http://www.libertytimes.com.tw/2013/new/apr/22/today-p1-2.htm（最後瀏覽日：2013 年 11 月 13 日）。

[20]國家災害防救科技中心（2012 年，4 月）。*關鍵基礎設施災害脆弱度評估與風險管理：災害衝擊評估方法 I*，120-122。取自 http://astdr.colife.org.tw/file_download.aspx?auto_id=68&pid=71（最後瀏覽日：2013 年 11 月 13 日）。

[21]立法院（2011 年，5 月 4 日）。*立法院議案關係文書院總第 310 號 委員提案第 10511 號*。取自 http://lis.ly.gov.tw/lgcgi/lgttsimgpdftxt?d0cfc6c6d0cfcbc8d0cfcec4cfcdcdccc4cfcdccb（最後瀏覽日：2013 年 11 月 13 日）。

國家除已有基礎之關鍵基礎設施安全防護政策、措施外，甚已開始探究更細緻之規範模式，值得我國借鏡。

以美國為例，該國智慧電網建置之實體發、供、配電等電力系統的保護是在關鍵基礎建設保護的政策與作為之範圍；近年因電網老化嚴重、熱浪、颶風和網路攻擊，使得政府機關因無電力可用而無法運作；尤其網路攻擊透過虛擬資訊通路傳播電腦病毒軟體、錯誤資訊，使實體發、供、配電設備不依指令運作設備，甚至直接癱瘓智慧電網之資訊反饋及傳遞的訊息集中器，進而達到癱瘓實體發、供、配電系統。為此，美國於 2007 年「能源獨立和安全法案（Energy Independence and Security Act of 2007, EISA）授權「美國國家標準暨技術研究所（National Institute of Standards and Technology, NIST）和「美國聯邦能源監管委員會（Federal Energy Regulatory Commission, FERC）」，負責智慧電網安全維護的協調，和制訂智慧電網相關的指引與標準。「美國責任辦公室（Government Accountability Office, GAO ）」對於智慧電網的安全維護，提出不定期的評估與產出建議事項[22]。

[22]請參見本報告附錄一、計畫成果 – 專題分析報告（三）「智慧電網系統安全維護研究報告」。

再以英國為例，英國特別針對關鍵基礎建設提出「國家關鍵基礎建設安全與核心功能恢復力指引（Keeping the Country Running：Natural Hazards and Infrastructure）」，當中包括國家風險評鑑機制、緊急事故範圍及影響、當地政府機關可提供之風險評估指令與與緊急應變計畫範本、關鍵基礎建設營運者之間如何進行資訊共享以強化應變和恢復力等；且該指引亦明確指出「國家關鍵基礎設施之業者以及營運商，因為不同部門和地理位置間的差異，沒有一個『一體適用』的方法可以改善恢復力。對於關鍵基礎設施業者、監管機構以及政府部門彼此應透過三方協商機制，以探究可提供關鍵基礎設施安全性之最佳機制以及戰略」[23]。

據此，我國關鍵基礎建設之應變與恢復力可參酌前述英國、美國之國家經驗：

1.宜考量就全國關鍵基礎設施之治理，擬定核心安全維護綱要與政策、法規，具體的進行法制規範與權責機關體系之建構，以利後續各主管機關之推動及跨部會之合作。

2.依據核心安全維護綱要與政策、法規，進一步因應國家關鍵基礎設施，異其機關性質和地理位置，以讓國家關鍵基礎設施具備防禦

[23]請參見本報告附錄三、計畫成果 - 資訊雙週報第 08-05 期。

及恢復力（Infrastructure）為基礎前提，制訂特定部門可操作、執行之防護計畫、規則、指南等。

3.以「全災害防護」（All Hazard Approach）角度出發，考量與反恐、防災政策共同合作，並強化關鍵基礎設施、政府部門、私人企業間之三方協商機制，以因應併隨恐怖活動、天然災害之複核性問題發生。

（三）打擊網路犯罪，促進公私部門和國際間的結盟合作以建立安全友善的網路空間之政策、措施[24]

資訊、情報蒐集之完整性和機密性與國家安全政策的規劃正確性息息相關，且資訊攻防戰的軟實力（Soft Power）不容忽視，蓋較之以實體力量進行武力侵犯，各國更傾向透過虛擬環境的管道進行網路攻擊和間諜活動。

2012 年迄今，英國、美國、新加坡、歐盟及其會員國如奧地利，均已通盤檢討並發布全國性的網路安全策略，包括點出尚待加強的領域與未來政策目標；當中對於公、私部門間網路安全情報的資訊共享機制及國與國間的互

[24]請參見本報告附錄三、計畫成果 - 資訊雙週報第 01-10、03-09、04-05、05-10、07-11、08-09、09-09、10-09、12-10、13-10、14-10、15-10、16-10、17-10、18-10、20-10、21-10、22-10、23-10、25-10、26-10 期。

助合作均額外重視，蓋網路犯罪具有無國界性之特性，必須藉由國際之合作方能建構開放、安全、強健的網路空間。

相較於各國之現行組織架構及作法，我國政府組織並無設立專掌資通訊安全之主管機關，因此相關權限與執法能量欠缺具完整性框架之網路安全政策，均散落於各機關（構）的內部組織下，例如國家通訊傳播委員會 2010 年 6 月 2 日以通傳技字第 09943013150 號函公告修正之「電信事業資訊安全管理作業要點」及「電信事業資訊安全管理手冊」[25]，以因應政府於 2010 年公告開放電信事業赴大陸地區投資電信業務後，作為保障民眾個人資料、企業營運機密、電信網路設施及金融交易資訊等整體資通訊網路與服務之資通安全要求。

另行政院國家資通安全會報發布指導文件，如資安政策[26]和作業規範[27]等，依行政一體原則之拘束力規範各行政機關（構），因此，對於非行政院轄下之公務機關並無強制力。

[25]國家通訊傳播委員會（2010 年，6 月 2 日），*「電信事業資訊安全管理作業要點」及「電信事業資訊安全管理手冊」*，取自 http://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=261&law_sn=1535&sn_f=1663&is_history=0（最後瀏覽日：2013 年 11 月 13 日）。

[26]行政院國家資通安全會報（2013 年），*資安政策*，取自 http://www.nicst.ey.gov.tw/News3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF（最後瀏覽日：2013 年 11 月 13 日）。

[27]行政院國家資通安全會報（2009~2013 年），*作業規範*，取自 http://www.nicst.ey.gov.tw/News.aspx?n=626B7A2643794AB0&sms=C43ECA251722A365（最後瀏覽日：2013 年 11 月 13 日）。

是以，我國國家安全層面之關鍵基礎建設之網路安全策略發展仍在初期，可參酌前述英國、美國、新加坡、歐盟及其會員國如奧地利之經驗：

1.宜儘速正視現行缺失，參酌國外之作法，統整現行資通訊安全管控體系及能量，考量是否應設立專法及建立更具全面性、前瞻性的網路安全策略。

2.以行政院科技顧問組（現行政院科技會報辦公室）擬定之「關鍵資訊基礎建設保護政策指引」（Critical Information Infrastructure Protection, CIIP）[28]，朝向進一步成立統合之專責關鍵資訊基礎建設保護單位，並依國際整體發展趨勢強化跨體系整合與關鍵資訊基礎建設保護發展進行規劃。

3.由於無專責機關，使資通安全維護相關的行政規則和制度文件，沒有統一檢視、整合各機關問題而一次解決改善之機會；至民間各行業則端視各主管機關依法所賦予之監督權限，進行資訊安全維護措施之指導，比如電信業及金融業等受高密度管制之行業會

[28]行政院科技顧問組（現行政院科技會報辦公室）（2012 年，12 月 30 日）。*關鍵資訊基礎建設保護（CIIP）政策指引*。取自 http://land.tainan.gov.tw/FileDownLoad/FileUploadList/744.pdf（最後瀏覽日：2013 年 11 月 13 日）。

被要求遵循資安事件之通報機制。

（四）建置完善的防災政策、措施

全球日趨極端的異常氣候變遷，如暴雨、洪災、海嘯及地震等天災，除將造成大量人員傷亡之外，關鍵基礎設施如交通、水、電和石油供給的中斷或癱瘓，均將引發國家正常運作之困難和經濟上的重創。

查日本基於 2011 年東日本震災之深刻體認，促使日本內閣府於 2012 年提出之防災白皮書(防災に関してとった措置の概況平成 24 年度の防災に関する計画）[29]重新檢討、修正「災害對策基本法（災害対策基本法)」，修正重點諸如：(一）強化災害資訊蒐集、傳遞及共有，(二）訂定國家層級因應規範，擴充地方政府相關的支援業務等規範至都道府縣層級，強化各地方政府間的互相支援措施，(三）創設救援物資確實供給予受災地區機制、創設受災者跨地區收容及安置的程序，(四）強化防災教育與多元主體參與等方法，提升地區防災力，(五）修正國家及地方政府防災會議與災害對策本部之角色劃分。

[29]日本內閣府（2012 年)，*防災白書-防災に関してとった措置の概況平成 24 年度の防災に関する計画*，取自 http://www.bousai.go.jp/kaigirep/hakusho/pdf/H24_honbun_1-4bu.pdf(最後瀏覽日：2013 年 11 月 13 日)。

而韓國國家災害管理署（Korea National Disaster Management Institute）防災規劃部，鑑於全球暖化導致世界各地因極端氣候引起之自然災害程度日趨嚴重，於西元 2012 年提出極端氣候之防災管理政策（극한기상 대비 현장에서 시행되는 방재정책）[30]，共有三項主要內容：（一）減少因極端氣候所造成之社會經濟損失和人民生命財產損害，（二）立於第一線、具預測、監控、災害資料廣播分享功能之救災管理中心系統，（三）設置緊急支援措施、迅速恢復受災民眾日常生活。

我國處於自然災害頻仍之地區，長年來政府已累積相當之救災經驗及防災準備，目前係依災害防救法第 6 條、第 7 條第 2 項規定，由行政院設「中央災害防救會報」[31]和「中央災害防救委員會」[32]，並由其下增設之「行政院災害防救辦公室」作為幕僚單位，而「災害防救專家諮詢委員會」、「國家災害防救科技中心」

[30]Korea National Disaster Management Institute（2012 年，9 月 17 日）。*재난 안전지 제14 권 제4 호 (통권57 호) 극한기상 대비 현장에서 시행되는 방재정책*，48-51。取自 http://www.ndmi.go.kr/promote/safe/list.jsp（最後瀏覽日：2013 年 11 月 13 日）。

[31]行政院（2012 年，5 月 10 日）。*院臺忠字第1010130598 號函修正中央災害防救會報設置要點*。取自 http://www.laws.taipei.gov.tw/taipei/lawsystem/lawshowall02.jsp?LawID=A040040131003100-20120510&RealID=（最後瀏覽日：2013 年 11 月 13 日）。

[32]行政院（2012 年，5 月 10 日）。*院臺忠字第1010130466 號函修正中央災害防救委員會設置要點*。取自 http://www.laws.taipei.gov.tw/taipei/lawsystem/lawshowall02.jsp?LawID=A040040131023800-20110601&RealID=（最後瀏覽日：2013 年 11 月 13 日）。

則提供中央災害防救會報及中央災害防救委員會，有關災害防救工作之諮詢；另搭配由內政部設置「災害防救署」(未來將由消防署轉型)[33]，以及各地方政府依災害防救法第 9 條、第 11 條規定設置之災害防救辦公室，建構成我國之平時救災防害體系；另災時則係依據災害防救法第 13 條，由中央開設災害應變中心，並視災情研判通知直轄市、縣（市）政府成立地方災害應變中心。

而我國現有之防災管理政策，如中央災害防救會報之災害防救白皮書、災害防救基本計畫、災害防救業務計畫、地區災害防救計畫[34]，以及內政部消防署於提出之 2013 年度施政計畫[35]、安全管理手冊[36]等可認完備。

惟從前述日本、韓國經驗，可得見亞洲區域目前均面臨日益嚴峻的天然災害及極端氣候之威脅；尤以 2011 年東日本震災造成地震、

[33]內政部（2010 年）。*災害防救*。取自 http://www.moi.gov.tw/child/policy_six.aspx?type=rescue（最後瀏覽日：2013 年 11 月 13 日）。

[34]中央災害防救會報（2013 年，11 月 8 日）。*災害防救政策及計畫*。取自 http://www.cdprc.ey.gov.tw/Content_List.aspx?n=46C9D62372482D9D（最後瀏覽日：2013 年 11 月 13 日）。

[35]內政部消防署（2013 年）。*民國 102 年度施政計畫*。取自 http://www.nfa.gov.tw/main/List.aspx?ID=&MenuID=277&ListID=3591（最後瀏覽日：2013 年 11 月 13 日）。年度關鍵績效指標係建構完整災防體系，確保民眾生命安全。

[36]內政部消防署（2011~2012 年）。*安全管理手冊*。取自 http://www.nfa.gov.tw/main/List.aspx?ID=&MenuID=318（最後瀏覽日：2013 年 11 月 13 日）。

海嘯及核能災變等綜合型態的嚴重災害，我國同屬於環太平洋地震帶，對此更應有深刻體認；據此，我國國家安全層面之防災政策，宜可參酌前述同處亞洲區域之日本、韓國經驗以及其他先進國家、國際組織之策略：

1.宜持續投注心力對防災管理、應變、災害後果承受力與災後復原力四大面向進行規劃我之防災政策，以期盡可能降低災害發生時的損失並儘速完成復原工作。

2.強化現有之中央災害防救會報和中央災害防救委員會，建置其成為國家單一應變機制單位，成為具預測、監控、災害資料廣播分享聯絡功能之救災管理中心系統，並統籌應變流程，使中央、地方政府及一般民眾均能有一致且有效的防災、避災之應變模式。

3.考量與反恐、維護關鍵基礎建設之應變與恢復力政策結合，以「全災害防護」（All Hazard Approach）角度出發，使政府部門、私人企業間之三方協商機制，以因應併隨恐怖活動、生化威脅、天然災害、核子事故之複核性問題發生。

4.參酌相關國際組織之研究，如「歐盟面對極端氣候之應變措施套案（EU Adaptation

Strategy Package）」[37]等，以利我國防災政策、應變措施、經濟衝擊評估與國際趨勢接軌，面對嚴峻的氣候變遷挑戰。

二、國家機密與公務機密維護方面

本計畫「國家機密維護」主題所涉範圍包括：竊取國家機密事件始末及洩密管道；軍事、國防機密資訊之維護措施；政府通信、資訊保密技術、設備或設施；為確保涉及國家安全或利益之機敏資料之措施等相關資訊。而「公務機密維護」主題所涉範圍包括：包括重大洩密案件、機敏資料、資（通）訊設備維護措施等相關資訊。惟查國家機密與公務機密維護兩大議題有密切之攸關且議題屬性類似，，爰謹將此兩議題合併討論，提出下列分析與建議。

（一）機密等級之核定、變更與解密程序[38]

近年許多國家均逐漸著手進行政府資訊之透明化，但在政府資訊公開的立基上，對於涉及國家安全或公務機關依法令或契約應予保密之機密文書，也需遵循嚴謹的機密資訊規範機制，來作為公務機密在核定密等、變更機密等級、解除機密或維護管理時之依據。

我國對於「國家機密」[39]之核定、變更與

[37]同註1。

[38]請參見本報告附錄一、重要議題分析報告（二）論我國公務機關解決公務機密核密等及與解密程序爭議之思考-以美國國防部與美國國土安全部機密管理機制為例。

解密程序有詳細完整之規範，然「一般公務機密」[40]，處理依據為「文書處理手冊」，規範密度與考量細緻度上稍嫌不足，以下謹就四點宜家修正、強化之面向進行說明，並以美國為例提，觀察該國如何在政府資訊公開與國家安全資訊保護兩者間界定較為完善的平衡點。

1.我國宜就「一般公務機密」重新量身訂定統一化、細緻化、明確化之核密標準，以利遵循。

美國歐巴馬政府於 2009 年頒布第 13526 號行政命令（Classified National Security Information）[41]，該行政命令主要係規範涉及公務機密（包含國家機密與一般公務機密）之密等核定、機密維護與機密解密或降密等事宜。本號行政命令係美國聯邦政府機關在其職責內涉及公務機密之公務資訊，如何就前述資訊建立其內部公務機密管理機制的

[39]依據國家機密保護法第 2 條規定，「本法所稱國家機密，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，經依本法核定機密等級者。」是以，所謂國家機密，係指攸關於國家安全或國家利益之所有公務機密而言，在該範疇外的各類公務機密將不受國家機密保護法之規範（國家機密保護法施行細則第 2 條。）。

[40]依據行政院祕書處所頒布之文書處理手冊第 51 點規定，「一般公務機密，指本機關持有或保管之資訊，除國家機密外，依法令或契約有保密義務者。」是以，所謂一般公務機密，係公務機關基於各機關的業務作用法與因私法上所產生的權利義務關係，而持有國家機密以外之公務資訊且負有保密義務者。

[41]The White House(2013)・*Exec. Order No. 13526*・Retrieved from http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information (last accessed May. 1, 2013).

範本。而美國國防部（Department of Defense）為了遵循美國行政命令第 13526 號的指示，對於其業內公務機密，亦建立「美國國防部公務機密管理機制」[42]，制訂相關來防止該資訊受到外國或恐怖分子的刺探或取得。另美國國土安全部（Department of Homeland Security）為了落實第 13526 號行政命令，美國國土安全部就其業內公務機密，對於機密分類機制的履行、管理與監督亦建制「美國國土安全部公務機密管理機制」[43]。

據上所述，考量美國聯邦政府機關針對公務機密狀態爭議設有完整的處理程序，來供公務機密持有者當就手邊的公務機密狀態有所質疑時可提出異議。惟該國相關規範在機制設計，亦有以處理「國家機密機制」來處理「一般公務機密」之疑慮，致生的權重失衡問題。

是以，我國對機密等級之核定、變更與解密程序，宜可參酌美國公務機關落實第 13526 號行政命令（Classified National Security

[42]Department of Defense，*DoD Information Security Program: Overview, Classification, and Declassification*，Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/520001_vol1.pdf (last accessed May. 1, 2013).

[43]Department of Homeland Security Management Directive System，*Protection of Classification National Security Information Classification Management*，Retrieved from http://www.fas.org/sgp/othergov/dhs/md11044.pdf (last accessed May. 1, 2013).

Information）之經驗、並去蕪存菁，宜重新審酌公務機關處理一般公務機密的實際運作環境，訂定細緻化、明確化之核密標準，或要求各機關應建立統一指引，讓轄下各單位有所依循。

2.我國宜全面檢討、修正一般公務機密爭議處理機制，配套宜包涵：爭議之提出及處理程序、上訴之程序、人身或職務安全之確保機制

據我國文書處理手冊關於機密變更與解密程序的規定，僅對於未標示保密期限或解除機密條件者，原核定機關承辦人員應依檔案管理單位定期清查機密檔案之通知或依其他機關來文建議，將原檔案調出審查。此規定並未提供原核定機關承辦人員對該一般公務機密可能遭不適當核密的情形提出質疑的管道，亦無後序處理程序、上訴之程序、人身或職務安全之確保機制；未來宜檢討、修正一般公務機密爭議處理機制，配套如下：

（1）一般公務機密爭議之提出及處理程序

美國聯邦政府對於公務機密狀態爭議的處理機制，使公務機密持有者有主動

提出質疑的機制，包括非正式的口頭、或正式的以書面向原核定機關或資訊管理單位提出，並附以有完整描述為何認有不適當的理由。原核定單位或資訊管理單位應於法定期間內查核完畢，再以口頭或書面形式回覆提出質疑的公務機密持有者，是否變更機密等級或解除機密的決定。

據此，未來我國公務機關在設計一般公務機密爭議處理程序時，除應考慮一般公務機密與國家機密有本質與特性的差異外，也須考量現行我國行政機關處理一般公務機密的實際運作環境，來制定出切合行政機關需求的一般公務機密爭議提出及處理機制。

（2）一般公務機密爭議之上訴程序（救濟機制）

美國聯邦政府對一般公務機密爭議之上訴程序，係由提出質疑者對於原核定單位或資訊安全管理單位就公務機密狀態爭議所為的初期決定（可能為維持原機密等級或機密等級變更未符合預期時）不服時，得向由中立第三方組成之機關提起上訴，該中立機關係由國務

院、國防部、司法部、檔案局、情報總監辦公室和國家安全顧問指派資深官員組成委員會，進行複審。

是以，我國若能完善規劃我國一般公務機密之救濟處理機制，整體公務機密核定體系將能提高運作透明度與強化核定公正性的效果，落實程序正義之概念。

（3）一般公務機密狀態質疑者人身或職務安全之確保

美國國土安全部安全為防範提出質疑者遭到報復，例如降級、績效考核威脅、騷擾或其他歧視行為，係由國土安全部安全工作室成為提出質疑者的代理人，匿名的進行爭議處理機制。

據此，未來若我國欲建立此一機制，是否可由機關內部政風單位或上級機關政風單位，來提供必要之協助，可作為一思考方向。

（二）資訊分類分級系統細緻化：敏感性資訊概念之建立[44]

我國政府機關目前對於所持有及保管資料之處理，僅區分為「機密文書」與「一般文書」，因此當法規或業務實際上要求賦予一定安全維護措施時，業務承辦人為安全起見，多傾向於全部核定為「密件」，以 2012 年甫上路的「個人資料保護法（下稱「個資法」）」為例，由於個資法要求對於個人資料檔案應建立一定之安全維護措施，使公務機關紛紛將其視為密件去作處理。惟此將造成機密不再機密的窘況，例如國稅局、勞工局或戶政機關等例行業務即係為人民提供服務的機關，此種作法將造成整個機關所持有的全部資料都是密件，不僅會嚴重延宕行政效率，亦無法使人員感受到何謂保密的重要性。

藉由檢視個人資料保護事宜的契機，機關宜清楚建立「保護敏感性資訊」與「保護機密」兩者乃不同概念。各公務機關職掌業務種類繁雜，經手文書態樣不勝枚舉，除個人資料外，為制訂政策而蒐集資料、會議文件或其他敏感性資料，均有保密而不宜公開之需求，然而「保密」並不等同於必須當作現行一般公務機密去

[44]請參見本報告附錄一、重要議題分析報告（一）論公務機密之保護- 以因應個人資料保護法之修正為中心。

處理、保管和限制，而係指應按其敏感性高低，賦予不同等級的安全維護措施。又文書處理手冊第 51 條對一般公務機密之定義，仍無法清楚劃分一般公務機密之範疇，實宜利用此一重新檢視敏感性資料的機會，盤點所有含「有保持秘密之義務」、「不得洩密」的法令規範，檢視究竟係指需核密抑或只是應提供如個人資料保護法所規定的安全維護措施；承上所述，我國宜就相關措施進行檢討，分述如下：

1.檢討現行機敏性資料分級系統及相關配套措施

查考英國的機敏性資料分級系統（Protectively Marked Information）[45]，在國家機密以下，將餘下的敏感性資料區分為「限閱級（Restricted）」和「防護件（Protect）」兩階；前者類似於我國之一般公務機密、後者則是指不宜公開的敏感性資訊，如稅務資料、（Tax Data）國家保險（National Insurance）和個人資料檔案。

承前，我國或可考量，針對需保護但強度不及於公務機密者，多闢低一階之「防護件」進行規範，與一般文書相區隔，規劃屬於我

[45]Protective Mark(n.d.). *The Government Protective Marking System*. Retrieved from http://protectivemarking.co.uk/images/downloads/gpms.pdf (last accessed Feb. 18, 2013).

國之機敏性資料分級系統（機敏性資料泛指所有之國家機密、公務機密與敏感性資料）。

2.整合資訊安全管理與個人資訊管理系統，建立全面性資安文化

為有效運作機敏性資料分級系統，相關之核定標準、分級處理及安全維護措施等配套機制亦必須併同建立。雖然各級機關單位之業務種類不一，仍建議或可由立法機關建立如英國機敏資料分級系統（Protectively Marked Information）之框架並命適當之機關進行配套機制與細節性規定之設計，再由如資通安全會報辦公室或其他具合適性之機關制訂分類分級標準，所有政府機關（不限於行政院及所屬機關）即有所依循並負一定法遵義務，依法辦理相關事宜，例如：由各部門的資深主管組成專責小組，按業務特性商討核定標準及核定流程，每年至少重新檢視一次核定標準，並開辦教育訓練培養業務承辦人鑑別資料價值的能力；宜規定業務承辦人應以書面記明核定為密件或限制件之理由，並定期檢查核定妥當性、解密條件及保密期限之適當性等。

（三）涉密人員之管理監控機制

近年因應政府組織改造，為活化公務人力運用、降低財政負擔及運用民間專業人才之資源，原則上就公共服務或執行性質之業務得全權委外、內部事務或服務如資訊、保全、清潔等亦得部分委外。

理論上，前開業務類型確實較不會涉及機密之使用（Access），惟實際面上仍有安全上之疑慮。例如美國政府便強烈建議禁止公、私部門使用中國電信設備商「中興」和「華為」作為資訊設備承包商，蓋其有利用建置網路系統標案的機會從事間諜活動之嫌疑。又清潔人員亦可能藉由清潔或處理垃圾時，拾得廢棄但未安全銷毀之機密檔案紙本或竊聽相關談話，進而對外洩漏。

此外，針對掌握或持有機密之公務人員，我國相關保密規範如保密義務、範圍及違反之相關罰則等，多聚焦於「在職者」。針對「退離職者」的規範非常有限，亦無準用「在職者」保密規範之明文。除此之外，各法律之間如國家機密保護法、公務員服務法、公務人員懲戒法及民刑法等就保密機制之設計均不相同，而可能產生具體個案適用時，產生部分競合、名詞解釋之衝突或概念上之模糊、矛盾等問題（如針對保密義務之範圍即無一致之定論），

而難以遵循。

承前，為求機密維護相關機制妥善性與完整性，我國未來法令規範之修正可先從下列三方面著手：

1.宜強化廠商人力來源評選機制[46]

我國現行法令所明文的評選廠商標準[47]著重在外在的「設備設施」、「經驗」、「實績」、「財務狀況」及「技術人員的技術及資格認證」，忽略了身家是否清白（如未與恐怖組織有涉或有參與間諜活動之嫌）的查核與「可信賴性」、「忠誠度」及「正直」等品德項目評鑑（如有高度動機或傾向洩漏國家機密）；其次，我國並未依資訊系統安全等級或機關資安責任等級，建立各機關統一適用之廠商評選標準，僅由招標機關個案操作；末者，機關的把關責任似乎僅需於招標文件中要求廠商提供證明文件，被動的進行書審，然而單純的形式審查，在特定具敏感性的採購案似難以達成政府機關所負的資訊安全維護責任。退步言之，縱使不在評選階段進行審

[46]請參見本報告附錄一、專題分析報告（二）為維護國家安全並因應資通安全政策之資訊業務採購評選廠商標準—以廠商人力來源之背景安全查核為核心。

[47]我國關於資訊服務廠商資格審查的評選項目，主要規定於「機關委託資訊服務廠商評選及計費辦法」、「行政院所屬各機關資訊業務委外服務作業參考原則」及「投標廠商資格與特殊或巨額採購認定標準」。

查，機關也並未在確定得標廠商後對工作人員名單進行安全背景查核的法源依據、程序、資源和認知。

查英國政府對其公務機關內部人員（包括公務員、約聘僱人員及承包商的執行人員）之管控，都必須通過基本的背景查核程序[48]（包括身份認證、工作經歷、國籍、移民地位等）；又若因業務執行而有可能接近機密資訊者，按所涉機密性之高低，需通過不同等級之「國家安全查核程序」（National Security Vetting），分別為：（1）反恐查核（Counter-Terrorist Check/簡稱 CTC）、（2）防禦查核（Security Check/簡稱 SC）、（3）進階查核（Developed Vetting/簡稱 DV）。查核內容可能包括刑事紀錄、查核問卷、更詳細的工作經歷、一定期間之居住證明、軍情 5 處的安全紀錄、財務狀況或身心健康鑑定等，以確認其「身分（Identity）」，且應具有「可信賴性（Reliability）」、「可靠程度（trustworthiness）」及「廉正誠實（Integrity）」等良好的品德。

惟我國若欲進行前開所建議之安全背景查

[48]英國聯邦政府於 2012 年修訂了安全維護政策架構(HMG Security Policy Framework April 2012)，並據架構制訂機關安全責任辦法(Industrial security – departmental responsibilities)、招標時的指導守則(Industry security notice(ISN)2011-4、2010-03)、英國聯邦政府查核政策聲明(Statement of HM Government's vetting policy) 及數部相關規範。

核，會有干涉人民基本自由權利和侵入隱私領域的問題，根據憲法第 23 條之法律保留原則，必須由法律加以授權方能為之。

據此，我國或可考慮強化廠商人力來源評選機制，謹提出三個強化面向：

（1）現行政府採購法增擬訂授權條文，賦予機關在具國家安全、機關安全等敏感性招標案時，得對廠商及人力來源的安全性擁有主動查核的權限，警政機關及情報機關於該特定目的下有配合查核之協力義務。

（2）針對「資訊業務」委外的部分，再於「機關委託資訊廠商評選及計費辦法」第 7 條，研增訂「廠商使用人力來源之背景安全查核」的評選項目，並於同條增訂第 2 項，定義人力來源並做列舉（如負責人、高階主管、技術人員、計畫主持人），具體的步驟和執行程序，建議同評選項目擬訂於同辦法內。

（3）強化機關責任，擬訂特定機關採購資訊服務或其他機關採購高安全等級資訊系統或涉及國家機密的資訊服務時，負有主動查核、核對廠商所提供資料及證

明文件（包括法人本身及其人力來源）的義務，機關認有必要時得請求警政單位或相關的公私部門配合，提供資料、紀錄或相關證明文件以審查受查核人的適格性，可考慮研發機關間連線的公文系統，省去紙本作業的耗時問題。

2.公務機關宜制訂完善的公務機關電子機密資訊系統內部威脅預防偵測及因應之政策機制與配套[49]

依據行政院主計處針對電子化政府資通安全推動現況與展望的作業報導[50]指出，我國之資通安全威脅，以來源進行區分，可分為「外部威脅（External Threat）」[51]與「內部威脅（Insider Threat 或 Internal Threat）」[52]；且有 8 成的資安事件及資訊外洩是來自於內部人員問題（即內部威脅），包括惡意洩漏及

[49]請參見本報告附錄一、專題分析報告（一）公務機關電子機密資訊系統面對內部威脅之作法。

[50]行政院主計處（2011 年，9 月）．*政府機關資訊通報第 287 期*，第 1 頁．取自 http://www.dgbas.gov.tw/public/Data/18261414671.pdf（最後瀏覽日：2012 年 11 月 30 日）。

[51]外部威脅（External threat）係指該威脅非由組織內部發生，而是由組織外部之人員或其他組織，透過一般的網際網路、互聯網系統，以未經授權之方式，對該組織之資訊設備，以植入惡意程式、或以駭客入侵等方式，進行侵入式的資訊系統攻擊，其目的係在於由外部取得該組織「有價值」的資訊。

[52]內部威脅（Insider Threat 或 Internal Threat）係指例如內部竊盜、系統失敗、惡意破壞、不遵守安全準則或是使用非法軟體等；相對外部威脅，係指自然災害，例如火災與地震，以及來自外部的惡意攻擊，例如盜賊、駭客、惡意程式，以及網路病毒等。

因資安意識不足而造成的疏失，但現行資通安全政策向來注重外部的駭客攻擊，近年來才慢慢將注意力放在內部威脅的管控，包括機關內部人員及委外廠商。

我國行政院及所屬各機關資訊安全管理要點第 27 點規定，機密資訊原則上不得以電子郵件或其他電子方式傳送；惟因機關業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，同點第 3 項規定得採用權責主管機關認可之加密或電子簽章等安全技術處理。此外，國家機密保護法施行細則第 21 條亦規定「以電子通信工具傳遞國家機密者，應以加裝政府權責主管機關核發或認可之通信、資訊保密裝備或加密技術傳遞」；我國公務機關現今（2013 年）對於機密資訊之管理與防護之實務作法，多採紙本方式輔以自然人憑證管理電子文件之作法，且使用隔離電腦、密碼行動碟，與加密隨身碟；惟自然人憑證之使用，僅能「辨識身份」，但並不一定是憑證的所有者載在使用資訊系統，故是否能有效達成防堵「內部威脅」和事後追查的目的效果其合適性應再三斟酌。

查美國歷經 2001 年 911 事件以及 2010 年維基解密等機密外洩事件後，建立了一系列監

控內部威脅的政策及法制措施，包括以行政命令發布內部威脅政策及最低監控標準[53]；而各機關如國防部（Department of Defense, DOD）的「網路內部威脅計畫（The Cyber-Insider Threat Program-CINDER）」、商務部「聯邦資訊系統與組織之安全與隱私控制（Security and Privacy Controls for Federal Information System and Organizations）草案」第四版（SP 800-53 Rev. 4）[54]也都各自訂立了內部威脅指引；前述內部威脅政策及最低監控標準，規範重點均包括了：對於內部人

[53]FEDERATION OF AMERICAN SCIENTISTS, (n.d.), *Obama Administration Documents on Secrecy Policy*,Retrieved from http://www.fas.org/sgp/obama/index.html (last visited Nov. 30, 2012). 歐巴馬政權針對機密資訊發布多項正式文件，以年度區分，截至 2012 年 11 月 30 日止，包括下列：1. 2009 年：「機密資訊和受管控的非機密資訊的總統備忘錄 (Presidential Memorandum on Classified Information and Controlled Unclassified Information, May. 27, 2009) 」、「第 13526 號行政命令-國家安全機密資訊 (Executive Order 13526: Classified National Security Information, Dec. 29, 2012) 」，與「國家安全機密資訊施行令的總統備忘錄 (Presidential Memorandum on Implementation of the Executive Order on Classified National Security Information, Dec. 29, 2009)」；2. 2010 年：「第 13549 號行政命令-國家、地方、部落，和私部門實體的國家機密方案 (Executive Order 13549: Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, Aug. 18, 2010) 」與「第 13556 號行政命令-受管控的非機密資訊 (Executive Order 13556: Controlled Unclassified Information, Nov. 4, 2010) 」；3. 2011 年：「第 13587 號行政命令-增進機密網路安全與機密資訊有責分享及安全維護的結構性改革 (Executive Order 13587: Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, Oct. 7, 2011) 」；4. 2012 年：「國家內部威脅政策和機關內部威脅方案的最低標準備忘錄 (National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, Nov. 21, 2012) 」。

[54]NIST. (Feb. 28, 2012). *Draft Security and Privacy Controls for Federal Information Systems and organizations* (Initial Public Draft). Retrieved from http://csrc.nist.gov/publications/PubsDrafts.html (last visited Nov. 30, 2012).

員及委外廠商都應接受一定的安全查核程序、以科技技術加以監管（例如偵測短時間內大量下載檔案或轉出信件、消費力顯著提高或情緒起伏大）等證據，進一步預防內部威脅的發生等。

近年來，我國公務機關同樣也面臨電子機密資訊系統內部威脅之問題，謹據前述美國實務經驗，提出二個修正面向供參：

（1）全面檢視機密資訊管理與保護政策與法制、配套標準及措施，並對機密資訊的管理與「內部威脅」的防範進行全面檢討。

（2）全國公務機關應有統一、水平的防範措施，例如，可先採取使用統一的公文系統，便能有效採取相同的保密措施，將資訊外洩的風險降至最低。

3.調和退離職公務人員保密規範[55]

我國公務人員保密義務之發生時點，系源自於其以法制架起其公務人員的身分[56]，一旦成為公務人員，即有保密義務，縱使於受訓

[55]請參見本報告附錄一、專題分析報告（四）涉密公務人員退離職後之保密。

[56]公務員服務法第 4 條規定，「公務人員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務，均不得洩漏，退職後亦同。公務人員未得長官許可，不得以私人或代表機關名義，任意發表有關職務之談話。」

期間尚未分派任務、退離職，或是被免職，保密義務仍然存續[57]。

依公務員服務法第 4 條第 1 項規定，「公務人員有絕對保守政府機關機密之義務，對於機密事件無論是否主管事務，均不得洩漏，退職後亦同。」；本條所稱之「機密」，又可二分為「國家機密」與「一般公務機密」，公務機關對於有關國家機密事項的機密文書，依國家機密保護法第 2 條[58]、國家機密保護法施行細則第 2 條[59]、文書處理手冊[60]第 49 條以及相關規定辦理。

---

[57]司法院大法官釋字第 637 號解釋文「『公務員服務法第十四條之一規定：公務員於其離職後三年內，不得擔任與其離職前五年內之職務直接相關之營利事業董事、監察人、經理、執行業務之股東或顧問。』旨在維護公務員公正廉明之重要公益，而對離職公務員選擇職業自由予以限制，其目的洵屬正當；其所採取之限制手段與目的達成間具實質關聯性，乃為保護重要公益所必要，並未牴觸憲法第二十三條之規定，與憲法保障人民工作權之意旨尚無違背…公務員離職後與國家間公法上職務關係雖已終止，惟因其職務之行使攸關公共利益，國家為保護重要公益，於符合憲法第二十三條規定之限度內，以法律課予特定離職公務員於一定條件履行特別義務，從而對於其選擇職業自由予以限制，尚非憲法所不許。」

[58]國家機密保護法第 2 條規定，國家機密係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，依該法認定機密等級者。

[59]國家機密保護法施行細則第 2 條

本法所定國家機密之範圍如下：

一、軍事計畫、武器系統或軍事行動。

二、外國政府之國防、政治或經濟資訊。

三、情報組織及其活動。

四、政府通信、資訊之保密技術、設備或設施。

五、外交或大陸事務。

六、科技或經濟事務。

七、其他為確保國家安全或利益而有保密之必要者。

[60]行政院秘書處（2010 年）。*文書處理手冊（第五版）*。取自 http://www.rdec.gov.tw/lp.asp?ctNode=14706&CtUnit=1813&BaseDSD=7&mp=100（最後瀏覽日：2013 年 5 月 11 日）。

我國對於「公務機密」並無於法規中加以定義；惟實務運作上，對於公務機密的內涵與範圍，則係以法令所規定「應秘密」之事項，包括：涉及檢舉人身分、個人資料與民眾隱私，或政府機關行政運作之內部資訊（人事或採購作業等），應予保密資訊。另若屬於未規制為國家機密或公務機密的「其他應保守秘密之公務資訊」，依學界目前通說「形式與實質秘密複合說」，係指形式上已被認定為公務機密者，且在實質上具有保護的價值之公務資訊，為「應保守秘密之公務資訊」，避免公務人員負擔過重的保密義務。

另查諸我國有關保密義務違反之刑事責任[61]、行政責任[62]、民事責任[63]，均聚焦於居於「職務任期內之公務員」；而「退離職公務人員」係至退離職後，才洩露或交付因其之前任職公務而知悉或持有之機密資訊，故前述規範是否適用於退離職公務人員洩露或交付先前任公務時所知悉或持有的機密資訊的特定情形，亦有疑問[64]。

[61]如為洩露與國家安全與利益有關的機密資訊，國家機密保護法訂有相關罰則於第 32-38 條。另於刑法當中，與秘密相關之刑事責任可分為「洩露國防機密罪（刑法第 109 條、第 110 條）」、「洩漏一般機密罪（刑法第 132 條）」、與「洩漏工商秘密罪（刑法第 317 條、第 318 條）」。

[62]公務員服務法第 13 條第 3 項、公務員服務法第 22 條、國家機密保護法第 38 條等。

[63]民法第 186 條公務員之侵權行為責任。

[64]例如刑法第 132 條第 1 項係為「公務員」洩露或交付國防以外機密（一般機密）

查美國總統第 12958 號行政命令 Sec.4.2（a）規定使用機密資訊的一般限制[65]：聯邦政府員工使用機密資訊前，必需符合下列三大前提要件，包括通過「人員安全查核（Personnel Security Investigation）」、「簽署保密協議（Classified Information Non-Disclosure Agreement，一般簡稱為 NDA）[66]」、「與執行職務所必要知悉（Need-To-Know）」，才得以使用機密資訊[67]。尤其以「簽署保密協議」在法律上為拘束簽署員工（前述通過安全查核之人員）與美國政府間的契約（Contract）[68]，規範該政府員工對於機密資訊的維護，

之規定，既然退離職公務人員已不具備公務員身分，使用此項進行處罰，不無疑義；如果以其第 3 項「非公務員因職務或業務知悉或持有」機密資訊觀之，則產生退離職公務人員知悉或持有機密資訊之「時點」，係身為「公務員」之時，洩密的時點係為「退離職之後」，而產生構成要件未必完全合致的情況。

[65]White House・*Executive Order 12958 Classified National Security Information (1995)*・Retrieved from http://www.fas.org/sgp/clinton/eo12958.html (last accessed May 11, 2013).
(a) A person may have access to classified information provided that:
(1) a favorable determination of eligibility for access has been made by an agency head or the agency head's designee;
(2) the person has signed an approved nondisclosure agreement; and
(3) the person has a need-to-know the information.

[66]NARA/ISOO・*Standard Form 312*・Retrieved from http://www.archives.gov/isoo/security-forms/sf312.pdf (last accessed May 11, 2013).
「保密協議」應經過「國家安全委員會（National Security Council）」批准，與「司法部（Department of Justice）」的審查，而為法院可執行，而且機關不得接受經簽署員工單方修改用語的「保密協議」。目前「保密協議」版本稱為 312 制式表格（Standard Form 312）。

[67]NARA/ISOO・*Classified Information Nondisclosure Agreement (Standard Form 312) Briefing Booklet (2001)*, P.1・Retrieved from http://www.fas.org/sgp/isoo/sf312.html (last accessed May 11, 2013).

[68]NARA/ISOO・*Implementing Rule of the "Classified Information Nondisclosure Agreement" Subpart B-Prescribed Forms §2003.20(a) (n.d.)*, P.55・Retrieved from

載明雙方的關係、政府員工的保密責任，以及違反保密協議的後果，並強調該保密協議的效力，一直持續至該員工的終身，這意味著，政府員工於不具安全查核的資格之後，或甚至是退離職之後，仍受保密協議的拘束。

因此，美國政府對於未經授權而揭露的機密資訊，係利用違反保密協議（違約，Breach of Contract）為手段，儘量減少機密資訊擴散的程度。再者，透過禁制令的方式，凍結並維持資訊的「現有狀態（Status Quo）」，並且還得於提起民事訴訟的同時提起刑事訴訟。

我國最常發生之退離職人員洩密案，多係因對於所揭露資訊是否實際上仍屬於機密（雖可能未經解密但實際上該政策已執行完畢或已為公眾所周知）產生爭議。為解決此一爭弭，美國維護機密的作法與概念，仍然有許多值得學習或參考之處；是以，謹對調和退離職公務人員保密，提出二個修正面向供參：

（1）機關內部密等認定指引與資訊揭露事前審閱機制

http://www.wrc.noaa.gov/wrso/forms/standard-form-312_booklet.pdf (last accessed May 11, 2013).

建議機關宜建立內部機密認定指引，增進公務人員對於機密資訊狀態的了解，以及保密義務是否持續；並將確認保密範圍列入退離職辦理程序內，且要求退離職人員日後欲揭露資訊時，應先提出予曾任職機關進行事前審閱（Pre-Publication Review）[69]。

（2）調和「退離職公務人員」保密相關規範

可參據前開美國作法後，訂明及調和不同法規範間有關退離職人員之保密義務、範圍及罰則的規定。復得以保密協議進行落實，不僅能強化退離職人員之義務、亦能於紛爭發生時視為已盡告知義務之證據，減輕機關舉證責任之負擔。

三、機關安全方面[70]

本計畫「機關安全維護」主題所涉範圍包括：危害機關或關鍵基礎設施之爆炸、破壞事件；偶突發意外事故、機關首長安全、重大陳抗事件；選舉或重大節慶期間之安

[69]類似「公務人員基準法草案」第 28 條第 3 項的概念，「公務人員就應守秘密之事項為證言時，應經服務機關或原服務機關之許可。」。該條文僅規範「公務人員」，對於「退離職公務人員」未有規範。為求縝密保護公務機密，或可於該條增訂「退離職公務人員」為秘密事項揭露時，應經服務機關或原服務機關之許可

[70]請參見本報告附錄一、專題分析報告（五）機關安全維護之研析–以實體設施及人員安全維護為核心。

全維護等相關資訊。

我國機關安全維護事項，查「政風機構人員設置管理條例」第 4 條第 8 款，係由政風機構執掌「機關安全維護處理與協調」，再依「政風機構人員設置管理條例施行細則」第 10 條第 2 款，其他應推行之政風事項包括了「危害或破壞本機關事件之預防事項」，法務部據此訂定了「政風機構預防危害或破壞本機關事件作業要點」[71]。除前開規定外，參行政院於 2005 年 6 月 29 日發佈的「安全管理手冊」[72]，機關安全維護的主要內涵，在於建設實體設備、設施及辦公環境的實體安全性，保護並同時管理、監督機關內部人員（包括公務人員、替代役、約聘人員、派遣人員及委外廠商駐點或執行人員）、訪客及洽公民眾，藉由對人員出入和設備設施使用的管控，確保機關實體安全性不會因內部侵入、外圍攻擊或其他天災人禍而有所減損或破壞。

又我國行政院曾於 2005 年 8 月 24 日通過「健全機關組織功能合理管制員額作業要點」[73]（已於 2009 年 8 月

[71]「政風機構人員設置管制條例」已於 2012 年 2 月 3 日修正，惟尚未訂施行日期，而其施行細則至 2000 年 1 月 12 日訂定施行至今，卻並未隨新法一併修正，造就施行細則未來可能會有無訂定依據、相關規定與新法無法相呼應的矛盾現象，蓋依新法，施行細則之訂定依據為第 12 條，而現行施行細則第 1 條明文「本細則係依.....（以下簡稱本條例）第 13 條規定訂定之」；又如新法對政風機構掌理之「其他政風事項」列於第 4 條第 8 款，然應與其相呼應之施行細則第 10 條，仍沿用舊法之條項：第 5 條第 7 款。茲建議主管機關應配合新法（縱使其尚未正式施行）儘速研議修訂施行細則，爰併此敘明。

[72]行政院內政部消防署（2005 年，6 月 29 日）．*安全管理手冊*．取自 http://www.nfa.gov.tw/main/List.aspx?ID=&MenuID=318（最後瀏覽日：2013 年 11 月 1 日）。

[73]行政院（2005 年，8 月 24 日）．*健全機關組織功能合理管制員額作業要點*．取自 http://weblaw.exam.gov.tw/LawArticle.aspx?LawID=J060015002（最後瀏覽日：

21 日廢止），鼓勵機關將適合委託民間辦理之業務盡可能委外，使得我國公務機關普遍仍偏於使用民間保全業者擔負實體安全維護工作。惟我國對於保全業之管制，法制設計上稍嫌不足，且保全人員流動性偏高、與機關間並無直接的僱傭關係，不易管理監督，因此流弊滋生。

近年來澳洲政府提出「實體安全管理指引：管制區及風險減輕控制」（Physical Security Management Guidelines - Security Zones and Risk Mitigation Control Measures）[74]等政策、措施[75]，使得公務機關對於場所、設備設施[76]及出入之內外部人員安全（Personnel Security）[77]之控管，有嚴謹縝密的管理機制與具體作法；據上相較，我國機關防護性安全政策及實體安全管理機制仍有待加以細緻化、強化，以下謹提出三個修正面向供參：

2013 年 11 月 1 日）。

[74]Australian Government，*Physical Security Management Guidelines - Security Zones and Risk Mitigation Control Measures*，Retrieved from http://www.protectivesecurity.gov.au/physicalsecurity/Documents/Security-zones-and-risk-mitigation-control-measures.pdf (last accessed Nov 13, 2013).

[75]Australian Government，*Australian Government Protective Security Policy*，Retrieved from http://www.protectivesecurity.gov.au/pspf/Pages/default.aspx (last accessed Nov 13, 2013).細部資料請參見本報告附錄三、計畫成果 - 資訊雙週報第 05-01、05-02、06-01、07-01、09-05、10-05、11-06、12-06、13-05、14-06、15-06、16-06、17-05、18-07、24-09、25-05、25-09、26-09 期。

[76]如澳洲風險管理標準 AS/NZS ISO 31000:2009（Australian Standard for Risk Management AS/NZS ISO 31000:2009）、澳洲 HB 167:2006 安全風險管理標準（Australian Standards HB 167:2006 Security risk management）、安全風險管理的配套指引（Supporting Guidelines for Security and Risk Management）等。

[77]Australian Government，*Australian Government personnel security management protocol*，Retrieved from http://www.protectivesecurity.gov.au/personnelsecurity/Documents/Australian%20Government%20personnel%20security%20management%20protocol.pdf (last accessed Nov 13, 2013).

（一）宜研擬建置更細緻化之機關安全維護框架

公務機關應對於實體安全維護的具體作法建置明確性、細節性的規範，強化自身之警醒程度，不宜過度仰賴委外安全維護廠商的安全管制建議；謹提出三個強化面向：

1.我國公務機關目前僅有「責任區」[78]的概念，可考慮引進澳洲「分級管制區（Security Zone）」[79]以及「關鍵路徑規劃(Critical Path)」[80]之概念，依風險評估的結果，對辦公場所進行區域及動線之劃分。

2.和民間企業共構合署之機關或有大量洽公民眾出入之機關，宜藉由建置門禁管制、巡邏安排、專人全程陪同訪客、機房重地限兩人以上停留、全天候監視（CCTV）系統監控等標準作業流程，以強化實體安全措施。

[78]「責任區」，係指將辦公場所劃分為數個區塊，由各區塊所在單位派一專人負責協調與處理該區的照明、水電、門禁管制、巡邏等安全維護事項等，避免某些公共區域或混合使用區域無人負責而導致安全漏洞。

[79]管制區（Security Zone）共分五個等級（一級管制區 Zone One ～五級管制區 Zone Five），亦即依風險評估的結果，對辦公場所進行區域劃分，並賦予相應的管控措施 。劃分不同層級的管制區可以延遲外人侵入的時間，有利於機關對侵入事件有餘裕進行適當的防禦回應。

[80]「關鍵路徑規劃」(Critical Path）係指辦公場所動線的設計，與有效的安全控制攸關，從外來危險的入侵到進入到辦公的核心區域，在動線上要讓應變小組有時間偵測到敵人、延遲敵人侵入到管制區的時間、並來得及回應和阻止侵入，並且讓入侵者無法快速、直接的到達目的地。

3.參據澳洲對於監控、入侵偵測及通報聯防等電子警報系統（Alarm Systems）的管理，三級以上管制區部分應由機關內部、受過訓練的專人直接管控。

（二）建議機關審酌自身需求性，考量於組織內編列保安人員

蓋專職維安人員因具備工作穩定性、歸屬感及位於行政體系內，較易培養責任感、榮譽心及向心力，除能運用其所學確實的指導、管理和監督值勤委外保全人員，尚能避免後者直接接觸機敏性高的資產和區域，有效阻絕帶槍投靠或因利洩密的風險。

（三）優化委外保全服務時之注意事項與配套機制

就實際執行任務之保全從業人員部分，機關可考量自身實際需求，是否要進行額外的安全查核作業，例如是否背負顯不相符收入之貸款、歷往工作經驗不穩定、性向測驗評估人格穩定度或有無憂鬱症或躁鬱症等，蓋保全人員得監看監視器（CCTV）系統和對工作場所進行巡邏，對於人員活動狀況及生態弱點相當清楚，不適合由具潛在洩密誘因者擔任。又機關得與委外之保全業者配合，提供一定福利及相當之薪資，使保全人員有意願長期服務和有餘

力進行專業能力進修，可節省機關重新適應和教育的成本，傳承和落實實體安全維護政策和措施。

四、資通訊安全方面[81]

本計畫「資通（訊）安全」主題所涉範圍包括：駭客網路攻擊事件及其發展趨勢(如社交工程、封包攻擊...等)、資安及通訊洩密事件、網路安全設備、最新病毒資訊、資訊網路安全政策、最新資訊安全認證、防火牆及措施等相關資訊。

惟打擊網路犯罪，公私部門和國際結盟合作等資通（訊）安全之政策、措施，已付如前述，請參見本報告第伍大點、一、(三）部分；以下謹敘討「關鍵資訊基礎建設之資訊安全方針和作為強化」部分。

電力與電信供給設施係屬維持國家安全、政府運作、民生及經濟秩序的關鍵基礎建設設施。根據經濟部能源局統計，預計 2025 年時，電力需求將占總能源消費需求 55.7%；因此，我國未來能源發展政策應朝確保能源供應之安全性、避免能源供應短缺之情況發生、同時減少對環境的衝擊三方面來進行。為達成前開目標，各國的關鍵資訊基礎建設（Critical Infrastructure）均以建置智慧電網（Smart Grid）為首要施政方向，參經濟部建設委員會，已整理出主要國家推動智慧電網的相關政策。

[81]請參見本報告附錄一、專題分析報告（三）智慧電網系統安全維護研究報告。

美國透過「美國復甦與再投資法案（American Recovery and Reinvestment Act）」[82]推動智慧電網相關投資補助、測試及人才培育專案；歐盟推動「歐洲科技平台計畫（European Technology Platforms）」[83]藉以推廣智慧電網；日本推動「離島智慧電網計畫」；韓國制訂「國家智慧電網路線圖（Korea Smart Grid Roadmap）」[84]，並支持國內企業籌組智慧電網測試聯盟，推動示範與測試計畫；中國大陸則將「智慧能源網」納入「十二五」計畫，積極擬定智慧電網發展規劃綱要、關鍵技術研究框架，以及相關技術標準[85]。

智慧電網係指，透過在傳統電網上建設高速通訊網路，利用感測、分析、預測、決策、控制等資訊處理技術，提供穩定的電力供應、降低用電量並能提升使用端的能源效率，尚能導入再生能源併網發電，抑制尖峰負載及節約能源。惟傳統電力控制系統因其獨立封閉及專用系統的特性較無安全性的疑慮，而智慧電網之建置因需使用網路進行即時資料交換及無接縫的通訊系統，將產生系統開放性，又為維系統穩定性及系統可用性，會傾向採用一般通用資訊軟體與標準通訊協定的網路進行傳輸，間接的犧牲資訊

[82]U.S.A.，*American Recovery and Reinvestment Act*，Retrieved from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf (last accessed Nov 13, 2013).

[83] European， *European Technology Platforms (ETPs)*，Retrieved from http://ec.europa.eu/energy/renewables/platforms_en.htm (last accessed Nov 13, 2013).

[84] Korea， *Korea Smart Grid Roadmap*，Retrieved from http://www.smartgrid.or.kr/10eng4-1.php (last accessed Nov 13, 2013).

[85] 行政院經濟建設委員會（2010 年），*智慧電網對我國之機會與挑戰*，取自（最後瀏覽日：2013 年 2 月 27 日）。

安全的要求。

因此，智慧電網可能面臨的攻擊威脅包括：

（一）利用蠕蟲、木馬等惡意程式進行資訊攻擊癱瘓電網的運作。

（二）系統安定性與成本，軟硬體設備的使用週期會盡可能的拉長，而無法因應資通訊安全之需求即時汰換產品或採用最新的資訊安全技術，導致資訊攻擊的成功門檻降低。

（三）電力工業控制系統優先重視可用性，然後才是完整性與機密性，恰與資訊系統的考量順序相反，因此電網所使用的通用資訊產品，其資訊安全等級可能比一般常用的資訊系統落後5到10年。

參據日本的「離島智慧城市計畫（島しょ型スマートグリッドモデル地域計画）」內閣官房資訊安全中心針對關鍵資訊基礎建設所擬訂的資訊安全方針和作為，我國可藉由下列方向建構智慧電網的資通訊安全性：

（一）參考國際關鍵基礎建設及其通用的工業控制系統的資訊安全標準擬定符合我國實際需求之標準。

（二）規劃關鍵基礎建設及其工業控制系統的資訊安全標準認證制度。

（三）建置關鍵基礎建設及其標準化及認證所必要的實驗場域。

（四）加強關鍵基礎建設及其工業控制系統面臨或發生攻擊或事故的應變組織及作法。

（五）培訓相關專業人才及持續教育訓練、宣導。

我國目前為因應智慧電網可能遭遇之資訊攻擊，僅有國家通訊傳播委員會對於網路資訊安全的政策計畫與稽核和行政院科技顧問組（現行政院科技會報辦公室）所提出之「關鍵資訊基礎建設保護政策指引」，均僅及於行政指導的層級，欠缺法源依據及對於要求民營化關鍵基礎建設業者的強制力。

是以，為強化關鍵資訊基礎建設之資訊安全維護要求，宜考量儘速制訂專法，授權單一主管機關執掌整體資訊安全維護事項，進行跨部門的資訊溝通、協調並針對不斷發生的資訊攻擊方法進行資訊蒐集、通報及消息發布。此外，可考慮由專法授權各關鍵基礎建設的目的事業主管機關稽核權力，查核所有公、民營關鍵資訊基礎建設是否已落實資訊安全防護之要求。

再者，可考量由專法授權建置作資訊安全技術研發機關，專責研發各類資訊安全防護作法，並使所發布安全防護的作法透過目的事業主管機關的查核能落實於各關鍵基礎建設中關鍵資訊基礎建設上，並建置「ICS 緊急應變小組（Industrial Control Systems Cyber Emergency Response Team /ICS-CERT）」，針對智慧電網等關鍵基礎建設及關鍵

資訊基礎建設發生遭到攻擊或事故時進行危機管理，方能順利對應。

據此，方能對智慧電網等關鍵資訊基礎建設，此一橫跨不同主管機關管轄之領域，進行全面性、完整性的管理及措施研議。

另外，若從我國建置智慧電網的主角，台電公司的角度觀之，若為確實達成資訊安全之要求，宜在設計智慧電網工程的同時，依國際標準 ISA99/IEC6244 建置資訊安全管理制度，依國際標準進行資訊安全管理制度的政策擬定、程序、執行與要件，並確實落實管理制度的運作，之後若能輔以專責單一主管機關的查核機制，便足以防範前開所提及之隱憂。

陸、結論與建議

本計畫之 5 大議題：國家安全、機關安全、國家機密維護、公務機密維護與資通訊安全政策，彼此間看似獨立，實則牽一髮動全身，猶如蜘蛛網般彼此影響牽制。是以，計畫面上，若我國政府欲建構完善、細緻、具前瞻性且不過度疊床架屋的整體安全維護策略架構，宜採取長期監測性的觀察、研究與分析，包括對世界各主要國家的動態，及國內各機關（構）的個別運作現況及待處理之困境，方能進行有效的總體規劃。我國的政府組織結構與法制設計上，就本計畫 5 大議題的安全維護能量上，具有發散之特性，故宜重視整合資源及跨部會協調等手段，來強化及改善現況。

再者，觀察釋出完整制度文件的國家，如英國、澳洲，針對「安全」此一議題，均設計有完整的安全維護政策框架及下位階的具體指導文件。以澳洲為例，澳洲政府分別發布了「國家安全戰略（Strong and Secure： A Strategy for Australia's National Security）」、「防護性安全政策架構（Australian Government Protective Security Policy Framework, 簡稱 PSPF）」及「網路安全策略（Cyber Security Strategy）」，而於「防護性安全政策架構」下，主要是針對國內的人員安全、資訊安全（包含機密性資訊）及機關實體安全三大面向做通盤的設計規範，包含應遵行的法律義務及技術標準，使各機關（構）及單位能依具體步驟按部就班，同時也明確知悉能彈性裁量的空間有多大。相較於此，我國於機關安全、機密維護及資通安全政策上，法規與相關制度文

件相對上發散且多傾向以行政規範進行指導，並由各個機關（構）自行設計細節性的內部行政規則，係以彈性及易於隨實際需求進行修改為考量。然而伴隨而來的問題是容易各自為政、不易上級機關有效的統一管理或跨部會整合、修正及調整且資訊欠缺公開透明之特性，當涉及法規競合或制訂新法時，易有扞格、矛盾或難以解讀真意的問題，政府的施政理念與政策目標亦不易有效率的推廣及落實。舉例而言，資訊安全包括了一般資訊管理、維護、傳遞機制和敏感性資訊（含一般公務及國家機密）的特別維護與保密問題，除了法制設計（如完整之政府資訊分級分類系統及分級標準）外，尚牽涉到資通訊技術標準、人員安全性（如知悉及利用權限之控管）、機關實體安全（如外部人士入侵加以奪取、儲存空間遭炸藥裝置破壞）之考量。

鑑於安全維護與機密維護具有多重面向，為能確實健全、改善我國國家安全與機密維護法令與制度，長期目標上宜建立跨部會協調機制，統一解釋與進行權責分配，並得辦理監督與觀察其他國家之整體性政策、措施與作法之計畫等工作。舉例而言，國家安全局負有綜理國家安全情報工作並統籌、指導、協調我國所有情報機構之相關情報蒐集、分析等事項，以及依法主管政府機關密碼管制政策以建立安全之資通保密網路；因此相關主管機關，例如：執掌機密維護之法務部廉政署、專責資通安全政策訂定之行政院資通安全會報辦公室等彼此間之橫向合作、交流即有相當之重要性，在資訊完整性的前提下，建立共通事項之管理原則，方有制訂具宏觀性、前瞻性、整合性之國家安全政策（含法規制度及技術標準）的可能。

又現行應立即處理之短期目標，可從整頓現行法制架構著手，蒐集並整合所有政府機關相關之行政規則及行政指導文件，檢討相關之法律、法規命令、解釋性規定及裁量基準，是否已落實明確性原則而無賦予各機關過度的裁量空間，並參考前已提及國外之作法，集中現行各安全維護議題之主管機關的能量，力行跨部會合作，建構我國之安全維護政策框架；以下就本計畫所擇定之議題，提供分析與建議。

一、特定議題建議

（一）公務機關電子機密資訊系統面對內部威脅之作法

1.緣起

約 80%的案件事來自於機關或企業內部人員，或是至少與內部人員有關，然而，機關單位與人員把對於資通訊安全與機密資訊的維護大部分的重心放在防範外來的入侵者（外部威脅），反而忽略了內部員工潛在對於資訊可能產生的危害（惡意的內部威脅）。這些入侵案件大部分擁有合法權限存取控制資訊系統，可合法存取控制系統，而不亦被發現。內部人員利用合法存取權限，為超出於其授權使用之對象、時間、範圍、目的，與用途等之行為，並意圖對於單位組織或是特定人、事、物等造成傷害，或是謀

取不當利益。這就好比擁有大門鑰匙一般，正當合法從大門出入，以及從事本來就可以做的事，而不易被發覺。再加上內部威脅事件通常因為證據不足、損害程度與花費於司法程序之時間、人力與費用無法平衡，或是因為提報對於公務機關的形象與信譽可能產生極大的負面影響，所以通常對於事件大抵只有表面上概略之描述。可能是因為內部威脅事件提報執法單位或是司法機關的比例較低，內部威脅對於公務機關機密維護所造成的危害嚴重程度很難估計。

2.我國現況

我國公務機關對於機密資訊之管理與防護，公務機關處理公務或與公務有關之文書，係辨識機密等級，依循國家機密保護法與文書處理手冊之相關規定按其等級進行保密（按國家機密保護法與文書處理手冊對於機密存取控制（Access）的行為，於在人員、實體與技術控管，以及查核與罰則等在法條內文都有相關規定），再配合身分確認等機制（例如：自然人憑證）。實務面的作法上除使用隔離電腦、密碼行動碟，與加密隨身碟，公務機關使用資訊安全相關技術，輔以保密與加密機制，以增進保密與資訊安全效果。以公務機關使用「自然人憑證」現

行作法為例說明，有關公務機關承辦人員通常使用「電子憑證」的方式進行，利用憑證進行身分識別、權限控管等安全措施，以確保電子文件的可認證性。惟自然人憑證創設之目的和功能，是為了便利人民進行行政庶務之申辦，政府係利用自然人憑證來辨認人民之身分。故公務機關是否能要求公務員使用自然人憑證來進行存取控制機密資訊的管控，於適法性上，不無疑慮。又自然人憑證之使用，僅能「辨識身份」，但並不一定是憑證的所有者載在使用資訊系統，故是否能有效達成防堵「內部威脅」和事後追查的目的效果其合適性應再三斟酌。

3.美國作法

美國針對內部人員對於國家安全與機密外洩的問題，歐巴馬政權立即採取相對應的措施，於 2011 年發布第 13587 號行政命令:「增進機密網路安全與機密資訊有責分享及安全維護的結構性改革（Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information ）」，與因應第 13587 號行政命令所規範之「內部威脅」議題，於 2012 年 11 月 21 日發布「國家內部威脅政策和機關內部威脅方案的最低標準（President

Memorandum-National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs）」的總統備忘錄。部會或機關紛紛對於內部威脅採取相關防範措施，例如國務院對於涉及機密的網路，採用新的審查與監控的工具，而在國防部也開始開發自動偵測內部威脅的辨識系統。在情報系統方面，商務部國家標準與技術中心與司法部聯邦調查局也訂立內部威脅指引，提供企業與機關單位遵循。情報系統委託 Carnegie Mellon University 的電腦緊急應變團隊（Computer Emergency Readiness Team，以下簡稱 CERT）內部威脅中心（CERT Insider Threat Center）進行多項內部威脅的研究。

（1）CERT 內部威脅專案：「公務機關內部非法網路活動（Insider Threat Study: Illicit Cyber Activities in the Government Sector）

A. 內部威脅人員特性：內部威脅人員通常持有管理權限，並利用其權限換取經濟利益，平時會有異常的表現。

B. 內部威脅主要的危害類：通常是資

訊的損壞或遺失。

C. 公務機關確保資訊的能力：政府必須制定相關措施，以保護資訊不被盜竊和濫用。

D. 資訊風險安全管理機制必須加入「內部威脅」之項目：政府機關應積極主動制定相關政策，包括風險管理流程的標準化，並將「內部威脅」的風險應作為評估的項目之一

E. 持續研究：委外、身份竊盜和恐怖活動的防範等面向。

（2）總統第 13587 號行政命令:增進機密網路安全與機密資訊有責分享及安全維護的結構性改革（Structure Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarsing of Classified Information）

A. 加強跨機關資訊有責共享的重要性

B. 確保政策、流程與技術的安全解決方案，與監督和組織文化的發展

C. 強調聯邦政府對於資訊必須實施一致的作法；與

D. 確保隱私、公民權和自由的保護。

E. 第 18537 號行政命令勾勒出美國政府對於增進涉及機密網路與機密資訊網路的結構性改革。不但成立跨機關的內部威脅專責小組負責草擬內部威脅的政策，機關亦必須依照指示時程，落實內部威脅政策的偵測方案，以及監控其運作是否符合政策的目標。

（3）國防部：網路內部威脅計畫方案（The Cyber-Insider Threat Program - CINDER）

利用「巨量資訊（Big Data）」分析多個來源的資訊，並進行分析和識別異常行為的個人。然而，政府是否允許裝置政府出產的控軟體或是商業軟體，則是另外一個問題。通常內部威脅的指標會以銀行存款的大量增加、開車上班方式的改變等，而 CINDER 只是將其行為延伸至網路間。CINDER 並非聚焦於防止威脅入侵，而是嘗試辨識間諜任務的

生命週期的正確性

行為異常檢測的主要優點在於可檢測出以前與未知的威脅，相對的缺點是，由系統偵測內部威脅通常會提供大量的警報，但其中很多是假的。不過，該專案研究人員表示，由系統偵測行為，並不是在尋找犯罪，而是尋找一個證據鏈（Chain of Evidence），並認為是未來安全防護的態樣之一。

（4）商務部國家標準與技術中心（National Institute of Standards and Technology, NIST）的「聯邦資訊系統與組織之安全與隱私控制草案」第四版（SP 800-53 Rev. 4）（Security and Privacy Controls for Federal Information System and Organizations）

該草案係由國防部、情報系統、國家安全系統委員會、國土安全部合作與協作的聯合專責轉型計畫（Joint Task Force Transformation Initiative）的一部分，主要提供於在技術方面，提供選擇和指定聯邦資訊系統和組織對於安全控制的目錄和指引，以及對抗新型資訊安全威脅，與增加新隱私控制項，提供聯邦機

關用以保護期資訊與資訊系統。第四版修訂主要緣起於聯邦政府資訊系統所遭遇之威脅類型，包含對於威脅的能力、意圖和目標，以及對於長時間蒐集攻擊資訊和狀態分析。

NIST 對於「內部威脅方案」提出的建議如下：

A. 內部威脅方案的程序；

B. 跨學科領域（Cross Discipline）的內部威脅事故處理小組（Insider Threat Incident Handing Team）的建置（如人力資源、法律、實體安全、人員安全、資訊技術和資訊系統安全部門等）；

C. 惡意內部活動之偵測，以及監督控管技術和非技術層面資訊的相關性；

D. 專業法律團隊參與，以確保機關之監測活動符合法律、法規、指令，以遵循內部威脅方案政策及相關準則，亦能協助擬定明確的政策並統籌內部威脅方案之執行，以實現內部威脅方案之最大效益；

E. 建議將安全意識、安全評估、特定能力-事故應變，與機關內部協調-事故應變加入管理項下加以落實。

（5）國家內部威脅政策和機關內部威脅方案的最低標準的總統備忘錄（National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs）

主要提供行政部門於防止、偵測與減低內部人員可能造成國家安全的威脅相關遵循方向與指引。因應內部威脅的能力將增進行政部門對於機密資訊的保護，並加強危及國家安全的敵對勢力或內部威脅的防禦，包括潛在的間諜活動，對國家或機關單位的暴力行為，以及未經授權揭露機密資訊，包括透過的美國政府互聯的電腦網路和系統處理的大量機密資料。該標準將提供機關單位建立有效的內部威脅所必要的要素。

備忘錄大約可分為下列各項：

A. 蒐集、整合、集中分析和應變主要威脅相關的資訊；

B. 監控人員對於機密網路的使用；

C. 提供人員對於內部威脅意識的培訓；

D. 保護人員的公民、自由和隱私權。

4.建議

觀察國外先進國家，以美國為例，內部威脅並不是一個新的概念，公務機關本具備一定的管理措施；惟在維基解密案（Wiki Leaks）爆發後，帶給美國政府極大的衝擊，美國也全面檢討與創制新的因應作法，並於政策面、制度面與技術面等不同面向，進行積極的研究與合作。

資通訊技術（Information Communication Technology, ICT）的多元應用與資訊系統的集中化，已逐步影響到機密資訊保護與管理的作法。對於機密資訊的保護與管理，已非傳統實體管制方式可以妥適處理。往昔公務機關對於機密資訊的外部威脅多予以較多的重視，並聚力於相關的管理措施與機制；然而，對於內部威脅（Insider Threat 或 Internal Threat）認知仍嫌不足，或欠缺明確的規範與作法，故實必須從以下幾個面向進行研議。

（1）現行以身分識別與系統權限管控方式無法因應內部威脅

我國對於機密資訊的管控，常聚焦於以涉及國家安全與損害嚴重發生的程度，於涉及機密業務的人員、技術、實體環境上作身分識別與系統權限的管控，然而，身分確認與權限控管的方式，仍然可能發生有權或無權存取控制機密資訊的情事發生，甚至對於機密資訊進行破壞或洩露。由於資通訊科技的導入，對於機密資訊生命週期內，可能將更加劇具有存取控制機密資訊系統之公務機關的公務人員、僱員，以及廠商對於機密資訊與安全威脅的嚴重性。

（2）建置檢視機密資訊管理與保護政策與法制配套措施

美國為因應「內部威脅」一連串的改革，顯見維基解密事件對於美國政府產生非常大的衝擊，更加凸顯了監控內部威脅對於國家與公務機關及其機密維護之重要性。歐巴馬團隊不但全面檢視其機密資訊管理與保護政策與法制、配套標準及措施，並對機密資訊的管理與「內部威脅」的防範進行全面檢討，並

對於相關制度與措施進行增修。我國公務機關同樣也面臨電子機密資訊系統內部威脅之問題，不妨可以美國為借鏡，制定完善的公務機關電子機密資訊系統內部威脅預防偵測及因應之政策機制與配套，以真正落實對於內部威脅的防範。。

（3）以科技技術輔助監督「異常」行為的表徵

我國公務機關對於「機密維護」已有相當認知、具備因應的作法與措施，亦著重資訊安全、身分認證與保密，惟我國公務機關仍面臨諸多政府資通安全威脅之內部問題，就內部威脅異常表徵之主動發現措施，仍有待進一步強化。為真正落實對於內部威脅的防範，透過科技技術進行監督（Monitor）等。機關在制定涉及機密資訊的政策法制、技術標準，與查核事項等事項時，應將「內部威脅」納入考量，就機密資訊存放地點、設備、授權使用之人員、相關系統或其他科技技術等因素設計相應之規範，例如以系統監控或查核人員的「異常」行為（如短期內大流量下載檔案/進入系統的紀錄、大流量轉出有附件的

信件、近日來消費能力顯著高於所得或情緒異常低落或起伏極大等)或預定特定的現象作為潛在威脅的表徵證據。再進一步因應與確認內部威脅的存在。

（4）全國公務機關共同合作落實

最重要的是,該制度與措施要求全國公務機關一起合作落實,以及分享潛在內部威脅的異常警訊,才能真正達成減低公務機關對於內部威脅的防範。在公務機關合作落實的規劃上,第一步驟建議各機關使用統一的公文系統,一來可以統一公務機密的分類標準、二來可以確保機關間保密措施的水準相當,而不會有甲機關慎重防護的公文書傳輸到乙機關後,因乙機關的保密措施不足進而提升外洩的風險。

（二）為維護國家安全並因應資通安全政策之資訊業務採購評選廠商標準-廠商人力來源之背景安全查核為核心

1.緣起

因應資訊科技快速變化及電子化政府的政策推動，各國政府機關囿於預算和專業人力

資源有限，傾向民間資訊服務業者採購資訊服務。在資訊業務委外成為趨勢的同時，宜建置周全的廠商評選標準，提供完善的事先預防措施，進行最初的把關。否則縱使各機關依「資通安全政策白皮書」的方針，建立資訊系統防護體系，但僅仰賴事後管控恐難有效避免資訊安全事故發生，而造成國家安全防護漏洞之危機。舉例而言，2012 年 9 月美國眾議會情報委員會公布調查報告，建議禁止中國兩大電信設備商「華為技術」和「中興通訊」成為美國政府及私人企業的資訊設備承包商，該委員會表示，兩家電信設備商利用承攬建至網路系統標案的機會從中進行間諜活動，竊取美國國家情報和機密資訊並提供給中國政府，威脅美國國家安全。是以，機關採購資訊業務而與機關安全或國家安全有涉時，實宜注重並檢討現行廠商評選機制是否完善。

2.我國現況

依「機關委託資訊服務廠商評選及計費辦法」及「行政院所屬各機關資訊業務委外服務作業參考原則」，政府資訊業務以委外為原則，只有在民間無法提供或民間辦理未能提昇效率的情形下，才由機關自行建置開發。政府機關資訊業務範疇包含三大類：一

般資訊服務（如軟硬體汰換更新或維護、網路管理等）、資訊應用業務（如單一機關需提供或結合數機關進行整合運作之特定系統等）和其他資訊業務（如客服中心、網路安全服務等）。

關於資訊服務廠商資格審查的評選項目，我國主要規定於「機關委託資訊服務廠商評選及計費辦法」、「行政院所屬各機關資訊業務委外服務作業參考原則」及「投標廠商資格與特殊或巨額採購認定標準」。觀前開規定細項，評選標準著重於廠商所具備的設備設施及軟硬體資源、經驗和實績；計畫主持人及團隊技術人員的專業技術水平、資格認證及經驗。若涉及特殊或巨額採購，機關得依個案需求要求廠商檢附、廠商登記或設立證明、納稅證明及財力證明。雖然「投標廠商資格與特殊或巨額採購認定標準」將廠商「信用證明」納入評選項目，惟亦是在強調廠商的「財務信用」。對於得標廠商所使用的執行人員，僅考量其學經歷，而對於背景、信用、品格等並不另行審查。

至實務執行面上，由於法源依據缺乏，機關間尚未建立合作管道以及查核成本所費不貲，又考量到若將品格跟身家背景的查核列為評選項目之一環，易引起是否歧視或有不

合理差別對待的爭議。是以，機關在評選階段並不會（實際上也欠缺資源和管道）對投標廠商的人員名單主動進行核對和過濾，而係等到得標階段，確定得標廠商後，方要求其提供工作人員名單，供以確認工作人員的「專業技術能力」是否符合要求，並要求簽署保證書和保密切結書，以履約管理的手段進行人員安全性管控。不過在極特殊具重大敏感性的採購案個案，如總統大選印製選票的印刷廠商和相關業務廠商之招募，招標機關擇定得標廠商後，會要求廠商提供工作人員名單，包括印前製作人員、印刷技術人員、包裝員及因應封廠需要的清潔工、烹飪廚師等，招標機關會去函調查局請求徹查相關人員的身份文件和刑事紀錄，若曾有前案紀錄者，一律需更換而禁止廠商使用該人員，但在未有法依據的情形下秘密的進行此種查核行為，是否符合法律保留原則及正當法律程序，不無疑問。

3.英國作法

英國聯邦政府於 2012 年修訂了安全維護政策架構（HMG Security Policy Framework），並據架構制訂機關安全責任辦法（Industrial Security – Departmental Responsibilities）、招標時的指導守則（Industry Security Notice

（ISN）2011-4、2010-03）、英國聯邦政府調查政策聲明（Statement of HM Government's Vetting Policy）及數部相關規範。

安全維護政策架構之中心理念為「信任」。英國將機敏性資訊被分為五階，由上而下分別為防護（Protect）、限閱（Restricted）、密件（Confidential）、機密（Secret）及最高機密（Top Secret），統稱為「保護標示資訊（Protectively Marked Information ）」。只要執行業務的人員因業務所需而必須接近、使用或持有（Access To）保護標示資訊/資產，前開人等必須至少通過「背景查核程序」（ Baseline Personnel Security Standard/簡稱 BPSS），包含身份認證、三年內工作經歷、國籍和移民地位。如果該職缺不會經任一階「國家安全查核程序」（National Security Vetting/簡稱 NSV）的查核，則會額外查核前科紀錄（Unspent Records）。另外如果在三年內在國外留滯超過 6 個月以上也必須呈報。機關會使用國家警政系統進行核對（Police National Computer/PNC）。

另按保護標示資訊/資產的機敏性等級，可能需接受 NSV。NSV 由低而高分為三階：1.反恐查核（Counter-Terrorist Check/簡稱 CTC）、2.防禦查核（Security Check/簡稱

SC）、3.進階查核（Developed Vetting/簡稱DV）。透過一定年限的居住證明、工作經歷、安全查核問卷（Security Questionnaire）、刑事紀錄、軍情五處的安全紀錄（Security Service Check）、財務狀況甚至是身心健康的鑑定，用以確認人員的「可信賴性（Reliability）」、「可靠程度（Trustworthiness）」及「廉正誠實（Integrity）」，規範客體包括公務員、短期約聘僱人員、承包商的人力來源，通過 NSV 後，會得到稱為「Security Clearance」的認證。

由於 NSV 需要多機關配合查核的工作，2011 年 10 月成立國防部審查局（Defence Business Service/DBS）專責負責「國家安全查核」（National Security Vetting/NSV），提供除了情報機關以外的各政府機關，整合性的國家安全查核服務，讓機關有效率的篩選出適合的員工及承包商。不過各機關可以自由選擇是否要委託 DBS 或自行進行安全查核程序。

4.建議

我國現行法令所明文的評選廠商標準著重在外在的「設備設施」、「經驗」、「實績」、「財務狀況」及「技術人員的技術及資格認證」，

尚未意識到身家背景查核（如未與恐怖組織有涉或有參與間諜活動之嫌）與「可信賴性」、「忠誠度」及「正直」（如有高度動機或傾向洩漏國家機密）等項目之評鑑機制的重要性；其次，我國並未依資訊系統安全等級或機關資安責任等級，建立具標竿性、指導性的廠商評選標準，僅仰賴招標機關個案操作處理；又機關的把關責任似乎僅需於招標文件中要求廠商提供證明文件，被動的進行書審，然而單純的形式審查，在特定具敏感性的採購案似難以達成政府機關所負的資訊安全維護責任。退步言之，縱使不在評選階段進行審查，機關也並未在確定得標廠商後對工作人員名單進行安全背景查核的法源依據、程序、資源和認知。

採購資訊服務時，機關評選廠商的項目不應僅著重於「廠商」本身擁有的軟硬體設備、技術、實績和計畫團隊人員的專業技術和證照，一味偏重於技術面並無法確實降低資安風險。考量到我國整體法制並未與英國有相似的安全維護架構，對所有能接近、使用、存取機敏性資產的人員都進行規範，以及安全查核之審核程序和項目會有干涉人民基本自由權利和侵入隱私領域的問題，根據憲法第 23 條法律保留原則，必須由法律加以授權方能為之。

據此，現階段建議參考英國的國家安全查核程序，於政府採購法增擬授權條文，賦予機關在具國家安全、機關安全等敏感性招標案時，得對廠商及人力來源的安全性擁有主動查核的權限，警政機關及情報機關於該特定目的下有配合查核之協力義務；針對資訊業務委外的部分，再於「機關委託資訊廠商評選及計費辦法」第 7 條，研增訂「廠商使用人力來源之背景安全查核」的評選項目，並於同條增訂第 2 項，定義人力來源並做列舉，具體的步驟和執行程序，建議同評選項目擬訂於同辦法內。執行面向上可考慮研發資訊分享平台直接讓機關與協力機關間有線上資訊交換管道。

其次，為因應目前實務上執行的可能性及成本考量，或可考慮將人力來源的評選時點，移至得標後再進行查核，惟這樣的作法可能產生的問題是，若該得標廠商自始無法提供安全人員名單，但此時已經不可能進行廠商的替換，而不得不放寬標準。最後，於同辦法研議關於機關應配合資訊系統安全等級分類或對機關所要求的資安責任等級，擬訂廠商人力來源分級背景安全查核機制，並制訂背景安全查核問卷範本作為辦法之附件，由採購機關因應實際需要進行問題的增刪。

（三）論機關公務機密之保護-以因應個人資料保護法之修正為中心

1.緣起

在 2012 年 10 月 1 日個人資料保護法（下稱「個資法」）正式上路後，象徵對民眾的隱私權和人格權保護已經全面性展開。與此同時，我國政府機關在執行公務過程中，會製造大量的紙本或電子化文書，當中包括一般公務機密與國家機密；則機關處理文書的過程--自製作文書開始、評定文書機密等級、內部傳輸、公文交換、歸檔、到對社會大眾依法公開，如何同時落實個人資料保護法和機密維護之相關規範，且不至於疊床架屋、避免不必要的處理與維護成本耗損以及過度限縮人民對政府資訊「知」的權利，其議題值得深究。

2.我國現況

（1）機關文書處理與機密維護現行規範

依國家機密保護法第 4 條及文書處理手冊第 1、50 條之規定，我國機密等級僅區分為三階國家機密與一般公務機密；後者指「機關所持有或保管之資

訊，除國家機密外，依法令或契約有保密義務者」，並被列為「密」等。惟實務上，有些機關為因應業務特性，會各自特定某些文書以「敏感（性）資料」稱呼之，並將國家機密、公務機密及前述所稱的敏感（性）資料以「機敏（性）資料」統稱，並加以訂定維護要點。以「經濟部駐外單位及國際貿易局機敏資料清單」為例，雙邊諮商及國際性會議、洽商協定、訪問行程及人員名錄等，若未被列入密等以上的機密資料，則列為敏感資料。

又國家機密的核定權責、報請核定程序及核定期間依國家機密保護法有明確規定；相較之下，一般公務機密由於各機關性質繁雜的業務種類，本手冊僅概括規定由各機關業務承辦人處理一般文書時進行審核鑑定，若認有保密價值及必要，即應改作機密文書處理。至於「密」等文書之核定標準，實務上的作法是，除來文已核定該公文機密等級為密件或法令有明文規定應予保密之事項時和契約約定之保密規定外，業務承辦人便會將該案相關公文書列為密等；其餘則由各機關業務承辦人就其主管業務權責範圍及內部規則予以裁量

是否保密。

至一般公務機密維護及協調，係由政風機構職掌，機密文書處理原則依「政風機構維護公務機密作業要點」辦理；另本手冊第 76 點規定機關員工對「任何文書」，除特許公開者外，均負有保密義務。就實體上之維護措施，是依「文書及檔案管理電腦化作業規範」辦理。機密文書依文書處理手冊，雖原則上應以人工傳遞，但若因機關業務特性而有需要，可採取相應保密機制後以電子方式傳送，惟實務運作上，機密文書仍一律以紙本處理、儲存及保管為原則。另避免機關人員不當知悉、存取與自身業務無關之公務資料，機關文書及管理系統會具備權限管制及帳密管制之功能，其餘則依行政院及所屬各機關資訊安全管理要點/規範為之。

（2）含有個人資料之文書與機密等級之判斷

新個資法第 18 條規定，公務機關保有個人資料檔案者，應指定專人辦理安全維護事項。另據個人資料法施行細則第 12 條訂有 11 項之安全維護措施。

各機關在宣導新版個資法要求時，多將個人資料之安全維護稱為公務機密之維護，其概念是否正確，不無疑問。首先，依本手冊第 51 及 52 點，一般公務機密之定義為，除國家機密外，依法令或契約有保密義務者；而保密事項之具體範圍應於最小必要範圍內為之，方符行政資訊公開原則，此概念亦為國家機密保護法第 5 條所彰顯。政府機關本即在為人民服務，全國人民的個人資料自係大量流通於機關內或機關間，故而若將個人資料之保護視為公務機密之維護，顯不符合立法者所明示之保密必要性原則，此點亦為法務部法律字第 100002319 號函釋所肯認。

其次，現行實務及相關法令規定對於密件以上之機密文書以紙本作業為原則的情況而言，若因文書含個人資料即要求機關列密處理，對例行業務本就在處理民眾個人資料之機關，如戶政機關及勞工委員會及所屬各機關等，顯係期待不可能，除了成本過鉅外亦將造成行政效率延宕，嚴重影響業務運作並可能使個人資料之本人在行使個資法所賦予的權利時，受有相當程度的阻礙。

承前，文書的敏感性與否、是否具保密價值，個人資料之存有僅為判斷元素而非必要條件；而個人資料之安全維護措施，亦不以列密為必要手段。究其原因在於我國對敏感性資料的層級分類不足以及判定標準並無參考準則，進而無法對應地制訂安全維護政策、作業程序文件及執行之標準流程。

3.英國作法

英國內閣辦公室在 2012 年 4 月發布第 8 版的「安全維護策略架構（Security Policy Framework）」表示，所有政府機關必須將人員、資訊及實體設施等三大政府資產納入考量，方能建立全面性維護國家及全體人民的安全。相關安全維護原則、指引和措施之規劃，必須合乎適當性和比例原則，使政府業務推動具備足夠的全面性同時又能促進營運效率，而當中最重要的面向，即為「資訊安全」。資訊安全目前由獨立機關的資訊專員辦公室（Information Commissioner's Office）執掌資訊保護、促進資訊公開同時衡平隱私保護等政策規劃的相關權責。

英國肯認個人資料屬於敏感性資料（Sensitive Data）中應受特別關注者，但個

人資料並不脫離機敏性資訊分級系統而獨立，仍係依其敏感性程度歸於系統的特定位階，除需遵守該位階一般性資訊安全管理維護機制外，另建置特別規範與作法，強化對人民隱私權及其他權益之保護。

英國將機敏性資訊稱為「保護標示資訊「(Protectively Marked Information）按敏感性高低建立分級系統：絕對機密（Top Secret）、極機密（Secret）、機密（Confidential）、限閱（Restricted）、防護（Protect)。含有機敏性資訊的重要文件必須標示等級在文件的頁首和頁尾，會接觸到相關文件者必須簽署確認並同意遵守公務機密法的切結書。第五階「防護（Protect)」指資料雖具敏感性不宜公開但管控程度與前四者有所區分者，個人資料則被歸類於此階，針對個人資料，英國訂立了資訊保護標準第 6 指令「個人資料保護與資訊安全風險管理」(HMG Information Assurance Standard No 6：Protecting Personal Data and Managing Information Security Risk)，但並未公開此項規範標準。不過仍可參考內閣辦公室發布之「跨機關之最低法定保護措施（Cross Government Actions: Mandatory Minimum Measures)」文件與資訊專員辦公室發布之「資料安全維護違反處理指引（Guidance on

Data Security Breach Management）」，一窺英國機關日常業務運行時，對個人資料的標準作業流程、具體之安全維護措施與資安事故發生時的應變程序。

4.建議

「機密」一詞既已作為所有機密文書/檔案的統稱性用語，則不宜再將「機密」作為最末階國家機密的專門用語。舉例而言，「機密檔案管理辦法」第 2 條：「機密檔案，係指『依法規定而為機密等級之檔案』」，若按文義解讀，可能會誤以為僅規範第三階國家機密檔案，惟規範範圍實際上及於所有的國家機密文書及一般公務機密文書。建議考慮於現行法制上改用其他專有名詞取代第三階國家機密等級「機密」之用語，以避免解讀上之混淆。又為能明確使讀者在文意上便能直覺感受到三階機密的高低次序，或可一併更改第二階國家機密之專有名詞，舉例而言，將第二階國家機密改名為「關鍵機密」、第三階則改名為「極機密」。

其次，各公務機關職掌業務種類繁雜，經手文書態樣不勝枚舉，除個人資料外，為制訂政策而蒐集資料、會議文件或其他敏感性資料，均有保密而不宜公開之需求，而安全維

護措施的嚴謹度應與機關資源的耗損、財政成本的支出及作業效率的降低為成正比之關係。

藉由檢視個人資料保護事宜的契機，機關宜清楚建立「保護敏感性資訊」與「保護機密」兩者乃不同概念。關於公務機密的範圍與敏感性資料的範圍，機關可藉由規劃個人資料管理與安全維護措施之機會，全面清查業務所保管持有之資料，並參考英國的機敏性資料分級系統，對需保護但強度不及至公務機密程度之敏感性資料，另闢低一階的「防護件（Protect）」規範敏感性資料，與一般文書相區隔；在用語上，或可將現行「一般公務機密」改稱「公務機密」，並將「防護件」等級（含）以上之文書/檔案，統稱為「機敏（性）文書/檔案」，規範客體及於敏感性資料之相關法規範亦應統一相關用語。

我國應於國情考量下重新建置機敏性資料分級系統，並訂立明確核定標準、分級處理程序與分級安全維護措施作為配套機制，雖各級機關業務種類不一而足，然仍建議宜由立法機關或資通安全會報辦公室提供如英國機敏資料分級系統之綱要，各機關得根據該綱要由各部門的資深主管組成專責小組，按業務特性商討核定標準及核定流程，

每年至少重新檢視一次核定標準，並開辦教育訓練培養業務承辦人鑑別資料價值的能力；宜規定業務承辦人應以書面記明核定為密件或限制件之理由，並定期檢查核定妥當性、解密條件及保密期限之適當性。

（四）智慧電網安全維護報告

1.緣起

近來，對於關鍵基礎設施之電力系統資訊攻擊事件頻傳，如 2003 年美國俄亥俄州 Davis Besse 核能發電廠微軟公司的資料庫伺服器遭到 Slammer 蠕蟲從該電廠之虛擬私人網路入侵造成該電廠的工業控制系統當機 5 小時；2010 年起，伊朗核設施工業控制系統遭惡意不法組織以 Stuxnet 病毒攻擊，感染約三萬台以上電腦，重創伊朗核子計畫；2011 年 Stuxnet 之變種病毒 Duqu 蠕蟲，該惡意程式專門用於蒐集工業控制系統製造商之資訊與擷取鍵盤敲擊在內之數位情報，以便未來對工業控制系統所控管之關鍵基礎建設發動攻擊。以上不論是無意或故意發動的網路資訊攻擊事件，已經開始危及全球各國關鍵基礎建設的安全，未來各國在關鍵資訊基礎建設所面臨如本文第參大點所述的新型資訊攻擊，將是更趨複雜且難以由單一機構

或機關處理的複合式威脅。

由於攻擊智慧電網之手段與手法多樣，有透過人或系統本身的弱點進行攻擊，或製造特定情況使人或系統誤以為發生事故進而採取行動，間諜病毒趁機進入並潛伏智慧電網的控制系統進行監控，並於適當時機發動攻擊。對於智慧電網的攻擊手法不斷推陳出新，各國於此莫不嚴陣以待。

2.我國現況

國家通訊傳播委員會鑑於電信事業擁有通信網路基礎建設重要資源，資通安全管理機制之導入極為重要，雖然部分規模較大之電信事業已取得 ISO/IEC 27001 驗證證書，然多數業者之實施範圍尚不夠完整。為建構政府及民間完整資安防護網，以保障使用者權益為前提，落實電信事業強化資通安全管理機制之責任，並以規劃管理與驗證稽核雙管齊下之方式，持續強化監督能量，降低電信事業資安風險。國家通訊傳播委員會已著手修正電信法配合增訂相關法規條文，賦予導入資通安全管理機制之法源，以要求電信事業全面落實資通安全管理機制，於電信法修正草案中明定電信事業應建立資通安全管理機制等義務，並要求資通安全管理機制實

施計畫須報核准，並得派員進行定期或不定期查核。

（1）目前國家通訊傳播委員會針對資通安全管理機制導入的作法有：

A. 於 2009 年 7 月 15 日首次公告「電信事業資訊安全管理作業要點」,並提供「電信事業資訊安全管理手冊」為業者內部稽核之依據。

B. 為因應政府於 2010 年公告開放電信事業赴大陸地區投資電信業務之資通安全需求，以保障民眾個人資料、企業營運機密、電信網路設施及金融交易資訊等整體資通訊網路與服務之安全，參考國際標準化組織（ISO）於 2008 年針對電信事業公布之資通安全管理實作指引（ISO/IEC 27011），於 2010 年 6 月 2 日公告修正「電信事業資訊通訊安全管理作業要點」，並隨後公告「電信事業資通安全管理手冊」,作為業者強化資通安全管理機制之參考依據。

（2）我國有關關鍵基礎建設與關鍵資訊基礎建設保護之立法情形

我國對於關鍵基礎建設與關鍵資訊基礎建設保護之政策之立法，目前僅於2011年5月6日立法院第7屆第7會期第12次會議由立法委員趙麗雲等人提出「關鍵基礎建設安全防護條例草案」。

該草案中特於第2條第1項第1款將重要能源、電力及水利設施訂於關鍵基礎建設安全防護範圍，並由經濟部及能源部為中央業務主管機關。

有關統合關鍵基礎建設安全防護之執行，該草案第3條授權由行政院召開關鍵基礎建設安全防護協調會報，並於草案第 4 條由中央業務主管機關建立關鍵基礎建設安全防護通報作業機制，其資料分析、分享與整合等工作則由國家安全局執行。

由上述條文，可以看出關鍵基礎建設保護與關鍵資訊基礎建設的保護之政策作為係屬表裡，兩者工作執行上實有密不可分的關係；惟我國迄今仍未完成相關的法律制訂，執行上仍以政策指引為

中心，欠缺對已民營化之關鍵基礎建設業者要求遵守的強制力。

3.外國作法

（1）日本

日本政府作法是認識到資訊攻擊的危險性，從防護資訊攻擊建立政府內部資訊防護的指揮體系，其第一步是先於政府內部建立防禦資訊攻擊的司令塔，由該機關主掌有關防護資訊攻擊的相關資訊技術研發、人才培育、資訊安全及事故通報機制後，再透過各種實際作為如各個關鍵基礎建設與關鍵資訊基礎建設的資訊安全演練提高其資訊防護的能力，從而達到防護關鍵基礎建設及關鍵資訊基礎建設的實體防護。此一作法可提供我國借鏡，早日建立統合關鍵基礎建設及關鍵資訊基礎建設的資訊安全防護專責部門，以達成平時負責培訓、演練提高資訊安全防護能力，非常時統一事權迅速處理危機事故的目的。

（2）美國

為解決智慧電網的網路安全問題，於

2007 年的「能源獨立和安全法案（Energy Independence and Security Act of 2007, EISA）授權「美國國家標準暨技術研究所和「美國聯邦能源監管委員會（Federal Energy Regulatory Commission, FERC）」,負責智慧電網安全維護的協調,和制訂智慧電網相關的指引與標準。「美國責任辦公室（Government Accountability Office, GAO）」對於智慧電網的安全維護，提出不定期的評估與產出建議事項。

除此之外，「北美電力可靠性公司（North American Electric Reliability Corporation, NERC），與「美國國家標準暨技術研究所」、「美國聯邦能源監管委員會」、「國土安全部和能源部」共同合作制訂電力產業得以遵循的安全維護措施,包括建立強制性和自願性的網路安全標準和指引。

「北美電力可靠性公司」和「美國聯邦能源監管委員會」亦已訂立並批准強制性的網路安全標準和附加的指引,並依據「美國國家標準暨技術研究所」已經確定的智慧電網網路安全標準,支持智能電網的互操作性,發出相關網路安全

指引以資遵循。

A. NIST 第 1108 號特別出版物與 NIST 第 7268 號機關報告。「國土安全部」和「能源部」也大力推動宣導安全實踐指引，並提供其他援助。

B. 「北美電力可靠性公司」訂立八項保護電力與網路資產相關關鍵基礎設施保護的標準，包括關鍵網路資產的識別、安全的控管、人員的培訓、電子的周邊安全、關鍵網路資產的實體安全、系統的安全管理，事故通報與因應和回復。該八項標準與「美國國家標準暨技術研究所」所訂立適用聯邦政府機關所應遵循的指引非常雷同。

4.建議

過去對於使用獨立封閉電力系統的關鍵基礎建設及建置於其上系統的關鍵資訊基礎建設於面對資訊攻擊時，可以以台電公司的單一組織，或透過隔絕獨立的發、供、配電系統的單一方法就可以達成的關鍵基礎建設電力系統的安全防護。

但我國目前對於因應為降低智慧電網所遭

遇資訊攻擊，僅有國家通訊傳播委員會對於網路資訊安全的政策計畫與稽核，或是由行政院科技顧問組（現行政院科技會報辦公室）所提出之「關鍵資訊基礎建設保護政策指引」，均僅及於行政指導的層級，欠缺法源依據及對於要求民營化關鍵基礎建設業者執行的強制力。

（1）訂立專法以強化關鍵基礎建設及關鍵資訊基礎建設之保護

因此為加強電力系統與所使用通訊網路的資訊安全的保護，有必要制訂專法同時對關鍵基礎建設及關鍵資訊基礎建設兩者進行保護，並給予法源基礎。

（2）透過專法授權單一主管機關的法源基礎

由專法中授權單一主管機關針對關鍵基礎建設及關鍵資訊基礎建設的整體資訊安全維護，進行跨部門的資訊溝通、協調並針對不斷發生的資訊攻擊方法進行資訊蒐集、通報及消息發佈。此外，亦可由專法授權單一主管機關對於各關鍵基礎建設的目的事業主管機關落實關鍵資訊基礎建設之資訊安全防

護作為，定期進行資訊安全維護的查核的行政權力並及於已民營化或民營化之關鍵基礎建設業者。並透過單一主管機關建置 ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）針對智慧電網等關鍵基礎建設及關鍵資訊基礎建設發生遭到攻擊或事故時進行危機管理，方能順利對應。

（3）建置資訊安全技術研發機關，針對安全防護作法與查核進行研究

再者，可考量於專法中授權建置作為單一主管機關的資訊安全技術研發機關，專責研發各類資訊安全防護作法，並使所發佈安全防護的作法透過目的事業主管機關的查核能落實於各關鍵基礎建設中關鍵資訊基礎建設上。

如此才能對智慧電網此一跨行政部門的管轄，跨關鍵基礎建設電力與網路資通訊的領域，以及電力工業控制系統與通訊網路的關鍵資訊基礎建設的議題進行管轄及相關作法研議，未雨綢繆避免於智慧電網建置完成後必須回頭檢視整體智慧電網系統中所可能遭遇攻擊的漏洞。

（4）輔以國際標準進行資訊安全管理制度

除以從政府部門統整建立防護智慧電網等包含關鍵基礎建設及關鍵資訊基礎建設的專法及專責單一主管機關;從在台灣建置智慧電網的主角台電公司的角度出發,執行智慧電網的保護的方法,就是於設計智慧電網工程的同時,依國際標準 ISA99/IEC62443 建置資訊安全管理制度,依國際標準進行資訊安全管理制度的政策擬定、程序、執行與要件,並確實落實管理制度的運作,之後再搭配專責單一主管機關的定期、不定期查核,就能提升自身的防護能力,不至於輕易在面臨新型資訊攻擊時造成整個智慧電網的癱瘓。

（五）論我國公務機關解決公務機密核密等級與解密程序爭議之思考–以美國國防部與美國國土安全部公務機密管理機制為例

1.緣起

我國於 2003 年 2 月 6 日頒布與施行「國家機密保護法」,行政院祕書處亦於 2010 年 3 月頒布最新版的「文書處理手冊」,欲藉由國家機密與一般公務機密之分類管理,來防

範我國公務機密無故揭露與曝光，而損害國家利益與人民身家安全。又 2005 年 12 月 28 日亦頒布與施行「政府資訊公開法」，期能建立公務資源與民共享的機制，提升大眾對於公務資訊管理和運用的信賴，並消弭政府資訊不夠透明的批評。

惟「文書處理手冊」雖就公務機密的等級變更與解除方式有所規定，但相較於國家機密保護法的規定，文書處理手冊在機密解除的規定上缺乏較細緻性的設計，造成實際持有一般公務機密之權責人員，對機密核定有質疑時，並無明確的處理機制可供權責人員提出異議。而在一般公務機密核定爭議尚未解決的環節中，也影響了該一般公務機密的解密程序，是否適當之疑慮。

2.我國現況

（1）國家機密之核定與解密

國家機密之核定與解密係依國家機密保護法為之，分依三個等級明確指定核定權責人員、核定時爭議之處理程序與主責機關、保密具體年限及解密條件、依實際狀況依職權或申請註銷國家機密之管道與程序，以及明訂解密的具體

情狀，包括年限屆至、條件成就、條件為成就但已逾保密年限等。又若國家機密於保密期限屆滿前或解除機密之條件成就前，已無保密之必要者，原核定機關或其上級機關有核定權責人員有即為解除機密核定之權責與義務。

（2）一般公務機密之核定與解密

一般公務資訊若有機密核定之必要，係均公務機關內部行政簽核程序以「密等」處理，依文書處理手冊第 56、57 點，核定權責係歸屬於該公務機關之業務主管或其授權指定特定人員處理，核定程序僅有簡要之規定，亦即由前開人員自行審核鑑定是否由保密之必要。

至解密部分，若已標示保密期限或解除機密條件者，期限屆或條件成就時，應依標示辦理變更或解密，且由檔案管理單位會商業務承辦單位依規定辦理之；但若未有標示，則端視原核定機關承辦人員依據檔案管理單位定期清查機密檔案之通知或依其他機關來文建議，將原案卷調出審查，若原核定機關經檢討後認有變更機密等級或無繼續保密必要時，應填具必要表單，陳奉原

核定機關業務主管後，通知前曾受領該機密文件之受文機關依規定辦理機密等級變更或註銷程序。

（3）分析比較

相較於國家機密保護法對於密等核定在其施行細則中已有明確的判定基準，文書處理手冊僅說明公務機關在因法令或契約約定有保密義務者，始需就該資訊核定為密等，但並未如國家機密保護法施行細則中，設計有明確之核定基準或例示，此項不足之處可能會造成密等核定遭濫用之情況。此外，文書處理手冊未賦予原核定機關（或人員）或其上級機關，有主動解除不適當密等文書之程序，僅賦予其消極被動的審查權，欠缺明確之爭議處理機制。

3.美國作法

為在政府資訊公開與國家安全資訊保護兩者間找到平衡點，美國於 2009 年頒布第 13526 號行政命令（Classified National Security Information），規範涉及公務機密（包含國家機密與一般公務機密）之密等核定、機密維護與機密解密或降密等事宜，共分為

六大部分。第一部份包括：機密分級標準、機密核定權限、機密分類、保密期間、機密識別與標示、機密分級禁止與限制、異議以及基本分級指導複查，提供聯邦政府機關制定內部規範的基準。

第二部份係規範使用派生機密分級（Use of Derivative Classification）情形並要求各聯邦政府機關需就派生機密之使用制定指引；第三部分為機密解密與降密機制，包括移轉、自動解密、系統性解密複查、強制性解密複查、請求處理與複查和建立國家資訊解密中心等；第四部分為機密維護措施；第五部份為本行政命令之執行與複審，包括相關機關之職責、分工、合作、相關程序及罰則；第六部份則針對名詞解釋、一般事項、有效日期與發佈等行政事宜提供完整說明。

為了遵循美國行政命令第 13526 號的指示，各聯邦機關均紛紛建置內部的機密管理機制，以美國國防部之公務機密管理機制為例，共分為六大部份：機制建立之參據（References）、國防部掌管國家安全資訊或活動官員之權責（Responsibilities）、美國國防部資訊安全工作概觀（DoD Information Security Program Overview）、機密資訊（Classifying Information）之分級政策/等級

劃分/最初分級與派生分級的規定與流程/保密期限與分級爭議處理、解密與變更（Declassification and Changes in Classification）及安全分級指導（Security Classification Guides）補充性規定。

在第四部份，國防部對於機密分類爭議設有明確之處理原則與程序，提供機密持有人對於現存機密分類狀態提出異議的雙重管道，並確保不會遭致內部報復行為、受異議之機密在決定解密前仍屬於保密狀態而受到保護。爭議程序之設計必須考量該機密係屬機關內部業務或是來自外部，爭議處理流程必須完整記錄並有由外部公正第三方機關或委員會再次複查的機會；自收受案件後承辦人應於 60 日內書面回覆處理情形，若為回覆必須提供預計之回應日期，提出異議者若於提出後 90 日內未收到國防部回應，得將案件轉交 ISCAP 來處理。

至爭議之處理限制，本規範說明若所涉機密在兩年內已經受有適當性之質疑或已在處理程序中，則不可再行提出異議申請，國防部應告知質疑者該機密現爭之情形並提供其合適的上訴程序。

4.建議

美國針對公務機密之爭議設有完整的處理程序，供機關或機密持有者對機密狀態有所質疑時可提出異議，不過該處理機制對於國家機密或一般公務機密狀有一體適用之特性，機制設計上似乎有偏重國家機密，而可能存有處理方式失衡之問題。我國若欲設計一般公務機密爭議處理程序時，應考慮一般公務機密與國家機密有本質與特性之差異，尚須考量現行我國機關處理一般公務機密的實際運作環境，制訂切合需求之爭議處理機制。

相較於美國聯邦政府機關對於公務機密狀態爭議（含國家機密與一般公務機密）訂有完整之處理方式，作為我國一般公務機密處理準則的文書處理手冊，僅要求對於納入檔案管理之機密文書，若有變更機密或解密者，應即按規定辦理變更或解密手續，但對於何人可提出解除機密或機密變更的聲請、提出解除機密或機密變更的方式、一般公務機密原核定機關對於解除機密或機密變更的處理期限、提出一般公務機密狀態是否適當之質疑者的人身或職位安全保障，抑或是對原核定機關解除機密或機密變更之決定有不服者如何提出複查之聲請，均未有

完整的規範。

由於文書處理手冊的規範，現行我國公務機關就一般公務資訊或有可能發生不當核密（或解密）的情況，其緣由可能因核定人員為防止不確定是否為機密之公務資訊有外洩之虞，抑或是因機關內部缺乏合適的諮詢單位，而導致核定人員誤將非機密之公務資訊以機密文書方式處理。因而，如何在一般公務機密核密狀態遭受質疑時，能提供原核定機關或持有一般公務機密者有適當管道或機制來作相應處理，乃是我國公務機關遲早必須面對的議題。

以下提出一般公務機密狀態爭議處理程序之關鍵形塑重點：

（1）一般公務機密狀態爭議的提出方式

文書處理手冊關於機密變更與解密程序的規定並不清楚，而原核定機關承辦人員僅有被動查核的義務，而無權責主動質疑核密之妥當性。

美國則提供了機關承辦人或相關利害關係人雙重的主動異議管道：非正式的口頭提出與正式的書面提出，受理機關有義務於一定期限內回覆之，並以法律

提供提出者相對應的保護。考量我國公務機關運作環境，可先採取書面正式提出之單一模式，讓質疑者以書面完整描述不適宜之情事及理由，使原核定單位或資訊管理單位能充分評估其質疑是否合理，較符我國實務上處理爭議案件時，講求程序正義與實質證據的情狀。

（2）一般公務機密狀態質疑者人身或職務安全之確保

美國提供對公務機密狀態質疑者人身或職務安全的確保，以及防堵其受到報復行為或類似報復之行政措施，例如解雇、停職、降級、騷擾或其他歧視行為等。又如美國國土安全部甚至提供匿名管道（使用代理人）來進行爭議處理程序。

因此我國在設計一般公務機密狀態爭議處理程序時，或可搭配機關內部政風單位或協同機關上級政風單位，提供前開之保護措施或必要之協助程序。另外當質疑者受到工作上之報復行為或類似行政措施時，或能透過外部公正第三人或團體的參與，配合機關內部人事單位進行審議與評估補償或回復之機制。

（3）一般公務機密狀態爭議處理程序

爭議處理機制設計應有明確的處理時程，提高運作透明度與強化核定公正性的效果。我國公務機關針對爭議處理程序，宜對爭議案件處理流程、處理程序追蹤或案件核駁決定有明確之規定並保存詳細的紀錄，確保程序正義；處理各階段之時程規劃，可能需考量不同機關之運作環境、不同案件之複查難度或需跨機關事務合作處理之可能，賦予一定的彈性度。

又為避免一般公務機密因該爭議程序的進行而有機密外洩的疑慮，在爭議處理程序中，仍應確保受爭議標的仍在密等狀態之保護下，進行各項複查程序或書面回覆等工作，防止第三人藉機竊取攸關機關安全的重要公務資訊。

（4）一般公務機密狀態爭議處理的上訴程序

對於原核定單位或資訊安全管理單位就公務機密狀態爭議所為的初審決定（可能為維持原機密等級或機密等級變更未符合預期時），若提出質疑者對

初審決定不滿時，美國允許質疑者可上訴至 ISCAP，由 ISCAP 進行複審。依行政命令第 13526 號之規定，ISCAP 的組成員將由美國國務院、美國國防部、美國司法部、國家檔案館、國家情報總監辦公室和國家安全顧問指派資深全職或永久兼職的聯邦官員來作為該委員會的成員。此外，對於源自於中央情報局的公務機密文件，中央情報局局長也可指派其內部資深全職或永久兼職的聯邦官員來參與該委員會的所有審議或進行協同工作。

因而，為避免初審決定可能有不公正或不適當情狀而有矯正可能，提供第二階段的上訴程序有其必要。我國對上訴程序的設計，除需依個案之不同、公務機密複查難度或需跨機關協力等因素來區分並制定適當的處理期限，對於上訴程序委員會成員之構成，或可考量納入外部機關公正人員或協同機關內部政風單位、法制單位或研考單位一併參與，確保上訴程序審查的公正性與客觀性。

（六）涉密公務人員退離職後之保密

1.緣起

日前發生有卸任（或退休）政府官員以出版回憶錄（即出書）的方式，將其擔任公職期間所知悉或複製留存的機密資訊於出版書籍中予以揭露，衍生其所揭露的公務資訊是否屬於機密文件，以及是否涉及退離職公務人員洩密的責任問題等，頗有爭議。

2.我國現況

對於退離職公務人員檢視有關違反保密義務之法律規範，加上特別考量「公務員」與「曾任公務員之人」身分別的因素，可區分為「一般」、「公務員」，以及「曾任公務員之人」類型，再依責任之法律性質，分為行政責任、刑事責任與民事責任，並分別於國家機密保護法、刑法、公務員服務法、民法有所規範。由上述條文內容文字可觀之，大部分有關保密義務違反的責任，仍聚焦於居於職務任期內之公務員。

再者，法律條文傾向以明文規定保密義務，但卻對於保密義務的違反無積極的處罰。以公務員服務法第 4 條為例，規範退離職公務員之保密義務，但對於保密義務的違反，似

乎並無相對罰則。

另外，對退離職公務人員保密義務法律責任是否違反，除取決於前揭對於保密義務對於「密」的定義與範疇之外，退離職公務人員的「身分」也是另一個需要考慮的議題。

退離職公務人員知悉或持有機密資訊，係源於其之前任職公務，至退離職後才洩露或交付機密資訊，倘將一般（非公務員之）人洩密的罰則，適用於退離職公務人員洩露或交付先前任公務時所知悉或持有的機密資訊的特定情形，亦有疑問。例如刑法第 132 條第 1 項係為「公務員」洩露或交付國防以外機密（一般機密）之規定，既然退離職公務人員已不具備公務員身分，使用此項進行處罰，不無疑義；如果以其第 3 項「非公務員因職務或業務知悉或持有」機密資訊觀之，則產生退離職公務人員知悉或持有機密資訊之「時點」，係身為「公務員」之時，洩密的時點係為「退離職之後」，而產生構成要件未必完全合致的情況。

目前仍在審議的「公務人員基準法草案」，若通過後，將取代公務員服務法。該草案立法目的在於健全人事法制，確認公務人員共同適用之基本規定，並對於公務人員的分類、權利、義務與權益做更進一步的完整性

規範，並改進不合宜之處。草案分為總則、權利與保障、義務與服勤、管理基準與附則。

由法條文字觀之，該草案為因應後續例外情況（例如同條第 2 項及第 3 項之規定），對於守密義務之範圍，將原「政府機關機密」修正為「國家機密及公務機密」，但「其他應保守秘密之公務資訊」，是否包括在守密的機密資訊的範圍內，仍不清楚。

然而，該草案規範主體仍僅針對「公務人員」，對於退離職公務人員守密義務，仍維持原公務員服務法的規定，以「離職後亦同」的文字規範。而且對於退離公務人員保密義務的違反，並無相對的罰則。

3.美國作法

美國規範認定，使用機密資訊的權限為被授與的特權，而不是與生俱來的權利。美國聯邦政府利用與員工之間的雇用關係，透過保密協議（契約關係）的方式，規範該政府員工對於機密資訊的維護，載明雙方的關係、政府員工的保密責任，以及違反保密協議的後果，並強調該保密協議的效力，一直持續至該員工的終身，這意味著，政府員工於不具安全查核的資格之後，或甚至是退離職之後，仍受保密協議的拘束。

凡涉及使用機密資訊之聯邦政府員工、承包商、授權人或受讓人等，於使用機密資訊前，必須完成「保密協議」的簽署，否則不得使用。該「保密協議」在法律上為拘束簽署員工（前述通過安全查核之人員）與美國政府間的契約（Contract），簽署員工承諾，非經授權不得向未經授權之人揭露機密資訊。「保密協議」的主要目的在於「告知（Informed）」簽署員工：因信任該員工而提供其使用機密資訊；簽署員工保護機密資訊不得未經授權揭露的責任；與未能遵循協議條款後果（使用機密範圍以該員工執行職務所必要知悉（Need-To-Know）為限。

除了對於員工本身的權利義務與罰則加以規範之外，美國政府亦特別著重於資訊的快速擴散性與保持機密性的需求，對於未經授權而揭露的機密資訊，利用違反保密協議（違約）（Breach of Contract）為手段，儘量減少機密資訊擴散的程度。例如，美國政府對政府員工提起告訴時，以舉證責任來看，證明違反保密協議民事的舉證責任，比需要證明行為人違反刑法規定的刑事舉證責任為輕。

再者，透過禁制令的方式，凍結並維持資訊的「現有狀態（Status Quo）」，並且還得於提

起民事訴訟的同時，提起刑事。

4.建議

由於英美法系與大陸法系法制體系與規範不同，再加上我國政府與公務人員，以及美國與其政府員工間之關係亦不相同，直接將美國作法複製至我國對於機密資訊的維護，可能會有問題，不過，美國維護機密的作法與概念，仍然有許多值得學習或參考之處。

（1）使用機密的權限以保護機密本身為出發點

政府機關對於涉及機密資訊人員的選擇，均經過層層縝密與嚴謹的查核與審查，才得授與該人員存取控制機密資訊的權限。值得參考的是，美國使用機密的權限與保密責任，是以保護機密資訊本身為中心而為設計。

當該人員業務將涉及機密資訊時，必須先行經過安全查核，通過的人員僅取得存取控制機密的資格，該人員還需完成政府機關加諸的多項安全維護措施後，如保密協議的簽署，才得被授與使用機密資訊的權限，且須遵守相關規

範，與背負相對的責任。

（2）以暫時禁制令「凍結」機密現狀

觀察我國對於保密義務之規範設計，一般多著眼於賦予公務人員或退離職公務人員保護機密資訊之義務，倘要規範一般第三人（並非公務人員或退離職公務人員之人）非法知悉或持有「機密資訊」的情形，則或宜建置其他機制，例如前述美國的暫時禁制令措施，藉之暫停可能侵害「機密資訊」的所有人活動。

我國曾參考美國使用「禁制令」保護機密的作法，於「國家機密保護法草案」於立法院審議過程中提出，不過，後來因該提案可能侵害新聞自由、事先抑制表現自由、禁制令之機制是否適用於我國法制環境等因素考量，而未獲通過。

禁止令之使用在美國往昔雖然不無疑問，例如紐約時報越戰機密案，但考量現今資通訊科技技術之發達，資訊傳播之快速，對於使用暫時禁制令「暫時凍結」機密資訊傳播於目的與手段間之適當性，以及對於被暫時凍結的資訊與表現自由的侵害程度間加以權衡，類似紐約時報越戰機密案之狀況，於今或許可

能會有不同的結果，亦即，禁制令之制度在當前越顯其意義。

（3）機關內部密等認定指引與資訊揭露事前審閱機制

觀察國內最常發生的退離職公務人員洩密案，通常為退離職公務人員不確定其所揭露的資訊內容是否仍屬於機密，以及對於已經落入公眾可得知來源的機密資訊，是否仍屬機密的情形。

於此，為增進公務人員對於機密資訊狀態的了解，以及保密義務是否持續，建議政府機關提供內部密等認定指引，提供公務人員與退離職公務人員對於機密資訊，有可遵循的方向。另外加以強調，機密資訊雖落入公眾可得知來源，若未達解密要件，仍屬機密，未經授權而被揭露的機密，將面對洩密的處罰。並建議退離職公務人員於資訊揭露前或不確定機密狀態時，將該資訊提相對應之政府機關進行事前審閱（Pre-Publication Review）。

（4）調和「退離職公務人員」保密相關規範

如前所述，我國對於機密維護的規範對

象，多聚焦於「公務人員」，明確針對「退離職公務人員」保密事宜的法令規範非常有限;而規範公務人員的保密義務、守密範圍、守密義務的違反與相關罰則，又無以直接適用於退離職公務人員，因此或宜於各該相關法令明文規定「退離職公務人員」機密維護之相關規範。

除此之外，於各法律規範之間，例如，國家機密保護法、公務員服務法（公務人員基準法草案）或公務人員懲戒法，以及民刑法等，針對保密義務、保密的範圍與義務違反的罰則等的法規範目的與具體規定不同，於此，或宜注意法律間之互相調和及競合問題，以免發生法律適用的扞格，以減少爭議，並提供政府機關、公務人員，與退離職公務人員以資遵循之方向。

綜上，於我國若仿美國使用簽署保密協議之保密方式，未必具備類似契約的拘束力，不過，為進行機密安全維護，政府機關或可考慮於公務人員退離職前，以書面告知退離職公務人員應保密的義務、機密的範圍（例如機關內部提供公務人員認定密等的文件）、保密義

務違反時的責任，與資訊揭露事前審閱的要求等，並要求簽署，或許可提供該退離職公務人員以資遵循的參考文件，政府機關也可以此簽署文件作為已告知之證據。

為因應退離職公務人員時有所生的保密問題，以及考量資通訊技術的發達所導致的機密資訊安全維護之變化，找尋可得以保護與維護「機密資訊」（標的本身）之方式，減少機密資訊的傳播擴散或許才是第一要務，再配合上述對於退離職公務人員的法制規範（接觸機密資訊的來源），與其他安全維護機制與作法（配套），多方面共同運作，適得以減低機密外洩的風險。

（七）機關安全維護之研析－以實體設施及人員安全維護為核心

1.緣起

根據「政風機構人員設置管理條例」第 4 條第 8 款，政風機構執掌「機關安全維護處理與協調」事項，再依「政風機構人員設置管理條例施行細則」第 10 條第 2 款，其他應推行之政風事項包括了「危害或破壞本機關

事件之預防事項」，法務部據此訂定了「政風機構預防危害或破壞本機關事件作業要點」（下稱「作業要點」）。除前開規定外，參行政院於 2005 年 6 月 29 日發佈的「安全管理手冊」，機關安全維護的主要內涵，在於建設實體設備、設施及辦公環境的實體安全性，保護並同時管理、監督機關內部人員（包括公務人員、替代役、約聘人員、派遣人員及委外廠商駐點或執行人員）、訪客及洽公民眾，藉由對人員出入和設備設施使用的管控，確保機關實體安全性不會因內部侵入、外圍攻擊或其他天災人禍而有所減損或破壞。

另為求提升政府的效能效率並合理運用預算，對於不涉及機密之一般業務，政府機關委託民間企業之專業能力與設備設施辦理相關業務乃不可逆之趨勢。就現況而言，相較於設置駐衛警察，機關仍偏於使用民間保全業者擔負實體安全維護工作。惟我國對於保全業之管制，法制設計上稍嫌不足。舉例而言，對於保全人員之資格，除了消極限制要件外，我國並無類似國家考試的統一考核機制，其背景考核及專業訓練均委由保全業者自行辦理，導致保全人員素質良莠不齊；其次，依我國現行薪資結構，保全人員工時長但時薪低使保全人員流動性偏高；再者，

派遣性質之工作本就難以期待有高度的向心力和責任感，且機關與保全人員間並無直接的僱傭關係，而不易進行有效之管理監督，因此流弊滋生。危安事件肇因中，有不少數是來自於保全人員的的能力低落或是監守自盜。

參國外立法政策，縱各國如英國、美國和澳洲政府亦同處於去任務化、去委外化之潮流中，然並不因此即將機關安全維護之職責全權轉嫁給民間保全業者，在法制設計上，對於如何維護機關安全訂有嚴謹的政策、程序、細節性的機制措施及文件範本，對於機關應遵守的強制性義務，再藉由委外之法律規範、招標文件及契約設計，來規範民間保全業者，同時對於保全從業人員之工作，設有證照制度、評鑑制度和強制的教育訓練等。我國若欲調整並改善現行機關安全維護的法制結構與實體安全維護工作之執行狀況切入，實可參酌澳洲之立法政策及框架。

2.我國機關實體安全現行法制與實務運作情形

參據行政院「安全管理手冊」第 2 條，機關所可能遭遇的安全威脅類型包括「危害、破壞、空襲、火災、竊盜、風災、地震及水災」等天災人禍，指述之安全面向為實體設施設

備之安全性與位於該設施內人員的人身安全。亦即包括：

（1）因內部威脅產生之資料或資產之洩漏滅失

如辦公場所未劃分不同等級的管制區域、責任區域或訂定人員管理之相關機制，使無權限之內部人員、委外廠商、採訪媒體或來訪者得輕易進行側錄、側拍、安置資料竊取裝置以及取走紙本文件或電子儲存媒體。

（2）機關外部威脅入侵招致人員傷亡、資訊洩漏或滅失及實體資產的損害

部分公務機關，例如：公路監理機關、勞工保險局或戶政機關等，因業務性質需要對外開放服務民眾，人員出入頻繁，執行個別安全查核的門禁管制措施實屬不易；又現行實務上，許多公務機關（或單位）的辦公場所並非位處於獨棟大樓，而是位於商辦大廈中與其他民間企業共構之合署辦公型態，對於門禁管控、巡邏的嚴謹度和其他保全措施的規劃，僅有參與權而無絕對主控權。若公務機關本身並無設立雙重門禁管制

或出入人員的控制，當有外部人士欲對機關內部人員進行人身侵害或破壞機關設施時，將極易得手而無法及時阻止或將傷害減至最低。

（3）實際設備、設施或場所因意外或疏失遭受破壞

現行許多機關係與民間企業混雜在商辦大樓中，例如行政院災害防救委員會所在地是在大坪林捷運大樓內、行政院金融監督管理委員會則是位於板橋火車站建物內，均與許多商家如餐飲業等共構，除出入人口複雜外，也易於發生火災或斷電等其他意外事故。以前陣子「是方電訊火災」為例，事故起因是外租給「數位通國際」存放 UPS 不斷電系統和電池設備的機房出現悶燒情形，雖然火災並未蔓延到起火點以外的樓層，但為安全起見，消防局要求台電停止供應整棟大樓的電力，導致台灣 9 成對外海纜斷訊、18 家網路供應商無法提供連線服務、上千家企業線上付款機制停擺，也因為整棟大樓的電力完全切斷，使備援機制亦無法派上用場。因此，縱非惡意人為破壞，光是單一意外事故，若未對機關實體設備設施有緊急

應變和備援的處理機制，則有可能導致機關業務完全中斷而癱瘓。

機關安全維護之業務包括預防危害、破壞及其他處理與協調事項，係由各機關政風機構所執掌，就其具體內涵及實際作法，主要係依「政風機構預防危害或破壞本機關事業作業要點」及行政院所發佈之「安全管理手冊」為依循。其他可參據規範尚包括：各級警察機關安全防護工作實施要點、屏東縣政府消防局機關安全維護作業要點、行政院國家科學委員會維護機關安全工作作業要點和臺中市稅捐稽徵處加強機關安全維護值日員工應確實遵守事項。

為節省國家人事及公共建設的財政支出、提供更良好的服務品質、活化機關人力及效率並有效利用民間豐沛的資源及專業能力，機關對於不涉及公權力行使之內部事務或服務之業務，傾向委託或外包民間辦理，以簡化政府業務，而機關安全維護委外給民間保全業者為現行趨勢。然而，根據 2007 年法務部調查局的調查報告顯示，機關所發生的危安案件當中，保全人員故意犯案的比例竟超過一半、若包括因保全過失導致的危安案件，比例上高達八成。

可能之肇因為：

（1）保全人員工時長待遇差而缺乏向心力與認同感；

（2）流動率高但市場需求量大，造成保全業難以篩選和給予適當之訓練，因此人員素質良莠不齊；

（3）機關對於保全人員未建立完善管控機制以及對派遣人員有實際約束上之困難；

（4）警察機關與轄內保全業者協調聯繫機制之欠缺，根據中正大學犯罪研究中心的研究報告指出，保全人員與警方聯繫頻繁程度只達 3 成，不及於社區守望相助隊的 7 成，使警方無法立即處理保全人員所駐機關之危安事故。

針對機關實體安全維護，我國規範方針及方向上並無太大疏漏，然而實際執行面向及科技技術應用面向上，蓋保全業實務運作之弊端非一日之寒，包括保全人員因待遇及前景有限，難以吸引優質人才但又缺工嚴重，導致保全從業人員素質良莠不齊且流動率極高；政府亦無統一的職前培訓計畫與專業訓練輔導機制，僅由保全公司自行決定訓練內容，以致保全從業人員在專業能力上恐存有

隱憂；另主管機關的定期查核亦因人力不足而流於形式。

保全業法修正草案曾 2009 年提出並囊括各世界主要國家之作法，惟立法者至今尚無下文，過往點出的各項弊端自延續至今。當務之急應係由機關本身有所警醒，對於實體安全維護的具體作法應建置更明確、細節的規範，妥善管理監督委外之保全業者。

3.澳洲作法

澳洲防護性安全政策架構（Protective Security Policy Framework/簡稱 PSPF）由澳洲司法部（Attorney-General's Department）發布。其架構設計成四個層次：

（1）第一層：政府業務安全性指令（Directive on the Security of Government Business）

屬於安全政策架構的基石，闡明澳洲政府對機關本身及委外廠商有哪些安全性要求。

（2）第二層：管制安排/核心政策/法定強制要求（Governance Arrangements/Core Policies/Mandatory Requirements）

核心政策分為三大面向：人員安全、資訊安全及實體安全。

（3）第三層：議定書、標準與指引（Protocol/Standard & Guidelines）

為遵循第二層的核心政策及法定強制要求，訂定實施指引、安全保護措施和風險管理文件的範本，包含應用標準，提供各機關一致性的作法，使跨部門業務之執行和資訊共享更加順暢。

（4）第四層：機關特定防護安全政策與程序（Agency-Specific Protective Security Policies & Procedures）

機關應自行發展出合乎自身特性和業務需求的專屬政策和程序，同時補充和支持其他機關營運和操作程序。

在「實體安全管理核心政策」下設有 7 條強制性要求，包括機關應建立具體可執行之計畫與必要項目內容；對於機關人員及其家屬的保護、事故通報、人員訓練及諮商、事故發生及因應的即時紀錄、報告等，機關應建立適當的機制；在規劃、選擇、設計和修正設施或設備的過程中，機關應確保實體安全維護的考量已納入相關計畫；機關在規劃實

體安全維護措施和行動時，應同時遵循保護機關員工職場健康及安全的法定義務；機關對於與自己有直接互動之第三方（如洽公民眾）負有實體安全維護的注意義務，保障第三方之人身安全；機關對於資通訊設備（ICT System）及資訊應實施一定水準的實體安全防護措施，最大限度的降低風險，確保資通訊設備能正常運作、控管存取、利用、刪除資訊的權限；機關應持續改善計畫和程序提升安全等級，整合緊急應變計畫，以因應緊急事故及新興的威脅。

於第三層次下，澳洲訂有「實體安全管理指引：管制區及風險減輕控制（Security Zones and Risk Mitigation Control Measures）」文件，敘明機關場所實體安全維護相關機制與作法，以及機關於委外服務時，機關如何管理委外的風險及委外契約訂定的相關規範及保全業的管理規定，藉此勾勒出澳洲政府機關是如何「安全」地將「實體安全維護」的任務交付與委外廠商的圖像。

規範內容可分成四大項：

（1）降低風險與確保措施（Risk Mitigation and Assurance Measure）

包括風險評估之具體操作標準、訂立場

所安全計畫、關鍵路徑規劃（辦公場所的安全動線，延遲入侵者進入核心區域的時間）以及透過環境設計預防犯罪（Crime Prevention Through Environmental Design/CPTED）等。

（2）管制區之方法論及要求（The Security Zones Methodology and Requirements）

管制區（Security Zone）共分五個等級，亦即機關應依風險評估的結果，對辦公場所進行區域劃分，文件並指定了相應的管控措施。劃分不同層級的管制區可以延遲外人侵入的時間，有利於機關對侵入事件有餘裕進行適當的防禦回應。

（3）個別控制要素（Detail of Individual Control Measures）。

為讓提供機關判斷、選擇控制措施的準則，機關可以根據風險評估的結果選擇額外的控制措施，控制要素包括：使用澳洲安全建設及設備委員會認可的產品、建築物結構、警報系統、門禁管制系統、整合警報系統與建築管理系統、訪客管控、安全人員、安全設備、CCTV

系統、安全照明、周遭環境的安全管控、安全儲藏設備、庫房及其他控制措施等。文件根據各項控制要素提供說明、判斷要素、國家已訂立之標準或官方認可產品清單等。

（4）行政管理上的實體安全要素（Physical Security Elements in Administrative Security）。

在行政管理的安全程序上，機關得使用一些實體設備設施，包括但不限於：人員在運送小量的實體資產或資訊出辦公場所以外或將複本要傳遞到其他機關時，應該使用保險箱、單獨封存的封套或集裝箱、其他密封信套、以及銷毀機密資訊時使用碎紙機、粉磨機等。

另外，防護性安全政策架構強調，由於委外服務的執行人員能夠進入機關內部辦公場所、接近機關資訊資產，故機關有責任建立一定人員安全控管程序（Necessary Personnel Security Procedures），管理委外服務的安全性風險。為協助機關將業務委外時，建立完善的委外政策和擬定契約並遵守，防護性安全政策架構架構之規定，澳洲政府發布了「防護性安全管理指引：委外服務與職能安

全性」的文件，提供持續性、結構性的方法幫助機關決定：委外廠商經營場所應有的安全維護措施、委外廠商使用人員的安全查核程序及契約中安全管理措施的約定。

末者，澳洲保全業的規範依行政區有不同的證照制度和規定，以澳洲首都區（ACT）為例，主要依據為 2003 年保全業法、2011 年保全業修正法及 2003 保全業規則。證照共分五種：保全公司證照、保全人員證照、保全教官證照、見習保全證照及臨時保全證照，保全人員依保全職務內容的不同，分成 12 種證照，又如果在販買酒精的工作場所擔任保全工作需另外取得酒精責任服務證照，又保全人員是可以使用槍枝的，但也必須取得許可。

保全人員資格之取得，除消極資格限制之外，2003 年保全業法按不同類證照設計不同種類課程之外，亦要求申請者通過澳洲聯邦警察機關或各行政區的「國家警察查核（National Police Check）」，另外，從 2012 年 9 月 27 日起新的申請者或申請換發者必須要提供指紋。又針對不同保全職務，法規上會有個別的要求，例如「群眾管制員（Crowd Controller）」之性質常需使用物理強制力應付暴力衝突，故保全業者（雇主）

必須確保「群眾管制員」工作時必配掛識別碼、留存並隨時更新其聯絡方式和撰寫工作日誌（日常任務中有發生衝突事件或強制驅離入侵者時）等。主管機關法制服務辦公室（Office of Regulatory Service）為確保保全業的運作符合法令規定，其法遵政策包括教育訓練、監督與查核、自我規範、資訊分享及強制執行。在查核部分包括定期查核及工時外的抽查，前者著重於解決申訴或抱怨案，給予證照的暫時中止或撤銷懲處；後者較具前瞻性且著重於高風險事件，例如非法經營的保全公司、不適當行為及保全業非法雇用未成年人員等。

4.建議

藉由對澳洲防護性安全政策及實體安全管理機制之研析，可發現澳洲政府機關對於場所、設備設施及出入之內外部人員的控管，有嚴謹縝密的管理機制與具體作法；相較於此，我國政府機關安全維護之相關法制框架尚有強化空間。簡言之，機關應仰賴自身，對於實體安全維護的具體作法建置明確性、細節性的規範，強化自身之警醒程度，不宜過度仰賴委外安全維護廠商的安全管制建議。舉例而言：

（1）我國機關目前僅有「責任區」的概念，可考慮引進澳洲「分級管制區」以及「關鍵路徑規劃」之概念，重劃辦公室的區塊及動線；

（2）和民間企業共構合署之機關或有大量洽公民眾出入之機關，宜藉由門禁管制、巡邏安排、專人全程陪同訪客與機房重地限兩人以上停留等安全措施強化實體安全性，可建置標準作業流程；

（3）參澳洲對監控、入侵偵測及通報聯防等電子警報系統的管理，三級以上管制區部分應由機關內部、受過訓練的專人直接管控。目前我國榮總醫院亦採類似作法，由駐衛警負責醫院院內監視系統的監看，僅停車場及大門口的監視系統由委外保全公司及駐衛警併同監看，惟夜間及假日僅由保全人員為之。

再者，機關實體安全維護任務，是否適合全權委外保全業者，尤以本身屬高重要性的機敏機關而言，值得再斟酌，在現今保全人員素質頗受爭議與警政機關因業務繁重而無法有效輔導管理保全業的困境下，以及鑑於日後駐警人力將悉數消失，機關或可考慮有無可能編列預算、於組織內編制專職維安人

員。蓋專職維安人員因具備工作穩定性、歸屬感及位於行政體系內，較易培養責任感、榮譽心及向心力，除能運用其所學確實的指導、管理和監督值勤委外保全人員，尚能避免後者直接接觸機敏性高的資產和區域，阻絕因利洩密的風險。

次查，委託民間保全維護機關安全之議題，無論是從保全業運作的面向抑或是自政府機關實際委外的情形進行分析和檢討，政府及學者專家實已從民國 90 年代中期即投入大量關注，根本問題為我國保全業相關法制有待完善，相關問題已如前述討論，是以，機關如有委外安全維護之需求，應考量己身需求與特殊情形而為採購專業服務之考量，自行客製化契約條款，而非僅以範本契約之援用即認符合安全性之要求。

另建議契約約款宜納入機關內部訂定之實體安全維護機制，不宜僅概括約定廠商必須遵守法律規範和機關內部相關規定，而係將具體安全維護機制內化至與保全業者的保全服務契約內，細緻化地定明權利義務關係、落實監督管理保全人員之辦法、監控畫面資料儲存、備份和刪除方式及保密義務範圍（如機關監視系統配置、巡邏時間）等。

參據澳洲之作法，考量機關日後對於安全性

要求之修正與變更可能，委外契約與安全性要求的細部文件宜分開訂立。在現行保全業法制規範不足之下，負責機關安全維護之主管機關，可定期檢討前述範本契約之不足，酌以適當之行政指示要求各單位建立自身安全維護之委外評估，藉由評估結果來完備委外契約或相關規範。

就保全人員管控部分，應秉持預防勝於治療之概念，除確定保全業者提供之人員名單均擁有良民證外，機關可審酌是否自行做額外的安全查核，例如負責監控機關內部監視系統或夜間巡邏辦公場所內部之人員，對機關生態、人員活動及弱點會相當清楚，故不宜由具「潛在洩密誘因」的人員擔任。另若欲提升保全人員的素質與向心力，機關應與委外之保全業者協力，以薪資、合理工時和福利降低流動率，進一步才有長期培訓專業能力之可能；最後，當保全人員離職時，應確保其門禁或資訊存取權限完全終止，並對內部公告其不再任職之消息。

二、未來研究方向建議

（一）關鍵基礎設施之資訊安全情報分享

隨著資通訊科技的進步，資通訊系統具網

網相連的特性，一旦有組織發生資安事件，除了因且其具傳播迅速之特性、極易危及與之相連的系統而可能造成作業中斷或癱瘓外，若資訊系統或資料庫亦遭侵入，網路犯罪也開始成為新興犯罪類型的主力，小則造成資料外洩的損害，大則可能造成國家安全的隱憂；因此，各國均期能建立開放、安全、可信任及健全的網路空間，為達此目的，國內外紛紛規劃預計透過法規制度，或規定發生特定資安事件類型時進行通報或分享，希望藉此降低所造成之損失。

1.我國現況

我國對於資訊安全的議題實際上並沒有特別去區分「通報」與「分享」的概念，現行的作法上，係採取混合強制性與自願性的要素，進行通報機制的設計，在通報機制中包括了必須通報跟鼓勵自願分享的理念。此現象可能源自於我國對於資通訊安全並未立有專法，除了特定法律如個人資料保護法要求有個人資料外洩事故時必須通報外，對於資安事件之通報，主要係以行政院國家資通安全會報訂定的「國家資通安全通報應變作業綱要」，依行政一體原則之拘束力規範行政院及所屬機關；但針對民間業者並無統一的通報法源，目前僅有高密度管制行業，依

主管機關的監督權限賦予相關通報義務。

再者，無論是公、私機關，資安事故屬於不可外揚的家醜，關鍵要素在於：對組織的信譽及民眾對組織安全性的信任感嚴重破壞、處罰潛規則與伴隨而來的職場壓力以及政府並未提供相對應的通報誘因或獎勵，可能的原因包括：通報結果於組織的信譽及民眾信任度的破壞過鉅、通報後伴隨而來的處罰潛規則與壓力、政府並未提供相對應的通報誘因或獎勵。

2.美國作法

一直以來，美國聯邦政府試圖對於聯邦政府與關鍵基礎設施之資訊安全系統所持續面臨的風險發展並實施策略以解決政府資訊系統的網路安全缺失、發展並實施泛機關間的網路安全計畫，並展示可衡量的進程以促進聯邦系統的網路安全。

美國企圖提出資訊安全相關法律以維護網路空間的資訊安全，但該保護國家電腦網路以及公共基礎建設預防數位攻擊法草案後來卻被參議院否決，歐巴馬總統決定將相關事務透過行政的力量執行，卻飽受以行政權凌駕於國會立法權之爭議，以及以總統行政命令的方式規範業界以自願遵循標準與最

佳實務之作法，其效力有限並在後續政策推動上可能遭遇困難。

2012 年 7 月美國兩黨政策中心（Bipartisan Policy Center）提出「網路安全專案-公私部門資訊分享（Cyber Security Task Force-Public-Private Information Sharing）」報告，提出，希望透過法制設計，在保護美國公民隱私和自由及提供可信賴情報保護規範的前提下，放寬公部門彼此間、公私部門間關於網路威脅相關情報分享的程序限制（特別是擴大關鍵基礎建設所有者和營運者分享機密情報的管道）的建議，方能有效建立網路安全機制和應變措施，現階段則可先採取與個別私營機構簽訂合約，給予一定保護機制讓私部門同意分享資訊給政府。

爾後，歐巴馬總統於 2013 年 2 月 19 日發布 13636 號行政命令:「促進關鍵基礎建設的網路安全（Improving Critical Infrastructure Cyber Security）」，目標是強化資訊分享機制並發展標準，以強化網路防禦能力，保護國家安全、工作和隱私權。其中一項作法便係指示各聯邦機關放鬆關於網路威脅的資訊分享之管道，建立一自願性、合作性的資訊分享程序讓聯邦政府能提供機密網路威脅及技術資訊給關鍵基礎建設業者，或提供安

全服務給前者的供應商，期藉由增加資訊分享與業界夥伴合作發展及執行網路安全架構之方式，強化關鍵基礎設施之網路安全。

（1）透過國防產業基礎資訊分享計畫（Defense Industrial Base Information Sharing Program）開放予其他部門參與

此行政命令擴張了自願性強化網路安全服務計畫（Enhanced Cybersecurity Services Program），允許幾近於即時的網路威脅資訊分享，以協助參與的關鍵基礎設施公司保護其網路。

（2）NIST 主導網路安全架構（Cybersecurity Framework）之發展

NIST 將參考現有的國際標準、實務與程序，與關鍵基礎設施利害關係人共同發展網路安全架構。

政府透過與產業合作保護國家最重要的關鍵資產免於受到網路攻擊，結合有關關鍵基礎設施設安全性及恢復力之總統政策指令同時發布，並透過以下的方式強化美國政府與其他關鍵基礎設施所有者與營運者的夥伴關係，以對抗網路威脅：

（1）提供機密與非機密性威脅與攻擊資訊予美國公司之新資訊分享計畫

此一行政命令要求聯邦機關撰寫與美國公司有關之威脅的非機密性報告且即時分享此報告。此一行政命令也擴張了自願性強化網路安全服務計畫，允許幾近於即時的網路威脅資訊分享，以協助參與的關鍵基礎設施公司保護其網路。

（2）網路安全架構發展

此一行政命令要求國家標準與科技機構（National Institute of Standards and Technology，NIST）主導網路安全架構之發展以降低關鍵基礎設施所面臨的網路風險。NIST 將參考現有的國際標準、實務與程序，與產業合作，共同發展此一架構。為了促進技術創新，此網路安全架構將提出技術中立且同時能夠增進關鍵基礎設施部門發展產品與服務之指引（Guidance）促使其可由競爭市場中獲利。

（3）此外，該行政命令亦基於資訊自由實務原則（Fair Information Practice

Principles)納入強大的隱私與公民自由保護

根據此一行政命令，機關必須將隱私與公民自由保護措施納入其活動當中。這些保護措施將會依據資訊自由實務原則與其他隱私和公民自由政策、原則和架構。機關將會針對其活動進行例行性的隱私與公民自由衝擊評估且評估結果將公開。

（4）建立自願性計畫以推廣網路安全架構之採用

國土安全部（Department of Homeland Security）將與能源部（Department of Energy）等產業特定部門（Sector-Specific Agencies)和代表產業的部門合作協調會（Sector Coordinating Councils）共同合作，以發展能夠協助公司執行網路安全架構及獎勵採用該架構。

（5）召集檢視現行的網路安全規範

法令主管機關將依據網路安全架構評估其所管的網路安全法令，以確認現有

> 的規定是否足夠，以及是否有任何現有的法規在已沒有任何效能的情況下需要被廢止。如果現有的法令沒有效率或不足夠，機關將依據網路安全架構且在諮詢其所轄產業之意見後，提出新的且具有成本效率的法令。並鼓勵獨立的法令主管機於其職權範圍內，權衡網路架構之要求，考量應採取之優先事項以減輕關鍵基礎設施所面臨的網路風險。

持續性的網路威脅確實逼迫美國政府對於資訊安全採取立即的行動，然而，以總統行政命令所頒佈的事項無法如同法案完整，以及行政權罔顧國會立法權之作法，使歐巴馬政府飽受批評。

與資訊安全之相關議題，每年都提出草案於國會討論，但是，後來均因為國會無法通過而告失敗。2013 年 4 月 18 日眾議院通過網路情報分享與保護草案（Cyber Intelligence Sharing and Protection Act），藉由立法提供保護並建立公私部門之間網路威脅情資分享的機制，以強化國家的網路安全。

該法案的主要內容為：

（1）情境共享認知之概念釐清

確立「情境共享認知」（Shared Situational Awareness）的概念，讓指定的網路運算中心間（Designated Cyber Operations Centers）建立一個能及時分享網路威脅相關情資的環境，使網路運算中心能針對已知的網路威脅提供有效的應變措施。

（2）情資分享程序之建立

要求各政府機關對於情資分享建立程序，並由國土安全部、檢察總長、國家情報部部長和國防部共同協商訂定，項目包括私營機構或個人在何種條件、資格限制下，得與政府機關分享威脅網路安全的機密情報；允許私營機構在徵得客戶同意的情況下跟政府和其他私營機構分享有關資訊；程序設計上，對於能防禦或減緩網路威脅之必要性情資，要避免其流動的延遲和阻礙，若相關情報能識別出特定個人，必須保護其身份不被揭露。上開機關亦需建立監督系統和機制，確保所有聯邦政府機關確實踐行法遵義務。至於政府情報機構如何將網路威脅情報分享給私部門（Private-Sector Entities）和公用事業（Utilities），由國家情報部部長負責建

置建立相關程序。

（3）強調資訊分享和流動注重及時性，並應以去識別化和必要性為原則，落實對隱私和公民自由（Civil Liberties）的保障，同時確保私營機構的營業秘密和其他敏感性資訊不會因通報而洩露或使信譽受損等，才能提高通報的意願和通報內容的完整性，因此相關程序的設計必須留意資訊接受者的資格審核、索取資訊目的、資訊利用範圍（如僅允許政府在達成建構更完善的網路安全法制及網路系統、調查電腦犯罪、保護個人免於生命、身體和其他重大損害等目的下利用資訊）、情資去識別化及監督不當利用（如資服業者利用情報為打擊競爭對手）的機制，並由國土安全部負責向國會提出年度報告，關於情資分享對隱私和市民自由的衝擊評估和有何改善及修正建議。

2013 年以涉及國家安全為由要求或鼓勵私部門對於資訊安全的網路情報進行分享與保護為新的方式，不過，網路情報分享與保護草案截至結案報告之繳交時點，仍未有更進一步的進展。

3.建議

（1）從通報（Reporting）轉為分享（Sharing）的概念

有鑑於強制性的通報機制不一定會有良好的成效（得不到足夠的通報案件數量），各國開始從「通報」轉向為「分享」的概念，期望能形成公、私部門良好資訊共享、互相交流的環境，瞭解產業真正的需求、訂定實用的安全性標準。

（2）公私部門夥伴關係（Public-Private Partnerships/PPP）的重要性

近年，各國如美國、英國、澳洲、日本、歐盟及其會員國均就資訊與網路安全進行檢討分析，並不約而同地提倡建立公私部門夥伴關係（Public-Private Partnerships/PPP）的重要性，透過建立公私部門之間資訊共享機制，發展永久性資訊共享環境，強調係以自願性的形式，提供誘因和動機，使民間組織願意與政府合作，交流網路威脅情報、資安預警、因應與修補手段、弱點分析或其他相關研究等資訊，而不僅限於已發生

的資安事件。

（3）以涉及國家安全的關鍵基礎設施(私部門)作為資訊安全情報分享的首要示範

參考美國經驗，對於如果以廣泛的資訊安全作為法律規範對象，可能受到政府強迫企業遵循政府所訂立之新資訊安全標準、妨礙企業對於資訊安全防護的商業模式，以及政府涉入規範企業業務執行的批評。再者，雖然情報分享的出發點可能是出於資訊安全的考量，但基於企業對於資訊安全事件發生的立場，對於事件發生的確認，以及資訊安全情報的分享對其業務與商譽可能造成衝擊，以致於企業自願遵循與參與情報分享的意願不高。

最後，美國政府選擇以國家安全為由涉入關鍵基礎設施之資訊安全，作為情報分享的規範對象。因關鍵基礎設施正面臨多樣化的風險和不斷變化的環境，關鍵基礎設施之資訊安全可能對於國家安全帶來重大的威脅，對此公私部門需要共同合作因應，設計參與意願高的自願性資訊共享機制，方能建構一完整情境共享認知的環境，而能蒐集到足夠的

實際攻擊案例，進一步做有效的對策模擬、預測可能的威脅，規劃具前瞻性、長遠性的決策機制，以減輕風險和威脅，並進行演習，以確保部門及其合作夥伴可以於事件發生時快速因應與恢復。

（二）增進公務機密維護之建議

1.我國關於文書核密與處理之現況

我國目前關於文書及檔案之分類，主要是依文書處理手冊（法位階：行政規則）及國家機密保護法及其施行細則為之。按前開規定，我國之機密文書共分為三階國家機密與一階「一般公務機密」，其等級由高而低分別核定為：絕對機密、極機密、機密與密，密等以下則泛屬於一般文書。在國家機密部份，關於核定標準、保密條件與期限、變更密等或其他爭議處理，設有相較於一般公務機密更加清楚之規範；惟一般公務機密之核定標準，文書處理手冊僅概括規定由各機關業務承辦人處理一般文書時進行審核鑑定，若認有保密價值及必要，例如來文已核定該公文機密等級為密件或法令有明文規定應予保密之事項時（例如政府採購法第 34 條規定之保密項目）和契約約定之保密規定

外，即應列為「密等」處理（參見文書處理手冊第 51 點）。

2.實務運作與現行法制之落差

（1）核密標準欠缺操作明確性

由於各機關業務種類繁雜多元，各業務承辦人亦有流動、轉調等情事，甚至可能有非公務人員而係短期聘僱人員進行單項業務之承辦，就現行密等文書的核定標準，實有過度概括而欠缺核定標準明確性之問題；再者，文書處理手冊第 76 點規定，機關員工對「任何文書」，除特許公開者外，均負有「保密義務」，則究竟何種條件下的「保密」等同需將文書列為密等、何種條件下不需列為密等而僅需盡其忠誠義務不以任何形式將資訊透露給內部同仁或外部人士，在無標準可循之情況下，對於公務人員在執行日常業務時，勢必產生相當之困擾。退步言之，縱有常年之慣例或內規為依循，然而究竟是否可能有過度核定密等文書或有應核定但未核定之情形，目前亦無一套全面性並定期施行的清查程序，承辦人員亦無主動提出異議的權限，僅賴檔案管理單位通知

和其他機關來文建議時，方有開啟審查程序可能（參見文書處理手冊第 73 點），對於密等文書變更之爭議處理，我國尚未有完善之規範。

（2）尚未建立妥適的機敏性資料分級系統

目前實務運作上，已發現現行機密文書分級系統已不符合實際需要，特定機關為因應業務特性，會各自特定某些文書以「敏感（性）資料」稱呼之，並將國家機密、公務機密及前述所稱的敏感（性）資料以「機敏（性）資料」統稱，並加以訂定維護要點。以「經濟部駐外單位及國際貿易局機敏資料清單」為例，雙邊諮商及國際性會議、洽商協定、訪問行程及人員名錄等，若未被列入密等以上的機密資料，則列為敏感資料。此番區分之實益為：以利於賦予不同機敏性等級的資料相應之保護措施，使維護成本與其利益相當。

（3）尚未意識到妥適的資料分級系統方能配置同等級之保護措施，確保行政效率及成本控制

我國對於機密文書，係以紙本處理、儲

存及保管為原則，在公文資訊系統中僅得會登錄（及顯示）密件來文日期與文號，主旨則會載明「密不錄由」，而以紙本處理之慣例方式，需消耗掉大量的紙張、人力維護與儲存空間。

2013 年 10 月上路的新個人資料保護法，由於當中規定各機關應訂有「安全維護措施」，致使許多機關將含有個人資料之文書傾向列為公務機密之維護，而變成必須採用紙本作業原則。然此舉對例行業務本就在處理民眾個人資料之機關，如戶政機關及勞工委員會及所屬各機關，顯係期待不可能。除了成本過鉅外亦將造成行政效率延宕，嚴重影響業務運作並可能使個人資料之本人在行使個資法所賦予的權利時，受有相當程度的阻礙。

3.英國作法

參考國外作法，英國對於機敏性資訊建有「政府防護標記系統（The Government Protective Marking System）」，機敏性資訊由高而低分為：三階國家機密、限閱級（Restricted）、防護級（Protect），並由主管機關資訊專員辦公室發布核定標準、舉例敘

明及依等級之對應處理程序與保護措施等指導文件。

美國則對於「受控制的非機密資訊（Controlled Unclassified Information）」係由總統發布行政命令加以定義並規範，指出特定資訊雖與國家機密或聯邦政府重要利益無關，但因含一定敏感性，必須以法律賦予保護措施、管控傳播管道以防止未經授權之揭露；同時這些受控制的非機密資訊應有統一的標注和管理機制，才能使機關間進行有效的資訊共享、情報分析以利國家政務之推行。目前主管機關為國家檔案記路管理局，協調各部會之意見後發布統一分類目錄、標記機制與實施指引（包含分類、標記、限制傳播、解除控制、查核機制及爭端解決等程序）。目前被劃分為此類的資訊共有 22 類，例如隱私、稅務資料、資訊系統脆弱點等。

4.建議

承前，就現行規範並對比實務運作之狀況，可認我國宜儘速建立「敏感性資料」之概念，考慮是否於密等下另闢位階規範較低敏感性之資訊，重新建置我國之機敏性資訊分級分類系統，並為使各機關均有統一標準可遵循操作，於核定標準、核定流程、對應處

理程序和保護措施及核定等級爭議處理機制等，實宜一併加以規劃設計。

蓋資訊若有濫行核密或核密標準不清之情事，有可能會不當限縮公眾對政府資訊知悉的權利、架空資訊分級的意義且會使機關和人員輕忽列密資訊的價值，而無法妥適建立安全維護意識與文化。

（三）政府對於承包廠商之安全查核事項

美國眾議院情報委員會調查報告呼籲美國政府機關和企業不應該讓「中興」、「華為」成為資訊系統相關設備或零組件的供應商，並敦促美國企業應該阻絕未來收購、購併及合併「中興」、「華為」的可能性。

其他國家如加拿大和澳洲，亦對「中興」和「華為」採取保留態度，加拿大政府表示為建立安全的通信網路系統，得援引「國家安全例外」，以「潛在的安全風險」拒絕某些企業的投標；澳洲則已經禁止「華為」參與資訊服務基礎建設的競標。

1.我國現況

雖然資通安全會報對於機關的安全等級作區分，但是卻沒有細分到各機關內部系統的

安全等級，而是下放給各機關自行管理。關於業務系統或設備的採購，部分機關並未依機密等級去作評選標準，部分較為敏感的機關在採購實務就會特別注重安全性，不過，在評選項目沒有特別去規定，以免遭受歧視廠商或是圖利特定廠商之批評，但在評分上會列入考慮。

國內機關資訊採購還是較注重履約能力，機關因應實際需求訂定相關的要求，但又不能限制競爭。面對華為的實例，國安局表示為恐危及國安，已決定禁止政府採購可能涉及國家安全之通訊設備產品。

2.美國作法

美國資訊安全監管署（Information Security Oversight Office，簡稱 ISOO）位國家檔案局下，負責發佈落實行政命令（包括機關單位與和機關單位合作的廠商或相關單位）的指令，與檢視機關單位的遵循情況，以及建置與發布機密資訊（包括處理、貯存、分配、傳送與損壞）的標準與指引，執行第 13526 號行政命令的現場遵循評估，以及與處理機關落實行政命令的投訴（Complaints）。

透過總統行政命令第 12829 號，在 ISOO 項建置「國家企業安全方案」（National

Industrial Security Program, 簡稱 NISP），以達成節省費用之目的，結合聯邦政府與企業（含承包商、被授權人、被批准人等）為夥伴關係，共同維護機密資訊的安全。NISP 以安全程序的一致性；在安全程序實現互惠，特別是有關設施和人員安全查核；消除重複或不必要的要求，特別是機關查核；與實現降低安全成本的目標等四大原則。並提出對於企業所持有之機密資訊建置單一整合一致的安全維護系統的要求，以實現各份與機密資訊相關的契約間對於資訊安全的要求趨於一致。「國家企業安全方案」的主要簽署部會為能源部（Department of Energy）、核能管理委員會（Nuclear Regulatory Commission）、國防部（Department of Defense），和中央情報局（Central Intelligence Agency）。

國防部依據「國家企業安全方案」於 2006 年 2 月發佈「國家企業安全方案操作手冊（National Industrial Security Program Operating Manul, 簡稱 NISPOM），並更新至 2013 年 3 月 28 日。該「操作手冊」係基於完善威脅分析和風險管理實踐的企業安全流程，並在政府機關間建立一致的安全政策和的作法。以公私部門協力的夥伴關係，在複雜且不斷變化的資訊系統安全和實體安

全上，授與企業更直接地管理其行政面的安全控制。該操作手冊於安全查核（Security Clearances）章節的部分，特別針對設備場所（Facility Clearance）、人員（Personneal Clearance）與受外國所有、控制或影響的美國公司（Foreign Ownership, Control or Influence, 簡稱 FOCI）加以規範。FOCI 政策為美國政府批准外資在美國境內從事投資活動，但前提是該公司必須通過符合保護國家安全利益的審核，並確保該公司不能威脅到美國的安全與出口控制，以及未經允許而使用（Unauthorized Access）關鍵技術的出口控制、機密資訊、與特別類別的機密資訊。

除此之外，美國外資投資委員會（Committee on Foreign Investment in the United States，簡稱 CFIUS）依據美國 2007 年所頒佈的「外商投資國家安全安全法案」（Foreign Investment and National Security Act, 簡稱 FINSA）之規定，對於符合特定條件的外資進行較為嚴格的審核，而特定條件係指參與交易的的外國公司（含個人）受外國政府所控制，而該控制國涉及防止核子武器擴散以及其他與國家安全相關的問題；或其曾經破壞會試圖破壞國家安全。

3.建議

（1）應依資訊本身的性質是否涉及國家安全進行分類，僅單以機關分級可能不足

處於資通訊發展快速與科技技術的進步，對於資訊的快速流通與存取（Access）資訊設備的採購應該因應所可能接觸的資訊（尤其是涉及國家安全的資訊）進行分級，不應單僅按機關的資訊安全進行分級。

（2）以資訊設備與服務全生命週期作為安全查核的標的

當資訊設備與服務的採購涉及國家安全時，建議應特別注意資訊之設備與服務的全生命週期進行安全查核，廠商於得標前後需持續保持符合國家安全的條件，否則將可能產生廠商於得標前後計畫的控管產生不一致，但又沒有相對的管理措施，使涉及國家安全的機密資訊陷於莫大的風險之中。

（3）在外人投資審查階段輔以國家安全的審查配套，並允許納入 FOCI 的政策考量

參考美國作法，進行外人投資案件審理時，將會特別考量該投資是否涉及國家安全，並審查該公司為外國所有、受外國控制或影響的公司。政府機關於進行資訊設備或服務採購時，應該允許機關特別考量涉及國家安全的採購政策。

（四）政府安全防護政策架構建議

1.我國現行法制架構下的「機關安全」概念

我國對於「機關安全維護」的內涵及考量，偏重於「實體安全」之面向上，亦即預防及阻止可能之天災及外部人禍而造成機關場所實體毀損、人員傷亡之後果。對於政府機關安全維護之任務，主要係交由法務部轄下的政風機構辦理，其權責之法依據為「政風機構人員設置管理條例」第 4 條第 8 項。至相關具體執行面上之規範，各機關單位主要是依法務部訂定之「政風機構預防危害或破壞本機關事件作業要點」及行政院所發佈之「安全管理手冊」為依循。

2.問題檢討

參考澳洲對於政府安全政策框架之設計，安全核心的元素實可分為：人員安全、實體安

全及資訊安全。確立核心政策要素之後，便能有效建構具全面性、整體性、符合個別安全要求但又能互相協調配合之安全政策框架；對應之法制設計，亦能減輕不同主管機關訂立法條時，可能會有的規範衝突、矛盾、重疊而產生法律概念不清楚而執行上亦產生困難之情狀。

我國歷來的機關安全法制設計上，侷限於實體安全之面向，而資訊安全及人員安全雖亦有相關法規規範，但由於理念上並未意識到各面向之政策、方針、措施及規範有相輔相成、互通有無及協力合作之必要，故規範設計上呈現發散、不同主管機關各自管轄的狀況，此番情狀易造成制度重疊、規範漏洞及灰色地帶或解釋上矛盾或不清楚的問題，宜重建「機關安全」之內涵，方能建立全方位、整合性的安全維護政策。

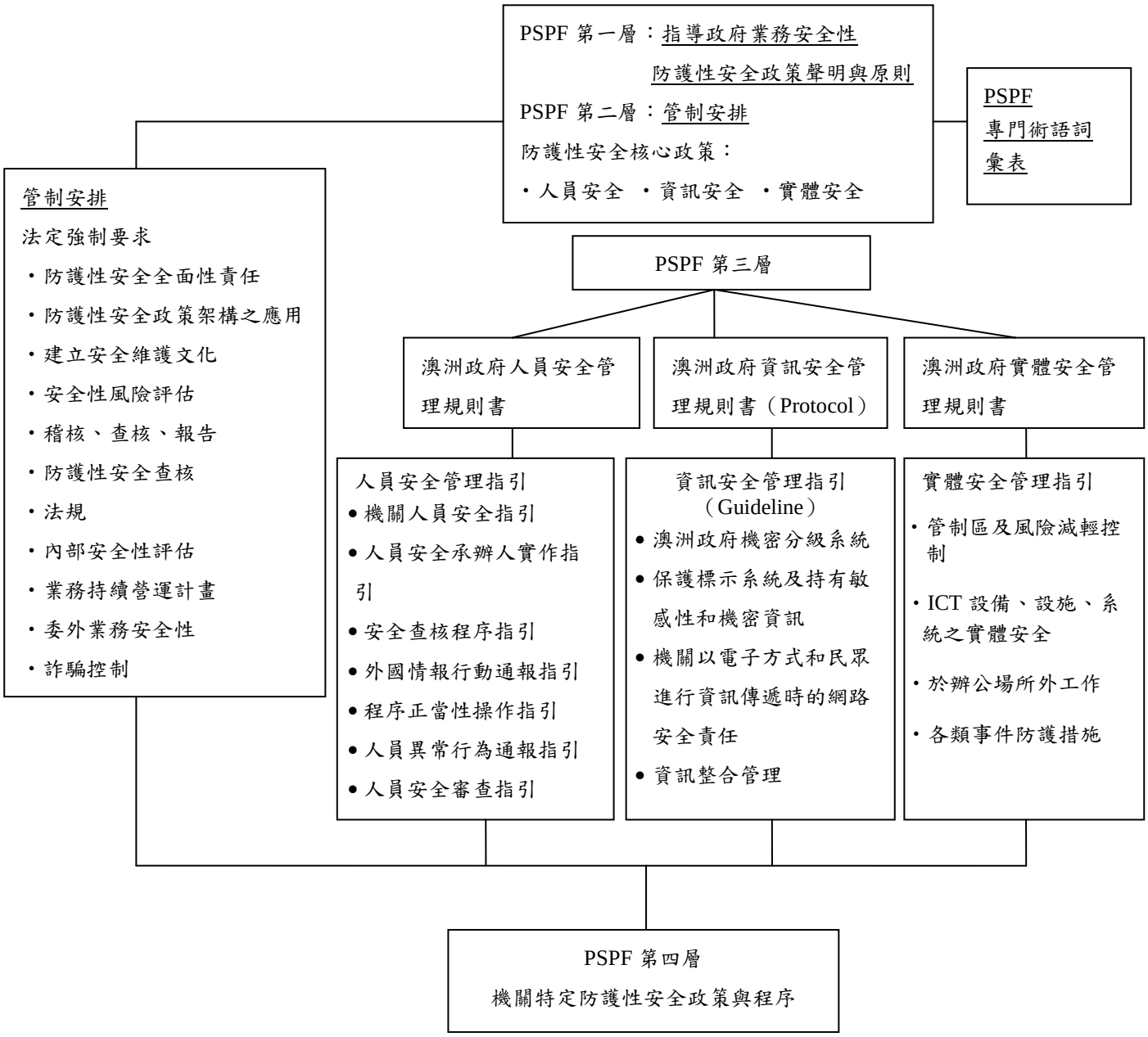
3.國外立法例之參考

以澳洲於 2012 年 12 月發布的防護性安全政策架構（Protective Security Policy Framework，簡稱 PSPF）為例，其對於安全政策之整體架構藍圖相當清楚、完整、細緻，對我國而言有極高的參考價值。

澳洲防護性安全政策架構整體規劃藍圖如

下：

圖 1：澳洲防護性安全政策架構整體規劃藍圖



資料來源：澳洲司法部網站

安全政策架構的第一層次，先闡明政策聲明及相關的上位原則。第二層次則提出三大安

全核心政策及 11 項的通則性的強制法定要求，各項要求下並另訂定指導文件，讓機關易於符合法遵需求。舉例而言，由於任一面向之安全維護任務，均有委外利用民間專業資源之可能，故第 10 項要求「委外業務安全性」便訂有「委外服務及職能安全性要求（Security Requirements of Outsourced Services and Functions）」之指導文件。另外，為避免各機關用語上之不一致或對於法律概念有歧異造成日後遵循上的困擾和衝突，特地編訂了專門術語詞彙表（PSPF-Glossary of Terms），提供詳細的定義說明與解釋。

第三層次則更細緻的提供機關得以具體執行安全要求的「管理規則書（Protocol）」及「指引（Guideline）」，例如：人員安全面向上，提供安全查核程序、人員異常行為判斷及通報的參考指引；資訊安全面向上提供機敏資訊分級系統與標準、安全保護措施及資訊整合管理指引；實體面向上，提供如何劃分辦公場所安全等級、實體安全風險評估及對應措施、如何擇用適當之安全設備等，提供各機關一致性的作法，使跨部門政府業務執行上能更為順暢，並幫助政府機關履行國際性的義務。

第四層次為「各機關之特定政策與程序」。各機關應依各自需求及其業務上之特殊性，制定最佳之安全保護政策和程序，這些政策和程序也必須同時補充和支持其他機關之運作。

4.建議

綜上，我國雖然在資訊及實體安全維護面向上均已設有安全維護規範，但主責之主管機關並不相同（資訊安全為資通安全辦公室辦理、實體安全維護由政風機構辦理），但目前尚未有進行整合、協調之動作；再者，關於人員安全面向，較注意外來之侵害而對於內部威脅較不甚重視，或可謂並無統一處理之上位原則或指導規範，係由各機關自行辦理。至為何有建立整合性安全框架之必要？舉例而言，若從資訊安全之面向出發，除了利用資訊分級、分類及利用科技技術管理、加密保護等確保資訊不會無故外洩、滅失或毀損外，如何管理內部人員、臨時聘僱人員、委外資訊廠商的執行人員或清潔人員等接近使用權限亦相當重要，此部份即會與「人員安全」產生重疊；又伺服器機房、紙本儲存空間及辦公場所的出入管制、動線設計、火/水災或電力供應等預防、管制措施又會與「實體安全」加以重疊。由此可知，整

體性地規劃全方面安全維護框架，實有其必要性，除能避免機關安全的維護上出現漏洞外，亦能使各機關執行法規要求時簡化作業程序，提昇效率並減少不必要的人事支出與其他成本，同時也能使各機關間配合、協調與互助更加容易。