行政院102年12月25日　核定

國家資通訊安全發展方案

（102 年至 105 年）

行政院國家資通安全會報

中華民國102年12月

目　次

第一章　前言

廿一世紀資訊科技運用的普及與網際網路的蓬勃發展，使資通訊科技應用儼然已成為每個人日常生活中的一部份，並改變了人類生活模式，然令人擔憂的是資訊科技帶來的資通訊安全問題，促使資通訊安全議題成為各國關注的焦點。

為強化國家資通訊安全能力，行政院於90年1月17日第2718次會議通過「建立我國通資訊基礎設施安全機制計畫（90年至93年）」（以下簡稱第一期機制計畫），並成立「行政院國家資通安全會報」（以下簡稱本會報），積極推動我國通資訊安全基礎建設工作。

94年至101年，行政院賡續推動「建立我國通資訊基礎設施安全機制計畫（94年至97年）」（以下簡稱第二期機制計畫）及「國家資通訊安全發展方案（98年至101年）」（以下簡稱第三期發展方案），在中央各部會、直轄市及縣市政府共同努力之下，已逐步達成「建立整體資安防護體系、健全資安防護能力」之階段性目標。

我國政經情勢特殊，面對全球複雜多變的資通訊環境，以及日益嚴重的資通訊安全威脅，持續落實並精進各項資通訊安全防護工作，實屬必要，爰此，本會報特研提「國家資通訊安全發展方案（102年至105年）」(以下簡稱本方案)，供為各機關現階段推動辦理資通訊安全防護計畫之重要依據。

第二章　全球資安發展趨勢

壹、全球資安威脅情勢

網際網路為人類帶來便利與快捷，然而伴隨網路普及化與消費者行為改變，引發的網路犯罪及個資保護等課題，已逐漸成為影響國家安全、社會安定的隱憂，全球正面臨嚴峻的資安威脅。(詳如圖1)

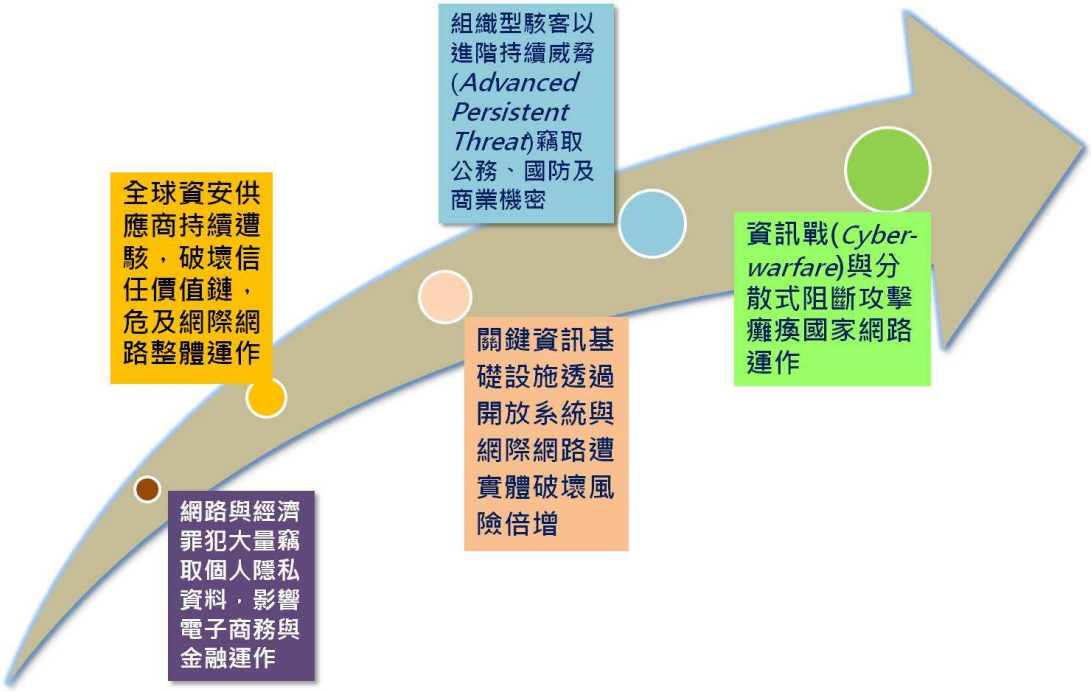


圖1、全球面臨的資安威脅

一、 組織化網路犯罪猖獗

國際上資安威脅已從個別、單純的炫耀，演變成有組織、以經濟或政治等特定利益為目的的入侵行為。近來網路犯罪組織趨於高度專業分工，加以「網路戰」發起不受時空條件限制，具足首戰即決戰之特性，已使國家安全之概念及範圍產生實質變化。

二、 個人隱私資料被竊與金融詐騙事件頻傳

駭客透過電子郵件社交工程或利用網站應用程式漏洞、網頁掛馬等方式，在受害電腦植入惡意程式，以竊取個人隱私資料，並與犯罪集團合作，進行金融詐騙。例如 2011 年 4 月日本 Sony PSN (Play Station Network)遭駭客入侵，導致近 8,000 萬筆個資外洩。

三、 關鍵資訊基礎設施資安風險增加

在數位經濟時代，重要資通訊設施一旦遭受破壞，勢將影響經濟、民生及整體政府運作；而各類關鍵基礎設施（Critical Infrastructure，CI）的監督控制與資料獲取系統（Supervisor Control And Data Acquisition，SCADA），通常較無堅實的資安防護設計，兩者均為網路駭客重要攻擊目標。

四、 進階持續性威脅加劇

進階持續威脅(Advanced Persistent Threat，APT)攻擊之特徵為針對特定目標、低調、隱匿、手法多變、客製化等。近期美、英、法、德、紐及澳等國政府，均相繼傳出疑似遭 APT 攻擊，企圖竊取該國政府重要及機敏資料。

五、 零時差攻擊造成資安防護困難

「零時差攻擊(Zero-day Attack)」係指在軟體弱點尚無修補方式之前，所出現之攻擊行為。駭客通常利用假冒寄件者身分、引人興趣之主旨與內文，並結合含零時差攻擊之附件檔，進行電子郵件社交工程攻擊。一旦收件者開啟電子郵件之附件檔，即被植入含零時差攻擊之惡意程式。

貳、主要國家資安政策發展趨勢

近年各主要國家、區域均積極推動新資安政策，以因應全球資安威脅情勢，茲綜整主要發展趨勢如下，以作為我國研議資安政策與策略之參考：

一、資安議題提升至國家安全層次

美國於 2009 年歐巴馬總統上任後，匯集各界專家學者的意見，針對過去美國的網路安全政策與現況進行綜合性評估，承諾建立起可靠且堅固的資通訊基礎，並宣布加強美國網路安全的新計畫，將資安提升至國家安全的層次。南韓藉由「e-Korea Vision 2006」政策，推動高速寬頻網路服務，並因應資安威脅所帶來的衝擊，在「Broadband IT Korea Vision 2007」政策中，將資安列為國家基本政策。日本政府為了增強國家競爭力與維持社會經濟發展，近年資安政策發展方向著重提升國家安全與系統安全、增強資安教育、促進國際合作等。中國大陸於 2008 年第 16 屆中國共產黨四中全會，將資訊安全列為國家安全的重要組成部分，明確提出「增強國家安全意識、完善國家安全戰略」，以確保「國家的政治安全、經濟安全、文化安全與信息安全」。

二、重視國民相關權益保護議題，尤其是個人資料與隱私權保護等

美國 2011 年發布「國家身分識別策略（National Strategy for Trusted Identities in Cyberspace，NSTIC）」，致力於協助技術或平台發展，以利進行更高層次信任之線上交易。新加坡政府自 2008 年起發展長達 5 年的資通訊安全發展藍圖，以提供高速網路及資通訊安全基礎設施創造更多加值服務的安全環境，像是以地區為基礎的市場行銷、物流的追蹤及更多可調適性的網路服務，

並應用於銀行業、教育業及健康照護等。日本於 2005 年實施「個人情報保護法（Japanese Personal Information Protection Act，JPIPA）」，明文規定保有個人情報的企業有義務保護個人情報並避免洩漏；並在 Information Security 2011 列舉加強國民和用戶的保護、推廣個人資訊保護等具體措施。

三、逐漸重視雲端運算相關安全議題

美國聯邦政府於 2009 年底針對各政府機關開設雲端運算技術和服務的網站，作為歐巴馬政府削減預算、提升行政效率、環境綠化等政策的重要基礎，並任命新的聯邦政府資訊長-Vivek Kundra，展開一連串的雲端運算政府(Government Cloud)改造計畫。美國國家標準與技術研究院(National Institute of Standards and Technology，NIST）於 2011 年底接連發布了幾項特別文件說明雲端運算安全的重要、問題與建議的做法：包括 SP 800-144 (公有雲的安全和隱私的準則草案)、SP 800-145 (NIST 對雲端運算的定義)、SP 800-146 (雲端運算簡介和建議草案)、SP 500-293Volume I & II (美國政府雲端運算技術發展藍圖)。日本在「Secure Japan 2010」中強調雲端安全之重要政策與措施，包括確保雲端運算技術的資訊安全、雲端資訊安全確保方案標準化、中小企業雲端運算資訊安全、擬定雲端服務水平的查核表、針對雲端運算服務的高信賴/省能源網路控制技術進行開發、推動資訊安全相關的策略性研究開發及新世代資訊安全技術的研究開發等。中國大陸在「十二五」規劃中提及，將推動國家七大戰略新興產業，而其中的新一代資訊技術，即將雲端運算發展列為重要發展項目。

四、重視政府與民間或產學合作議題

美國 85%的 CI 屬於民營，為此美國提出實質防護 CI 之國家政策，對政府、CI 業者、民間團體及個人如何建立合作及聯盟的新典範，提供具體策略，以增進國家安全。日本 2010 年「守護國民資訊安全戰略」計畫，持續過去政府與民間合作的推動模式，在保障安全、危機管理的觀點下，將規劃方向與推動體制予以重點式的加強，以期能達到更大的政策效果。中國大陸在「國家中長期科學和技術發展規劃綱要」中，提出將「信息產業及現代服務業」列為國家長期重點發展產業，在「面向核心應用的信息安全」中點出關鍵資安技術方向，且以研發減稅、政府採購、軍民合作及國際合作四大面向之鼓勵措施，推進中國資安技術發展。韓國當地的大型企業都很願意和學術單位合作，並投入大筆資金，發展出韓國相當重要的資訊研發成果。

五、重視國際合作防護與交流議題

美國歐巴馬總統 2011 年正式宣布推動「國際網路空間策略（International Strategy for Cyberspace）」，其中闡述了美國在網路空間的國際策略，從國內到國際，從國際到全球的全方位整合政府與民間力量，結合美國自由民主與自由市場的傳統價值與網路科技的應用，積極佈局後 911 的網路空間新秩序。韓國亦與國際組織密切合作，如發展與國際組織合作的領域，並對外國政府提供政策諮詢，以及電子政務和公務員培訓的行政措施。新加坡政府 2006 年 6 月公布「智慧國家 2015」（Intelligent Nation 2015, iN2015）計畫，以創新、整合及國際化為主軸，希望在 2015 年達到「用資通技術來建立一個智慧型國家與全球性的城市」，將資通訊科技融入民眾的生活、工作與休閒活動中，把新加坡發展

成一個「科技、基礎架構、企業與人力」四者綜合一體的科技城市。日本在 Information Security 2011 強化資訊安全政策，以適應資訊安全環境的變化，並強化國際聯盟，加強與美國、東盟、歐盟的聯盟關係，以及透過國際會議，如 APEC(Asia- Pacific Economic Cooperation)、ARF(ASEAN Regional Forum)、ITU(International Telecommunication Union)、Meridian 及 IWWN(International Watch and Warning Network)等具體措施。中國大陸在「國家信息化安全標準化『十一五』規劃」之重點在於進行資安戰略與基礎理論研究、資安標準之制定與推廣工作，以及定期參加國際標準化活動。

第三章　資安現況分析

壹、組織架構

依據102年1月修正之「行政院國家資通安全會報設置要點」（詳如附錄1），本會報負責國家資通訊安全政策、通報應變機制、重大計畫之諮詢審議及跨部會資通訊安全事務之協調及督導，下設網際防護及網際犯罪偵防等2體系。（本會報組織架構詳如圖2）

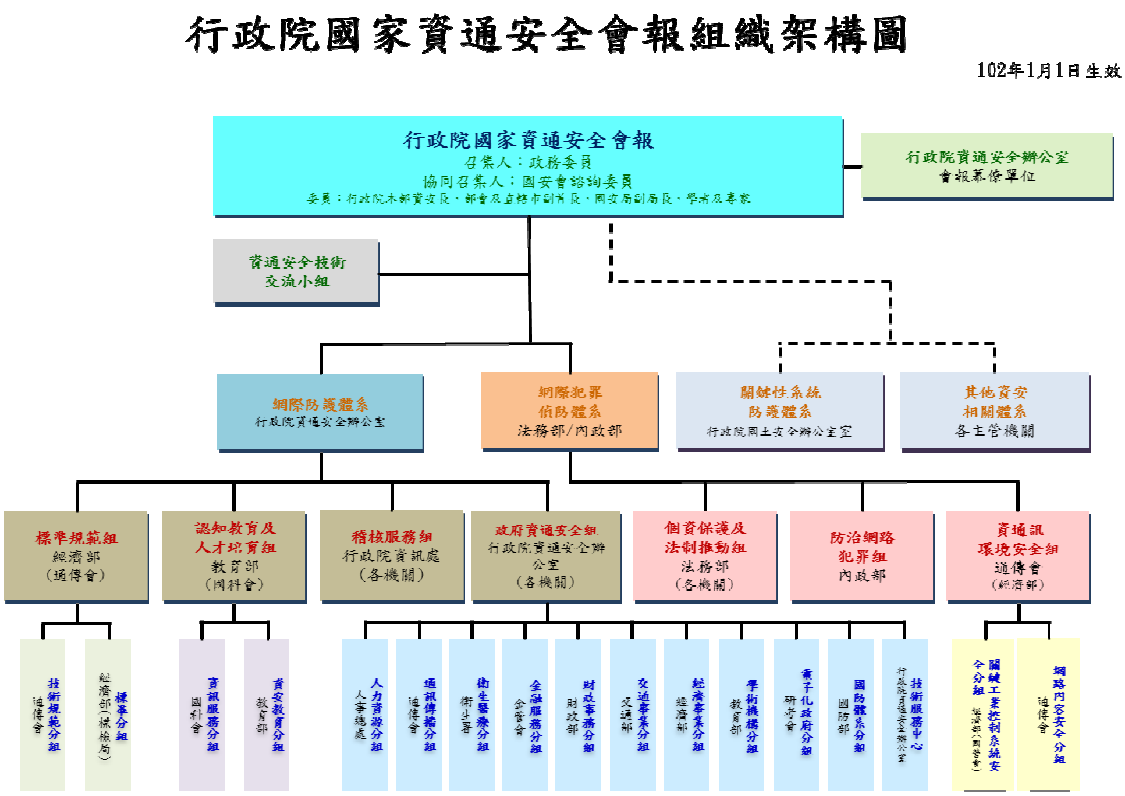


圖2、行政院國家資通安全會報架構圖

本會報自90年1月成立以來，早期是由前行政院科技顧問組兼辦幕僚作業，後考量整體資安情勢日趨嚴峻，行政院於100年3月修正「行政院國家資通安全會報設置要點」，成立「行政院資通安全辦公室」，期強化國家資安政策規劃、提升資安通報應變效率及加速重大資安計

畫推動。配合101年1月1日行政院院本部組織再造後，「行政院資通安全辦公室」成為行政院常設任務編組之一，依「行政院資通安全辦公室設置要點」規定，該辦公室除辦理本會報幕僚作業外，主要任務如下：

一、 國家資通安全政策與措施之研擬及推動。

二、 國家資通安全事件之通報、應變及管考。

三、 國家資通安全重大計畫之推動與管考。

四、 國家資通安全相關法制及規範之協調、聯繫及推動。

本會報各體系與分組之主辦機關（單位）以及任務如下：

一、 網際防護體系：由行政院資通安全辦公室主辦，負責整合資安防護資源，推動資安相關政策，並設下列各組：

(一)標準規範組：由經濟部主辦，負責發展資安產品與管理系統之認驗證標準及體系，推動資通安全之技術規範及管制，發展、維護政府機關資安作業規範及參考指引。

(二)稽核服務組：由行政院資訊處主辦，負責推動落實資安稽核制度，協助各機關強化資安防護工作之完整性及有效性，並透過持續改善以降低資安風險。

(三)認知教育及人才培育組：由教育部主辦，負責推動資安基礎教育，強化教育體系資通安全，提升全民資安素養，提供資安資訊服務，建立資安人才培育體系。

(四)政府資通安全組：由行政院資通安全辦公室主辦，負責規劃、推動政府各項便民資通訊應用服務之安全機制，輔導政府機關資安技術服務、資安防護及應變，統合政府機關

資安人力充實及運用。

二、 網際犯罪偵防體系：由法務部及內政部共同主辦，負責防範網路犯罪、維護民眾隱私、建立資通訊基礎設施安全等工作，並設下列各組：

(一)個資保護及法制推動組：由法務部主辦，負責檢討修正維護民眾隱私及防制網路犯罪相關法令規章，建立安心信賴之資通訊法制環境。

(二)防治網路犯罪組：由內政部主辦，負責網路犯罪查察、電腦犯罪防治等工作。

(三)資通訊環境安全組：由國家通訊傳播委員會主辦，負責促進網路內容安全，防制網路犯罪，強化關鍵工業控制系統安全，建立資通訊基礎設施安全信賴機制。

為能掌握資安技術發展趨勢，充實資安作業能量，本會報自101年8月起設「資通安全技術交流小組」，按季邀集產、官、學、研代表研討資通安全技術，並分享特殊或重大資通安全案例發生原因與改善建議等。

貳、重大資安政策進程

本會報自90年1月成立以來，陸續推動3個階段，各為期4年之重大資通安全計畫或方案(詳如圖3)，已有效提升我國資安完備度，謹說明各期計畫或方案重點如下。

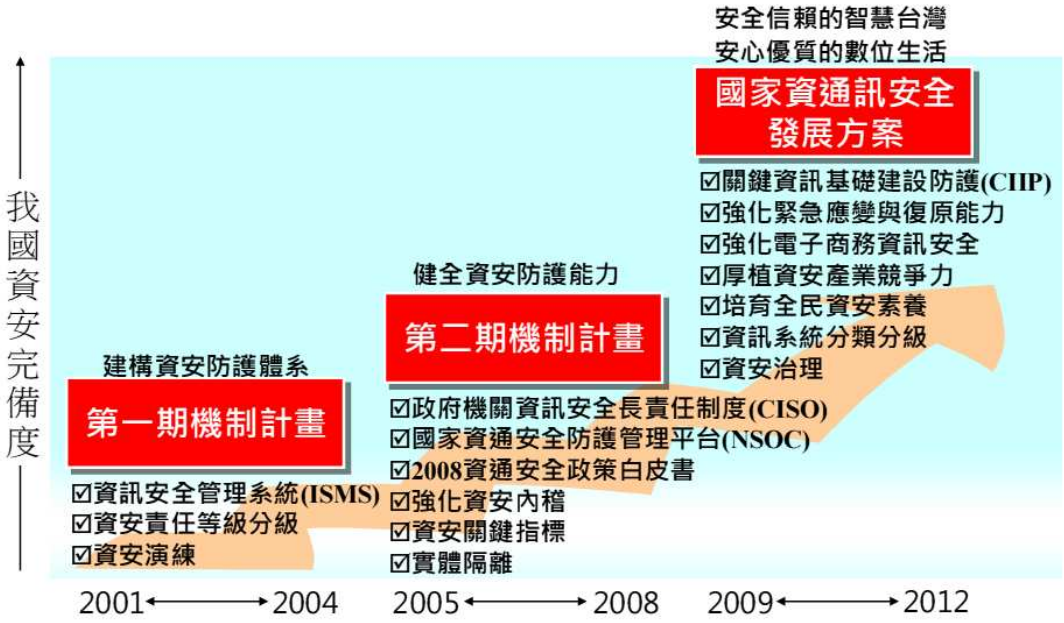


圖3、我國重大資安政策發展進程

一、第一期機制計畫

為統籌並加速我國資通安全基礎設施，行政院於90年核定第一期機制計畫，實施期程為90年至93年。本期計畫主要致力推動全國3,713個重要政府機關（構）建立整體資安防護體系。在實務作業上，將政府機關區分為國防、行政、學術、事業1（水、電、石油、瓦斯）、事業2（交通、通信、網路、航管）、事業3（金融、證券、關貿）、事業4（醫療）等7個不同屬性類別，每項屬性類別下再區分為A級重要核心單位、B級核心單位、C級重要單位及D級一般單位等4個等級，針對不同等級提供不同的資安支援並訂定不同的工作要求，以期在有限資源下，做好全面的資通安全防護工作。

此外，針對20多個CI的資訊系統實施資安管理方案，以推動建立資訊安全管理制度為首要工作，要求在限期內完成異地備援系統及通過國際資訊安全管理系統驗證。在資安認知推廣

及教育訓練方面，則規定資訊人員及主管人員應接受必要之資安技術訓練或管理課程。同時，亦規劃建立資安監控中心（Security Operation Center，SOC）預警及通告機制等項目。

二、第二期機制計畫

為延續第一期機制計畫之成效，行政院於93年核定第二期機制計畫，實施期程為94年至97年，為因應環境變遷於96年2月修正部分內容。

第一期機制計畫對於建立我國整體資安防護能力至為關鍵，本期計畫主要政策則包含政府機關資訊安全長（Chief Information Security Officer，CISO）責任制度、國家資通安全防護管理平台（National-Security Operation Center，N-SOC）、強化資安稽核、加強資安責任等級分級作業與機密資訊保護、建構資安關鍵指標等，對強化政府機關之資安能力產生一定的影響。

政府機關資訊安全長責任制度之推動始於94年，目前行政院院本部、35個部會與24個直轄市及縣(市)政府，均已由副首長兼任資訊安全長，負責督導「資通安全處理小組」，推動機關內之資通安全相關計畫。透過資訊安全長責任制度的落實，強化政府機關本身資通安全防護與管理責任，不僅彰顯資通安全專責人員的重要性，也使得各機關的資通安全工作更加受到重視。

N-SOC不僅提供一般監控與預警服務，且將重要核心政府機關納入防護範圍，並依其業務需求配置不同監控設施，如佈署入侵偵測系統、網域名稱系統（Domain Name System，DNS）

警示系統、內部網路警示系統、使用者端警示系統等。除了強化通報應變網站功能、定期進行通報演練外，亦適時針對資安聯絡人，發布系統漏洞、駭客訊息等資安警訊，有效提升整體通報應變之時效。

本會報稽核服務組（前行政院主計處電子處理資料中心主責）自90年起每年選擇20至30餘個重要核心機關進行資安外部稽核，提供稽核建議，協助受稽機關(單位)落實資安防護工作之完整性與有效性，並於94年起推動主管機關進行內部稽核。

奠基於92年之資通安全責任等級分級作業，95年重新界定分級標準，並將實施範圍擴及教育體系，納管單位數由3,713個增加為6,797個。依前行政院人事行政局發布行政院所屬各機關暨地方政府機關數，本項作業涵蓋率已達80%以上。

為預防使用者電腦遭駭客透過惡意電子郵件社交工程等方式攻擊，本會報於95年規劃執行電子郵件社交工程演練，並規定重要機敏機關，依需求評估採用有效的實體隔離作法與加密保護措施，以有效保護機密資訊的安全，目前相關機關均已落實執行。

而為評估我國資安發展現況，俾利規劃相關政策措施，積極推動資安防護，本期計畫自95年起亦開始建構資安關鍵指標，透過量化的數據，呈現近年來我國資通安全在認知與環境、整體防護能力及緊急應變功能上的表現。

三、第三期發展方案

前兩期機制計畫實施以來，對於促使各機關重視資安與帶動民間投入具一定成效。然我國資安整體資源投入有限，實不

利於正確評估資安風險，並將其有效地控制在可接受的範圍內。鑒於大環境因素及資安問題仍層出不窮，有訂定資安賡續發展計畫，加強實施各項資安作業之必要性。爰行政院於98年1月訂頒第三期發展方案，實施期程為98年至101年。本期方案考量資安政策延續性，以達成「安全信賴的智慧台灣，安心優質的數位生活」為願景，朝「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」四大政策目標努力。在執行上，分別從「需求端」與「供應端」，規劃符合政府、關鍵資訊基礎設施（Critical Information Infrastructure，CII）及企業需要的5項資安措施、共20個行動方案；在環境面，規劃強化法制建立、認知宣導、創新合作及衡量指標等利於形塑資安文化的4項措施、共10個行動方案。

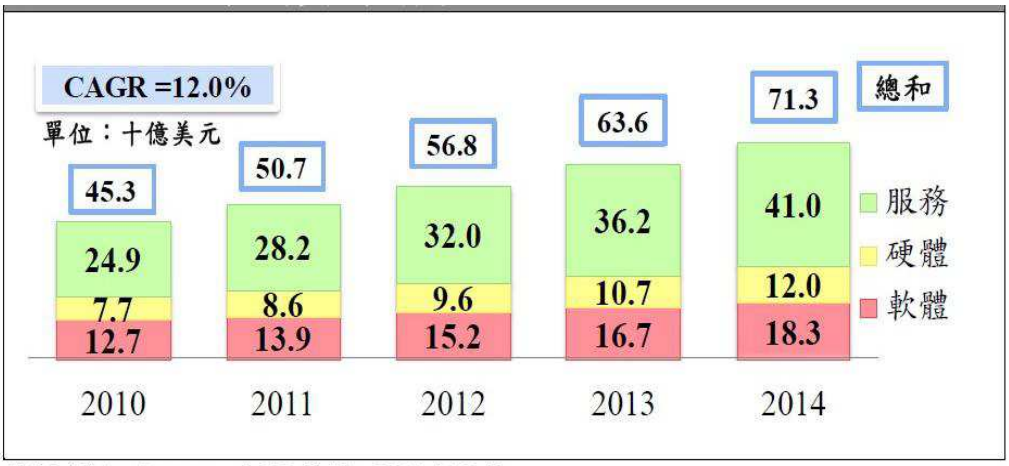
透過落實上開30個行動方案，在101年底已達成增加資安資源投入、提高資安法規整備度、提升全民資安素養、強化整體資安防護能力、推升資安演練比率及降低事故損失程度等效益，並逐步將政府推動資安的經驗擴散至民間及企業。

參、資安產業現況

一、全球資安市場規模

全球資安市場可區分為軟體、硬體及服務三大類別，其中軟體從2010年127億美元成長至2014年183億美元，年複合成長率(Compound Annual Growth Rate，CAGR)為9.6%；硬體從2010年77億美元成長至2014年120億美元，CAGR為11.7%；服務從

2010年249億美元成長至2014年410億美元，CAGR為13.3%。全球整體資安市場則從2010年453億美元，成長至2014年713億美元，年複合成長率為12.0%。(詳如圖4)

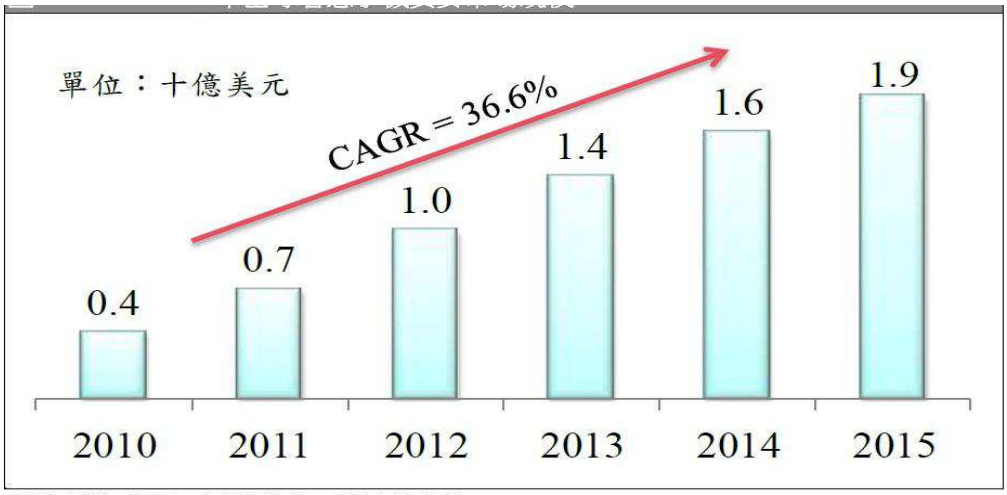


資料來源：Gartner，MIC 整理，2011 年 2 月

圖4、2010-2014年全球資安市場規模

整體資安市場將呈現持續成長之趨勢，主要趨動因素包含全球各地法規持續影響、環境威脅攀升(新型攻擊模式出現，如APT等)、智慧行動裝置與企業營運逐漸結合所引發新的安全弱點，以及雲端運算虛擬化所延伸之安全問題(如資料傳輸安全、權限控管或稽核問題等)。其中仍以法規及環境威脅為主要驅動因素，原因為前者牽涉企業營運之賠償問題，後者則因企業不易對其進行防護且市面上尚無完整解決方案。

其次為智慧行動裝置延伸出相關的安全需求，進而促使智慧手機資安市場成長，全球智慧手機資安市場規模從2010年4億美元，成長至2015年19億美元，CAGR為36.6%。(詳如圖5)

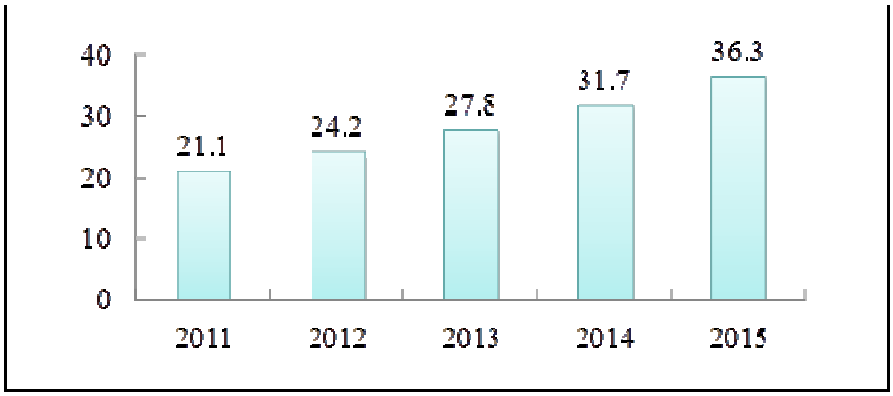


資料來源：IDC，MIC 整理，2011 年 5 月

圖5、2010-2014年全球智慧手機資安市場規模

二、台灣資安市場規模

台灣資安市場可分為台灣廠商與外商，其中台灣廠商將從2010年62億新臺幣成長至2014年127億新臺幣，CAGR為19.6%；外商將從2010年123億新臺幣成長至2014年190億新臺幣，CAGR為11.6%。整體台灣資安市場將從2011年211億新臺幣，成長至2015年363億新臺幣，CAGR為14.6%。 (詳如圖6)



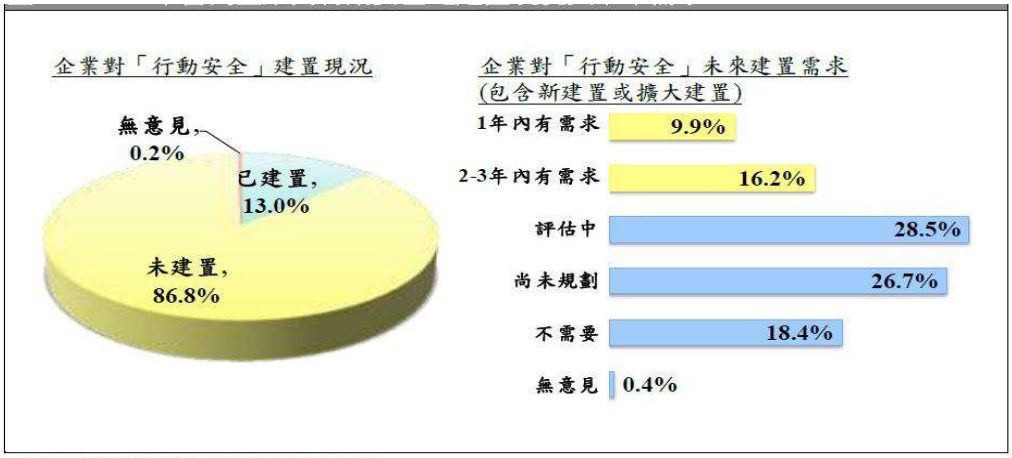
備註：單位為十億新臺幣
資料來源：MIC，2013 年 2 月

圖6、2011-2015年台灣資安市場規模

為因應急速變遷的社會環境，提升個人資料保護的周延程

度，個人資料保護法除將保護範圍由原本僅限於電腦處理之個人資料，擴大到所有個人資料，同時提高了賠償金額與刑事責任，並增列可進行團體訴訟等機制。更重要的是，適用行業從原本的公務機關與八大行業，擴大至公務機關、非公務機關及個人，該法於2012年10月1日正式施行後，已順勢帶動台灣資安市場發展。

其次為行動安全(Mobile Security)，因近年智慧行動裝置普及，企業內部員工使用智慧行動裝置結合工作或金流等情形日益增加，導致企業的資安防護邊界擴大(如個資外洩、網路詐欺、社交工程等)，進而延伸相關安全需求(詳如圖7)。台灣市場2011年企業於行動安全之建置比例雖為13.0%，但在未來三年內有相關需求之比例，則有26.1%，顯示整體台灣市場未來三年內將對行動安全需求有成長趨勢。



註1：有效樣本數 506 家大型企業
註2：行動安全，包含手機防毒、防火牆、防竊尋回、遠端控制、資料加密、身分認證、防垃圾郵件等功能
資料來源：MIC，2011 年 4 月

圖7、2011年台灣企業對行動安全之建置現況與未來需求

此外，在雲端運算安全(Cloud Security)需求方面，雖然目前台灣市場上雲端運算仍處於建置成長階段，但雲端資安產品

服務在近3年內，企業採用需求亦有增加之趨勢。且基於雲端運算的採用，以往多在企業內部進行資料儲存、傳輸、運用、管理等流程與地點，將隨之轉變，進而影響企業在各層面對資料的安全性考量，對於雲端資安產品服務之採用比例應有明顯增加的趨勢。

肆、資安發展優劣勢分析

經過3期機制計畫或發展方案的推動，以及政府與民間的共同努力，我國整體資安環境已有長足的進步，惟距離「建構安全資安環境，邁向優質網路社會」的願景，仍有一段距離。以目前的狀況而言，欲實踐前述願景，有關內部環境之優劣勢與外部環境之機會與威脅，如表1所示。

表1、我國資安整體SWOT分析

優勢（Strengths; S）	劣勢（Weaknesses; W）
1. 我國資通訊產業發達，擁有優秀資通訊、科技人才。 2. 擁有高素質的人力，具創新性且對於新科技接受度高。 3. 設立行政院資通安全辦公室，統籌政府資通安全工作。 4. 國家安全會議下設國家資通安全辦公室，統籌國家資通安全工作。	1. 使用者在行為面並未落實資安，認知與警覺性仍有待提升。 2. 資安相關法制之完備性仍有努力空間。 3. 資安組織、人力與預算未法制化。 4. 資安治理已推動4年，但成效仍有待提升。 5. 應用程式安全仍存在許多漏洞，資安事件頻傳，駭客手法防不勝防。 6. 政府資安防護分工較不明確。 7. 關鍵資安科技被先進國家所掌握且不易突破。 8. 資安產業發展條件受限。 9. 資安國際合作空間受限。 10. 雲端相關法制與技術能量之完備性不足。 11. 資安防護能量遠不及組織型駭客

	攻擊能量。
機會（Opportunities; O）	威脅（Threats; T）
1. 政府持續發展資通訊應用，透過行政院組織改造契機，優化政府資訊架構，並提升整體資通安全。 2. 隱私權與智慧財產權保護議題受重視且個資法業已施行。 3. 在資安事件蔓延、法令規範效應下，促使全球資安市場成長。 4. 行政院國家資通安全會報技術服務中心之轉型，可為資安產業帶來契機。 5. 在國際社會中，各國皆須強化國際地位與影響力，並積極擴展資安合作機會。	1. 資安績效評量與稽核不易，潛在效益經常被忽略，致資安資源投入不足。 2. 數位證據保全不易，且鑑識能量不足。 3. 網路已成為犯罪工具、犯罪場所及犯罪目標。 4. 資安資訊分析分享機制未盡完善。 5. 先進國家積極投入資安科技研發與資安鑑識產業，保持優勢並拉大與後進者差距。 6. 兩岸特殊政經情勢，制約台灣直接參與國際相關組織或活動。 7. 駭客手法日益精進，且已成為組織型犯罪，資安威脅大增。

在當前情況下，我國之資通安全發展環境實不容樂觀。我國目前所擁有優秀資通訊、科技人才與高素質人力及創新性等優勢，隨著各國對於人才培育的重視，很快地將不復存在，同時資安防護經驗與駭客行為模式資料等亦具時效性限制，須及時妥善運用。因此，如何積極看待、處理及充分利用目前的優勢，使其朝向正向發展，至關重要。

政府必須清楚地意識到現階段所面臨的資安問題與可能遭遇的威脅與挑戰，掌握時機、用前瞻及策略的角度思考問題、分析問題與解決問題。是以，確立本方案願景與策略目標，針對現階段我國發展資通訊安全所面臨問題，制訂有效的解決對策，實為當務之急。但「徒法不足以自行」，更為重要的是積極落實對策並持續檢討改進。

第四章　願景與策略目標及發展藍圖

壹、願景

隨著資通訊科技日益蓬勃發展，如何提供安全、安心、可靠的網際網路使用環境，創新資安服務價值，掌握雲端運算優勢，朝向虛擬整合化資安服務，已成為邁向優質網路社會的關鍵議題。我國已完成3期機制計畫或發展方案之推動，資通安全管理機制已日趨健全，個人資通安全意識亦日漸提升，然如何結合產、官、學、研各界資源與能量，讓網路社會朝向良性發展實屬重要。本方案以達成「建構安全資安環境，邁向優質網路社會」為願景，期經由前瞻政策引導，在政府與民間共同合作之下，透過國家整體資源力量，逐步推動並落實優質網路社會。(詳如圖 8)

圖 8、願景與策略目標

貳、策略目標

我國為提升國際資訊產業競爭力，積極投入資訊科技的研發及建置，在政府「愛台 12 項建設」總體計畫中積極推動「智慧台灣」計畫，期在生活型態快速變遷趨勢下，任何人都能夠不受教育、經濟、區域、身心等因素限制，透過多種管道享受經濟、方便、安全及貼心的優質 e 化生活服務，並將台灣建設為安心、便利、健康、人文的優質網路社會，實現「資訊服務島」的願景。由於資訊科技的推動及資訊化的普及，使得我國與全球其他國家同樣面臨高度依賴資訊環境可能引發的資安風險。隨著資通安全問題層出不窮，使得資通安全議題已經提升為影響國家及政治、經濟安全等重大問題。為了落實我國優質網路社會願景，特提出 4 項策略目標如下：

●目標一：強化國家資安政策，建立安全資安環境。

網際網路的快速發展已帶來政治、經濟、社會、文化、科技及軍事等各層面的資安威脅，我國要如何建立安全及可信賴的資通安全環境，保護個人、企業及政府各部門的資通安全，維護國家關鍵基礎設施，增進民眾的信心，確保經濟、社會及國家安全，乃政府必須優先處理的課題。在複雜的網際網路環境中，因為資通安全是全方位的工作，必須就適法性、外在競爭環境的變遷、資產風險評估原則、資產價值，以及相關資訊服務等因素擬訂資安策略，不斷精進國家資安政策，投入相當資源，強化自我資通安全防護能力，建構國家整體性的資通安全服務環境，才能有效杜絕資安危害，維護國家資通安全。

●目標二：完備資安防護管理，分享多元資安情報。

為建立可信賴的資通安全環境，確保資料、設備及網路系統的安

全，保障民眾權益，建置政府專屬 G-ISMS (Government- Information Security Management System)體系，以提升政府機關資通安全管理作業，妥善保護各機關資訊之機密性、完整性與可用性並建立機關聯防機制，降低資安事故之風險至可接受之程度，並加強 G-SOC (Government-Security Operation Center)資安防護管理二線監控機制及情蒐與分享之整合，透過資安技術服務雲端化，擴大資安監控範圍；另透過 G-ISAC (Government -Information Sharing and Analysis Center)分享平台，建立具資安自動通報作業之平台。

●目標三：奠基資安技術能量，整合科技實務應用。

加強與企業及學研機構之資安技術研發合作，發展新一代全方位資安整體技術解決方案，涵蓋資安弱點偵測、滲透測試、入侵威脅、網站應用程式(Web AP)安全、防火牆應用與事故通報管理等領域核心技術。同時在網路應用方面，研究新興資安科技應用及技術標準，掌握雲端、虛擬與行動資安防護等關鍵自主技術，提升資安威脅整合分析之鉅量資料運算能力，並進行新興資安技術實務之應用。

●目標四：擴大資安人才培育，加強國際資安交流。

擴大資安科研人才培育合作，制訂政府資安人才引進與培育配套規劃，發展資安專業職能及相關認證機制，參考國際資安人才培訓經驗，建置資安人才訓練與實習之專業學習環境；積極佈建國際資安合作交流平台，參與國際資安組織相關活動，維護 APCERT(Asia Pacific Computer Emergency Response Team)、APWG(Anti-Phishing Working Group) 、 AVAR(Association of anti-Virus Asia Researchers) 、 FIRST(Forum of Incident Response and Security Teams)等會員身分，掌握國際資安最新發展趨勢，並透過 G-ISAC 資安資訊分享機制，與國

際資安組織包括日本 JPCERT/CC(Japan Computer Emergency Response Team /Coordination Center)、馬來西亞 MyCERT(Malaysian Computer Emergency Response Team)及韓國 KrCERT/CC(Korea Computer Emergency Response Team /Coordination Center)等擴展國際資安相關合作計畫，以加強國際資安交流。

參、資安策略發展藍圖

本方案定位為我國未來四年(102~105 年) 推動資安防護計畫之依據，作為貫通政府、產業與民眾資安防護之價值樞紐，爰透過宏觀的資安科技發展趨勢分析，進行資安整體性規劃，期透過資安防護資源之投入與執行，提升我國資安產業競爭力，作為資安防護與產業創新的關鍵推手。本方案每個目標有多個對應執行策略，而每個執行策略有多個對應行動方案。(詳如圖 9)

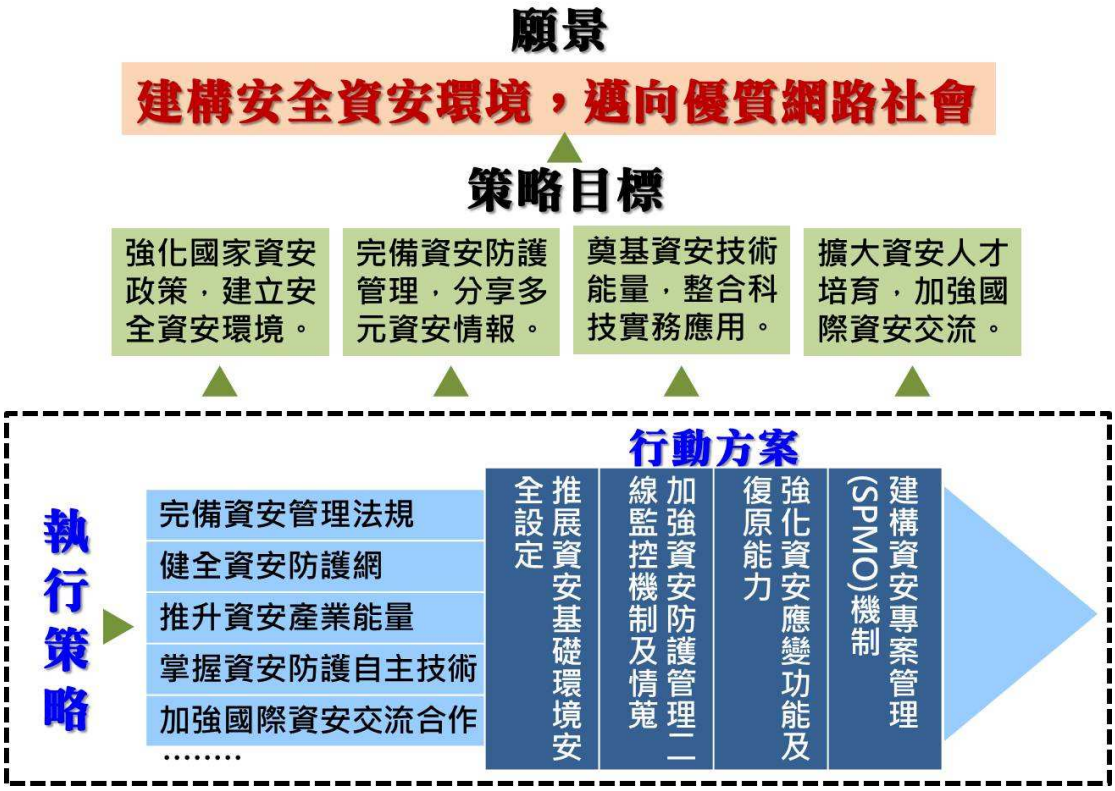


圖9、執行策略與行動方案圖

本方案將透過「推展資安基礎環境安全設定」、「加強資安防護管理二線監控機制及情蒐」、「強化資安應變功能及復原能力」及「建構資安專案管理(SPMO)機制」等行動方案，達成「強化國家資安政策，建立安全資安環境」、「完備資安防護管理，分享多元資安情報」、「奠基資安技術能量，整合科技實務應用」及「擴大資安人才培育，加強國際資安交流」4 大策略目標。

此外，本方案內涵可從「需求端」、「供應端」、及「基礎環境」3 個面向加以考量。(詳圖 10)

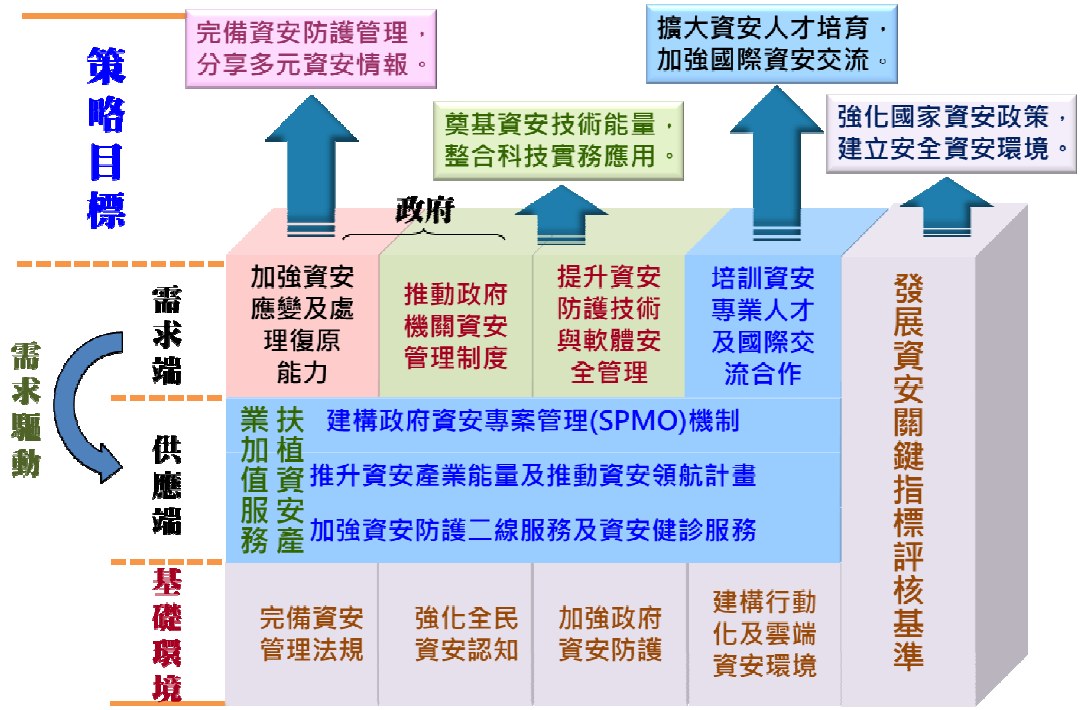


圖10、發展藍圖

「需求端」包含政府、CI、企業三個主體，分別透過加強資安應變及處理復原能力、推動政府機關資安管理制度、提升資安防護技術與軟體安全管理、培訓資安專業人才及國際交流合作等措施，預期可達成強化政府整體應變及處理能力、提供安心可信賴的資安服務、提升資安產業競爭力等目標。

有關提升優質化資安產業競爭力，還需要「供應端」的支持，透過建構資安服務產業發展環境，包含技術、人才、共同契約等，藉由資安專案管理(SPMO)機制，趨動服務創新，進而發展資安產業加值服務。

基礎環境面，包含完備資安管理法規、強化全民資安認知、加強政府資安防護、建構行動化及雲端資安環境等，分別設計相對應的行動方案，以達「邁向優質網路社會」的目標。

第五章　重要執行策略與行動方案

為使各項資安工作能順利推展並落實，本方案分別依據 4 大策略目標，規劃 20 項執行策略及 52 個行動方案 (如表 2)，分工係依各行動方案之性質分由行政院各相關部會及各機關負責辦理。

表 2　重要執行策略與行動方案（分工）

目標	執行策略	行動方案	主辦單位	協辦單位
目標一：強化國家資安政策，建立安全資安環境。	1.1.研訂資安相關準據	1.1.1.研訂資安政策	資通安全辦公室	研考會
		1.1.2.增修資安規範、指引、標準及手冊	資通安全辦公室、經濟部	研考會
	1.2.完備資安管理法規	1.2.1.研議資安管理相關法規	資通安全辦公室	法務部、 各主管機關
		1.2.2. 推動個資資安防護機制	資通安全辦公室 經濟部	行政院資訊處、法務部、各機關
	1.3.推動功能性資安組織	1.3.1.推動資安合理人力及預算	資通安全辦公室	研考會、人事總處、主計總處、各機關
		1.3.2.建構政府資安專案管理(SPMO)機制	資通安全辦公室	科技會報辦公室
		1.3.3.推動技服中心行政法人化	資通安全辦公室	人事總處
	1.4.建構資安關鍵指標	1.4.1.研議整體資安防護指標	資通安全辦公室	國安會、國安局、國防部
		1.4.2.研訂資安警示等級及燈號	資通安全辦公室	國安會、國安局、國防部
	1.5.推升資安產業能量	1.5.1.扶植資安產業加值服務	經濟部、通傳會	科技會報辦公室
		1.5.2.推動重點產業資安躍進計畫	經濟部	
目標二：完備資安防護管理，分享多元資安情報。	2.1. 賡續推動資安治理與分類分級	2.1.1.推動建立資安治理架構	資通安全辦公室、各機關	
		2.1.2.落實資訊系統分類分級及防護規定	資通安全辦公室、各主管機關	
	2.2.健全資安防護網	2.2.1.加強各機關資安防護縱深	資通安全辦公室、各機關	國安局
		2.2.2.擴展國內、外資安聯防	資通安全辦公室	外交部、國防部、各機關
		2.2.3.加強資安事故緊急應變及處理復原能力	資通安全辦公室、各機關	

目標	執行策略	行動方案	主辦單位	協辦單位
		2.2.4.研訂關鍵資訊基礎設施資安防護基準	資通安全辦公室	國土安全辦公室、各機關
		2.2.5.強化網路內容安全管理機制	通傳會	內政部、教育部、經濟部、文化部、衛生福利部、資通安全辦公室
		2.2.6.落實資安攻防演練	資通安全辦公室	國土安全辦公室
	2.3.落實資安管理與稽核制度	2.3.1.推動政府資安管理制度	資通安全辦公室	各機關
		2.3.2.推展資安基礎環境安全設定	資通安全辦公室	各機關
		2.3.3.落實資安稽核作業	各機關、資通安全辦公室	國安局、行政院資訊處
		2.3.4.落實資安健診作業	資通安全辦公室、各機關	
	2.4 掌握資安威脅全貌	2.4.1.強化資安二線監控機制	資通安全辦公室	各機關
		2.4.2.建構鉅量資料分析能量	資通安全辦公室	
	2.5.蒐集與分享資安情報	2.5.1.強化資安資訊分享及分析	資通安全辦公室	各機關
		2.5.2.強化資通安全威脅情蒐	資通安全辦公室	各機關
		2.5.3.蒐集及發布重要資安情報	資通安全辦公室	各機關
目標三：奠基資安技術能量，整合科技實務應用。	3.1.掌握資安防護自主技術	3.1.1.建構資安防護技術研究能量	國科會、經濟部、國防部	資通安全辦公室
		3.1.2.推動資安防護技術整合應用	經濟部、資通安全辦公室	國安局
	3.2.加強網路犯罪偵查能量	3.2.1.強化網路犯罪偵查科技應用	內政部、法務部	資通安全辦公室
		3.2.2.建置網路犯罪偵查整合性「知識庫」	內政部、法務部	資通安全辦公室
	3.3.建立數位證據保全及鑑識能量	3.3.1.完善數位證據保全及相關標準作業程序	法務部、內政部	資通安全辦公室
		3.3.2.研議建立數位鑑識實驗室驗證制度	法務部、內政部	資通安全辦公室
	3.4. 強化軟體安全管理	3.4.1.建置國家軟體資產控管機制	資通安全辦公室	各機關
		3.4.2.推動「安全軟體發展生命週期（SSDLC）」	資通安全辦公室	科技會報辦公室、各機關
	3.5.建構政府行動化安全機制	3.5.1.建構政府行動軟體(APP)安全檢測機制	資通安全辦公室	研考會
		3.5.2.規劃政府行動化安全防護機制	資通安全辦公室	研考會
		3.5.3.提升政府無線網路安全措施	資通安全辦公室	研考會
目標四：擴大資安人才培	4.1.強化全民資安認知	4.1.1.辦理資安推廣活動	教育部、資通安全辦公室	各機關
		4.1.2.推廣全民資安認知及個資保	資通安全辦公室	各機關

目標	執行策略	行動方案	主辦單位	協辦單位
育，加強國際資安交流。		護		
	4.2.培訓資安專業人才	4.2.1.培訓資安種子師資及專業人才	資通安全辦公室、教育部、內政部、法務部	
		4.2.2.推動資安專業訓練認證機制	資通安全辦公室	教育部
	4.3.建立多元資安學習管道	4.3.1.資安納入各級學校課程或學程	教育部	資通安全辦公室
		4.3.2.規劃多元資安學習管道	教育部、資通安全辦公室	
	4.4.推動公務人員資安職能訓練與評量	4.4.1.規劃各類職務應具備資安知識及技能	資通安全辦公室	
		4.4.2.訂定職能課程開發與評量相關規範	資通安全辦公室	
		4.4.3.發展資安職能數位及實體課程教材	資通安全辦公室	
		4.4.4.建立資安職能評量制度	資通安全辦公室	
	4.5.加強國內、外資安交流合作	4.5.1.參與國內、外資安組織相關會議及活動	資通安全辦公室	外交部
		4.5.2.參與國際性網路犯罪偵防相關活動	法務部、內政部	資通安全辦公室
		4.5.3.加強國際資安學術發表	國科會	資通安全辦公室、教育部

第六章　推動組織、資源需求與計畫管理

壹、 推動組織

依據「行政院國家資通安全會報設置要點」，行政院資通安全辦公室為資通訊安全相關政策統籌規劃及推動單位，將負責本方案之整體規劃及推動。

貳、執行規劃

本方案各行動方案之執行要點與績效指標(詳附錄 2)，細部執行規劃由各主辦機關依政府施政計畫編審相關作業規定訂定年度計畫。

參、預算來源與執行

各主辦機關所提年度計畫之預算來源由各機關自行調配支應或另循相關行政程序籌措。年度計畫之執行應每年進行檢討，並配合預算審議與綜合評估結果等做必要之修正。

肆、相關行動方案之管考

本方案之執行要點與績效指標，由行政院資通安全辦公室運用既有督導機制，落實執行管考。

伍、方案核定與修訂

一、 本方案經行政院核定後實施，修正時亦同。

二、 本方案應於 4 年施行期滿前，整體檢討修訂未來 4 年發展方案，並視需要每年滾動式檢討發展方案及相關推動計畫。

附錄

附錄1.行政院國家資通安全會報設置要點

附錄2.行動方案執行要點與績效指標說明表

附錄1. 行政院國家資通安全會報設置要點

行政院台 90 經字第 069579-1 號函訂定發布
中華民國 92 年 3 月 17 日行政院核定修正
中華民國 94 年 4 月 18 日行政院院台科字第 94008356 號函修正發布
中華民國 95 年 9 月 14 日行政院院台經字第 0950091248 號函修正發布
中華民國 97 年 7 月 29 日行政院院台經字第 0970088180 號函修正發布
中華民國 98 年 12 月 31 日行政院院台經字第 0980099344 號函修正發布
中華民國 100 年 3 月 7 日行政院院臺經字第 1000093156 號函修正發布
中華民國 102 年 1 月 4 日行政院院臺護揆字第 1010155308 號函修正發布

一、行政院（以下簡稱本院）為積極推動國家資訊通信安全政策，加速建構國家資訊通信安全環境，提升國家競爭力，特設國家資通安全會報（以下簡稱本會報）

二、本會報任務如下：

（一）國家資訊通信安全政策之諮詢審議。

（二）國家資訊通信安全通報應變機制之諮詢審議。

（三）國家資訊通信安全重大計畫之諮詢審議。

（四）跨部會資訊通信安全事務之協調及督導。

（五）其他本院交辦國家資訊通信安全相關事項。

三、本會報置召集人一人，由本院院長指派之政務委員兼任；協同召集人一人，由國家安全會議諮詢委員兼任；委員十八人至三十人，除召集人及協同召集人為當然委員外，其餘委員，由本院院長就推動資通安全有關之機關、直轄市政府副首長及學者、專家派（聘）兼之。

四、本會報之幕僚作業，由本院資通安全辦公室辦理。

五、本會報下設網際防護及網際犯罪偵防等二體系，其主辦機關（單位）及任務如下：

(一) 網際防護體系：由本院資通安全辦公室主辦，負責整合資安防護資源，推動資安相關政策，並設下列各組，其主辦機關（單位）及其任務如下：

1. 標準規範組：由經濟部主辦，負責發展資安產品與管理系統之認驗證標準及體系，推動資通安全之技術規範及管制，發展、維護政府機關資安作業規範及參考指引。

2. 稽核服務組：由本院資訊處主辦，負責推動落實資安稽核制度，協助各機關強化資安防護工作之完整性及有效性，並透過持續改善以降低資安風險。

3. 認知教育及人才培育組：由教育部主辦，負責推動資安基礎教育，強化教育體系資通安全，提升全民資安素養，提供資安資訊服務，建立資安人才培育體系。

4. 政府資通安全組：由本院資通安全辦公室主辦，負責規劃、推動政府各項便民資通訊應用服務之安全機制，輔導政府機關資安技術服務、資安防護及應變，統合政府機關資安人力充實及運用。

(二) 網際犯罪偵防體系：由法務部及內政部共同主辦，負責防範網路犯罪、維護民眾隱私、建立資通訊基礎設施安全等工作，並設下列各組，其主辦機關及任務如下：

1. 個資保護及法制推動組：由法務部主辦，負責檢討修正維護民眾隱私及防制網路犯罪相關法令規章，建立安心信賴之資通訊法制環境。

2. 防治網路犯罪組：由內政部主辦，負責網路犯罪查察、電腦犯罪防治等事件工作。

3. 資通訊環境安全組：由國家通訊傳播委員會主辦，負責促進網路內容安全，防制網路犯罪，強化關鍵工業控制系統安全，建立資通訊基礎設施安全信賴機制。

為掌握資安技術發展趨勢，充實資安作業能量，本會報得設資通安全技術交流小組。

六、前點各組得置召集人一人，由主辦機關之委員擔任之，並依需要訂定各組作業規範。

資通安全技術交流小組置召集人一人；副召集人一人至二人，由本會報召集人指派適當層級人員兼任。委員十人至十五人，除召集人及副召集人為當然委員外，其餘委員，由本會報召集人就推

動資通安全有關之機關及學者、專家派（聘）兼之。

七、本會報原則上每半年召開會議一次；必要時，得召開臨時會議，均由召集人主持。

八、本會報委員及各組召集人，均為無給職。

附錄2. 行動方案執行要點與績效指標說明

行動方案	執行要點	績效指標	主（協）辦單位
1.1.1.研訂資安政策	1. 比較研析各國資安重大政策計畫。 2. 檢視國內、外部資安環境及資安資源(包含資安組織特性、資安科技及產業能量等)。 3. 擬訂資安政策白皮書，定期檢討發展方案及推動計畫。	1. 每年召開資安策略研討會，提出資安建言。 2. 每年進行資安科技及產業能量調查，作為資安政策擬訂參據。 3. 104 年完成資安政策白皮書。 4. 每年滾動式檢討發展方案及推動計畫。	資通安全辦公室(研考會)
1.1.2.增修資安規範、指引、標準及手冊	1. 研析國際資安規範、指引、標準及手冊訂定發展趨勢。 2. 全面檢討資安相關規範、指引、標準及手冊適宜性。 3. 檢討現行資安分類、分級制度。 4. 訂定我國各級政府機關資安管理基本要求。 5. 研訂資安規範、指引、標準及手冊整體發展藍圖。	資通安全辦公室： 1. 102 年完成資安管理相關規範、指引、標準及手冊之盤點。 2. 103 年完成資安管理要點及相關規範之修訂。 3. 103 年完成「政府機關(構)資安責任等級分級作業施行計畫」及「各機關資安管理基本要求」之修訂。 4. 103 年完成資安規範、指引、標準及手冊整體發展藍圖之研訂。 5. 104 年起每年至少完成 3 本資安相關指引或手冊之增刪修訂及推廣運用。 經濟部： 配合國際資安標準更新，每年檢討更新或新增我國資安國家標準。	資通安全辦公室、經濟部 (研考會)
1.2.1.研議資安管理相關法規	1. 比較分析各國資安管理法規、位階及重要立法精神。 2. 盤點我國資安管理相關法規。 3. 研議制定資安專法。	1. 102 年完成資安相關法規之盤點。 2. 103 年完成資安專法條文之研議。	資通安全辦公室(法務部、 各主管機關)
1.2.2. 推動個資資安防護機制	1. 督促各級政府機關善用資安技術保護個資。 2. 每年檢視各級政府機關個資資安防護機制。 3. 協助企業建立個資保護與管理制度。	資通安全辦公室： 每年配合年度稽核，檢視各政府機關個資資安防護機制。 經濟部： 協助企業導入個資保護與管理制度，訓練個資管理專業人員並驗證企業內部隱私權管理能力。	資通安全辦公室 經濟部(行政院資訊處、法務部、各機關)

行動方案	執行要點	績效指標	主（協）辦單位
1.3.1.推動資安合理人力及預算	1. 評估各機關資安合理人力及任用機制。 2. 逐年推動資安預算單獨編列及調整適當比率。	1.103 年完成各機關資安合理人力評估作業。 2.104 年完成資安人力任用機制之評估。 3.每年檢討適當資安預算之比率及編列方式之合理性。	資通安全辦公室(研考會、人事總處、主計總處、各機關)
1.3.2.建構政府資安專案管理(SPMO)機制	1. 建構政府機關資安專案管理(SPMO)機制，提供資安技術與管理諮詢服務。 2. 評估供應商資安服務品質、等級與合理之計價基準。 3. 檢討資安服務納入共同供應契約。 4. 配合導入民間優質資安能量，逐步引導政府機關完成資安監控服務委外作業。	1. 102 年完成政府機關資安服務品項，制定品項規範及服務水準協議。 2. 102 年完成資安服務需求說明書(RFP)範本。 3. 102 年資安服務納入共同供應契約。 4. 103 年起每年檢討共同供應契約資安服務項目。 5. 每年辦理資安服務廠商評鑑。 6. 協助政府機關資安監控服務委外作業。	資通安全辦公室(科技會報辦公室)
1.3.3.推動技服中心行政法人化	1. 進行「技服中心」行政法人化後功能內容、組織型態及營運模式規劃。 2. 協助進行技服中心行政法人化相關立法作業。	1. 102 年完成「技服中心」行政法人化相關規劃。 2. 103 年由監督機關成立籌備小組及推動立法程序。	資通安全辦公室(人事總處)
1.4.1.研議整體資安防護指標	1. 發展與國際資安指標接軌之關鍵指標。 2. 調查與發布資安關鍵指標。	1. 103 年完成資安關鍵指標之研議。 2. 104 年起每年發布資安關鍵指標。	資通安全辦公室(國安會、國安局、國防部)
1.4.2.研訂資安警示等級及燈號	建構資安警示等級及燈號。	1. 103 年完成資安警示等級及燈號規範，並逐年檢視。 2. 104 年完成資安燈號試編。	資通安全辦公室(國安會、國安局、國防部)
1.5.1.扶植資安產業加值服務	1. 提升資安產業自主技術能量。 2. 推動資通設備安全驗證作業。	經濟部： 輔導資安業者開發符合新興應用(如個資安全、鉅資分析、雲端應用等)之資安產品或服務每年 2 案。 通傳會： 1. 積極參與國際認驗證組織與相互承認體系相關研討會，以掌握國際脈動。 2. 每 2 年檢討增加資通設備安全檢測之項目。	經濟部、通傳會(科技會報辦公室)

行動方案	執行要點	績效指標	主（協）辦單位
1.5.2.推動重點產業資安躍進計畫	1. 掌握商業服務重點產業(指批發零售及電子商務產業)個資管理與資安應用狀況。 2. 研訂商業服務重點產業個資管理與資安法令規範、管制措施或指導方針。 3. 規劃推動產業輔導措施，強化商業服務重點產業個資管理與資安效能。	1. 每年進行商業服務重點產業個資管理與資安應用調查。 2. 103 年完成商業服務重點產業個資管理與資安法令規範、管制措施產業需求盤點。 3. 103 至 105 年逐年研訂商業服務重點產業個資管理與資安法令規範、管制措施或指導方針每年至少 1 案。 4. 依產業調查結果、法令規範與相關措施、方針研議情形，每年滾動式規劃執行配套輔導措施。	經濟部
2.1.1.推動建立資安治理架構	1. 運用已開發之資安參考指引，規劃建立政府機關資安治理架構。 2. 評估各機關資安治理成熟度。 3. 每年檢討資安治理成熟度提升比率（導入機關自訂）。	資通安全辦公室： 103 年開發資安治理評核系統(檢核表)，協助政府機關進行資安治理評核。 各機關： 104 年起各機關每兩年進行一次資安治理成熟度評估。	資通安全辦公室、各機關
2.1.2.落實資訊系統分類分級及防護規定	1. 檢討政府機關資訊系統之分類分級作法。 2. 各機關進行資訊系統分類分級，落實基本資安防護要求。	資通安全辦公室： 1. 103 年完成資訊系統分類分級及防護規定之檢討。 2. 104 年起依資訊系統鑑別之等級(高、中、普) ，配合年度稽核或以抽檢方式檢視各機關基本資安防護情形。 各主管機關： 1. 103 年起各主管機關推動辦理資訊系統分類分級與鑑別作業。 2. 104 年起由各主管機關推動辦理資訊系統需逐步達到安全等級基本資安防護之要求。	資通安全辦公室、各主管機關
2.2.1.加強各機關資安防護縱深	1. 檢討整合內、外部網路監控系統部署情形。 2. 加強政府機關資安防護部署與 GSN 骨幹防護縱深。 3. 強化政府機關資料安全防護，積極部署保密裝備。	資通安全辦公室： 1. 103 年起每年實施政府機關資安防護部署計畫之調整。 2. 每年至少完成 10 個政府機關網路與資訊系統滲透測試。 各機關： 每年檢討政府機關保密裝備之部	資通安全辦公室、各機關(國安局)

行動方案	執行要點	績效指標	主（協）辦單位
		署，應使用或加裝密碼主管機關核發獲認可之通資訊保密裝備。	
2.2.2. 擴展國內、外資安聯防	1. 配合國內、外資安聯防交流議題，積極爭取參加相關活動與會議。 2. 與國內、外資安相關組織建立合作交流窗口，交換資安威脅情報、網路犯罪趨勢等。 3. 與國際資安相關組織建立資安聯防互惠機制。 4. 推動政府機關資安防護共用機制，落實資安聯防有效性」。	1. 每年參與國內、外重要資安聯防議題之活動或相關會議。 2. 擴展與國內、外資安組織或業者建立聯防合作關係與聯絡窗口。 3. 爭取國內、外資安聯防合作專案，建立互惠機制。	資通安全辦公室(外交部、國防部、各機關)
2.2.3. 加強資安事故緊急應變及處理復原能力	1. 檢視我國整體資安事故緊急應變機制。 2. 調整資安事故緊急應變作業標準程序（含事故偵測、識別及分析與回應等）。 3. 研析資安事故發生原因，強化資安事故辨識及處理復原能力。 4. 研議異地備援建議方案。	資通安全辦公室： 1. 103 年完成資安事故緊急應變作業標準程序之修訂。 2. 103 年完成異地備援建議方案。 3. 每年結合年度演練遴選重要資通訊系統實施緊急應變及處理復原能力之檢測。 各機關： 103 年完成資安事故緊急應變及處理復原能力之檢討。	資通安全辦公室、各機關
2.2.4. 研訂關鍵資訊基礎設施資安防護基準	1. 檢視「關鍵資訊基礎設施」資安防護作為。 2. 研訂「關鍵資訊基礎設施」資安防護基準。 3. 演練「關鍵資訊基礎設施」資安防護計畫有效性 。	1. 103 年完成「關鍵資訊基礎設施」資安防護相關計畫之檢視。 2. 104 年完成「關鍵資訊基礎設施」資安防護基準之研訂。 3. 105 年起每年擇「關鍵資訊基礎設施」辦理資安防護計畫演練。	資通安全辦公室(國土安全辦公室、各機關)
2.2.5. 強化網路內容安全管理機制	1. 強化網路內容申訴及通報單一窗口(WIN 網路單 e 窗口)之執行及運作能力。 2. 強化單一窗口回復民眾網路內容安全問題能力及時效。 3. 建構網路內容安全事件通報相關權責單位之快速處理機制。 4. 執行內容防護機構計畫，辦理網路素養宣導，招募網路志工活動，以保護兒童及少年安全上網。	1. WIN 網路單 e 窗口受理案件須於 7 日內回覆民眾。 2. 民眾對於 WIN 網路單 e 窗口回覆滿意度為 60%以上。 3. 建立並更新相關權責單位或網路平臺服務提供者之緊急聯絡窗口名單。 4. 每年辦理 2 場次宣導網路安全觀念活動 。 5. 我國與合作國家間垃圾郵件濫發源資料之年度交換筆數達	通傳會（內政部、教育部、經濟部、文化部、衛生福利部、資通安全辦公室）

行動方案	執行要點	績效指標	主（協）辦單位
	5. 配合資安事件通報及應變處理作業，督促業者加強管理垃圾郵件，維護民眾網路使用環境。	30 萬筆以上。	
2.2.6. 落實資安攻防演練	1. 辦理政府機關資安演練作業。 2. 規劃資安情境演練與實兵演練。	1. 配合年度演練辦理政府機關資安攻防演練作業。 2. 每年召開資安攻防技術研討會。	資通安全辦公室(國土安全辦公室)
2.3.1. 推動政府資安管理制度	1. 研提與國際標準接軌之政府專屬資安管理標準。 2. 規劃建立政府專屬資安管理標準認驗證體系。 3. 推動政府機關選定核心業務，建置資安管理系統，並視需要以全機關納入驗證範圍為目標。	1. 103 年完成政府專屬資安管理標準之訂定。 2. 104 年完成政府專屬資安管理標準認驗證體系之規劃。	資通安全辦公室(各機關)
2.3.2. 推展資安基礎環境安全設定	1. 持續規劃不同系統政府組態基準設定。 2. 針對服務目錄網域環境與單機作業環境，分別設計其組態部署機制。 3. 針對政府組態基準辦理教育訓練。	1. 每年至少完成 1 項資通訊設備政府組態基準。 2. 103 年完成自動化組態基準設定(SCAP)檢測系統之開發，並逐年增加檢測項目。 3. 每年辦理政府組態基準教育訓練。	資通安全辦公室(各機關)
2.3.3. 落實資安稽核作業	1. 各機關應定期進行資安內部稽核作業。 2. 選定政府重要機關實施資安外部稽核，評估受稽單位落實資安管理及保密設備部署程度，且進行持續改善。 3. 依據每年稽核作業成果，彙整稽核缺失資料。	各機關： 1. A 級機關每年至少辦理 2 次資安內稽，B 級機關每 2 年至少擇期辦理 1 次資安內稽，C、D 級由各主管機關規定。 2. 保密設備部署每年至少清點 2 次，並依現行規定彙報及備查。 資通安全辦公室： 每年至少選定 20 個重要機關辦理資安外部稽核，並彙整稽核缺失資料。	各機關、資通安全辦公室(國安局、行政院資訊處)
2.3.4. 落實資安健診作業	1. 各機關定期進行資安健診及追蹤改善。 2. 加強資安健診服務檢視項目及能量。	資通安全辦公室： 1. 依據各機關資安健診作業報告與資料，每年檢視資安健診項目及其合宜性。 2. 104 年完成資安健診「樣態資	資通安全辦公室、各機關

行動方案	執行要點	績效指標	主（協）辦單位
		料庫」之建構。 各機關： 1. 103 年起 A 級機關每年至少辦理 1 次資安健診，B 級機關每 2 年至少辦理 1 次資安健診，C、D 級由各主管機關規定。 2. 各機關依據資安健診作業時程，提供資安健診報告與資料。	
2.4.1. 強化資安二線監控機制	1. 規劃建置 SOC 二線監控服務架構與平台。 2. 建立 SOC 二線監控服務範圍，增加與民間資安業者情資交換與服務機制。 3. 加強 SOC 二線監控服務能量，增進情資研析技術，提升資安監控服務水準。	1. 103 年完成 SOC 二線監控服務平台之建置。 2. 103 年起與民間資安業者進行資安情資交換。 3. 每年培訓 SOC 二線監控專業人才，提升資安情資研析能力。	資通安全辦公室(各機關)
2.4.2. 建構鉅量資料分析能量	1. 研析鉅量資料流記錄、保存及分析探勘方法。 2. 善用鉅量資料關聯性，加強資安威脅整合分析運算能力。 3. 運用鉅量資料儲存與資料分流技術，強化資料處理速度與比對深度。	1. 103 年結合虛擬及雲端架構環境，完成鉅量資料運算分析架構之規劃。 2. 104 年完成鉅量資料分析平台之建置。	資通安全辦公室
2.5.1. 強化資安資訊分享及分析	1. 與各界進行情報分享、事故處理及相關資安技術合作。 2. 建立資安情報跨領域合作機制與國際資安組織進行資安交流與經驗分享。 3. 提供政府機關資安諮詢及技術服務，並發布資安訊息 4. 加強資安技術交流平台運作。	3. 持續維運政府資安資訊分享與分析中心（G-ISAC）。 1. 透過 G-ISAC 機制發布資安情資，每年至少 500 則 2. 每日透過 G-ISAC 機制分享惡意中繼站資訊，提升資安防護廣度。 3. 每季召開 G-ISAC 會議，進行情報分享與經驗交流 4. 每季召開 1 次資安技術交流會議。	資通安全辦公室(各機關)
2.5.2. 強化資通安全威脅情蒐	1. 加強網路安全威脅情蒐能量，針對殭屍網路追蹤與垃圾郵件進行分析。 2. 進行國內網路攻擊資訊情蒐作業。 3. 與國際資安組織建立資安威脅情報交換管道。	1. 與國內、外資安相關組織或學研單位合作，每年擴增網路情蒐點，增加情蒐廣度。 2. 即時更新惡意中繼站域名與網路位址(IP)阻擋列表資料。	資通安全辦公室(各機關)

行動方案	執行要點	績效指標	主（協）辦單位
2.5.3. 蒐集及發布重要資安情報	1. 研究資安威脅蒐集與分析自動檢測核心技術，建立自動蒐集分析機制，降低資安可能危害。 2. 維運政府資安警訊發布服務管理系統，將各類警訊與發生之事件類型進行統計與分析。 3. 蒐集與發布國內、外重要資安情報資訊(包含攻擊趨勢與手法、系統弱點與漏洞等)。	1. 每月彙整資安相關情資，並提出情資報告。 2. 透過網站、電子報或郵件等管道，每年至少發布 200 則資安訊息。	資通安全辦公室(各機關)
3.1.1. 建構資安防護技術研究能量	1. 運用國家科技資源，創新資安防護技術及人才培育。 2. 創新技術佈局建立關鍵智財保護機制，強化新興資安自主技術競爭力。 3. 參與資安治理國際標準驗證，提升技術成果涵蓋度及成熟度。 4. 技術佈局資安檢測與威脅防護，建立關鍵智財保護，強化資安跨領域自主技術競爭力。 5. 產研合作，發展企業應用之行動安全技術。	國科會： 1. 每年投入適當（或穩定）之經費比率於資安領域。 2. 運用國家科研資源，加強培育資安專業碩、博士。 經濟部： 1. 102 至 103 年起針對資安治理、資料防護及智慧終端安全領域，每年申請至少 2 件專利技術。 2. 103 年資安治理技術研發與國際接軌通過國際認證。 3. 103 至 104 年針對資安檢測與威脅防護領域，每年申請至少 2 件專利技術。 4. 104 年針對行動終端導入企業應用安全議題，產研共同合作，發展 BYOD 企業應用之行動安全解決方案。 國防部： 1. 培育國防資安防護科技研發人才。 2. 參與產、官、學、研合作資安防護技術研發專案。	國科會、經濟部、國防部(資通安全辦公室)
3.1.2. 推動資安防護技術整合應用	1. 協助資安業者切入新興個資保護、資安治理及智慧應用等新興資安需求市場。 2. 推動智慧應用資安信任服務能量，開創新興資安加值服務市場機會(提供共通性之資安設備檢測服務)。	經濟部 ： 1. 發展個資加值服務至少 1 案。 2. 推動新興資安需求重點應用至少 1 案。 3. 104 年完成聯網設備資安檢測服務實驗室之建置，提供至少 5 種聯網終端設備資安檢測。	經濟部、資通安全辦公室(國安局)

行動方案	執行要點	績效指標	主（協）辦單位
	3. 研提資安網路及端點安全(Endpoint)整合性應用技術解決方案，安全機制涉及密碼技術應符合安全鑑測標準。	資通安全辦公室： 1. 103 年完成資安端點安全(Endpoint) 技術解決建議方案。 2. 104 年完成網路端安全技術解決建議方案。 3. 前述資安端點(Endpoint)及網路端安全技術解決方案，若涉及機密部分應採用密碼主管機關核發或認可之通資訊保密裝備。	
3.2.1. 強化網路犯罪偵查科技應用	1. 研發及推廣高科技犯罪偵查工具。 2. 辦理相關教育訓練，提升科技犯罪偵查能量。 3. 增加產官學合作，研擬新興犯罪偵查技術強化網路資料探勘分析模型。	內政部： 1. 每年辦理 1 次「全國性科技犯罪偵查人員講習」。 2. 每年辦理 2 次「全國刑事人員講習班」編排網路犯罪偵查相關課程。 法務部： 每年辦理網路犯罪偵查教育訓練。	內政部、法務部(資通安全辦公室)
3.2.2. 建置網路犯罪偵查整合性「知識庫」	1. 建置網路犯罪偵查整合性「知識庫」，以有效掌握犯罪動向。 2. 加強與各地科技偵查單位之連結，建立溝通與犯罪情報分享平台。 3. 持續充實「網路犯罪資料庫」完整性。	內政部： 1. 103 年完成建置「科技情資匯流平台」。 2. 持續強化「強化網路秩序與詐欺偵防能力系統」分析模型。 法務部： 持續充實網路犯罪手法及違反法條之態樣資料庫。	內政部、法務部(資通安全辦公室)
3.3.1. 完善數位證據保全及相關標準作業程序	1. 訂定符合證據能力的數位證據保全標準作業程序。 2. 推動所屬各機關依標準作業程序進行數位證據保全。	法務部： 1. 103 年制訂數位證據保全標準作業程序規範 (參 ISO 27037)。 2. 104 年起落實數位證據保全標準作業程序執行情形。 內政部： 1. 103 年訂定現場數位證物蒐證手冊，以強化數位證據保全。 2. 103 年起逐步辦理現場數位證物蒐證人員之認證。	法務部、內政部(資通安全辦公室)

行動方案	執行要點	績效指標	主（協）辦單位
3.3.2.研議建立數位鑑識實驗室驗證制度	1. 評估國內數位鑑識實驗室運作現況。 2. 推動國內數位鑑識實驗室驗證制度。	法務部： 1. 103 年取得實驗室認證(ISO/IEC 17025 實驗室認證規範及鑑識科學實驗室技術規範)。 2. 104 年評估導入數位鑑識實驗室認證模式(如 ASCLD / LAB)。 內政部： 1. 逐年強化數位鑑識實驗室品質管理及鑑識作業流程。 2. 104 年起逐步推動實驗室認證及數位鑑識人員之認證。	法務部、內政部(資通安全辦公室)
3.4.1.建置國家軟體資產控管機制	1. 建置國家軟體資產資料庫。 2. 建立軟體資產安全品質管控機制。 3. 建立軟體資產檢測及安全風險評量、分析機制。 4. 建置政府機關及我國軟體開發業者軟體資產威脅情報查詢及通報平台。	1. 103 年完成國家軟體資產資料庫及軟體資產安全品質管控機制。 2. 104 年起定期提供軟體更新及漏洞資訊。 3. 104 年起各機關逐步進行軟體資產風險評量及分析作業。	資通安全辦公室(各機關)
3.4.2.推動「安全軟體發展生命週期（SSDLC）」	1. 規劃建立軟體安全測試流程與品質保證機制。 2. 推動各級政府機關於採購案 RFP 中納入安全軟體要求項目。 3. 辦理「安全軟體發展生命週期（SSDLC)」教育訓練。	1. 103 年完成安全軟體發展流程、安全測試指引及其相關二階文件之指導文件。 2. 104 年起每年依據安全指引及指導文件，輔以實務上常使用之相關工具辦理教育訓練。	資通安全辦公室(科技會報辦公室、各機關)
3.5.1.建構政府行動軟體(APP) 安全檢測機制	1. 建立政府行動軟體安全上線安全檢測機制。 2. 建置政府行動軟體資產資料庫及行動軟體資產安全更新管控機制。 3. 蒐集行動軟體威脅情報，並通知政府機關及相關業者。	1. 103 年完成政府檢測行動軟體上線安全檢測機制之建立。 2. 104 年完成政府行動軟體資產資料庫之建置，定期發布行動軟體威脅情報。 3. 105 年起進行政府行動軟體安全檢測作業。	資通安全辦公室(研考會)
3.5.2.規劃政府行動化安全防護機制	1. 訂定行動化安全防護管理規範。 2. 規劃建立行動裝置及可攜式媒體安全防護管理機制。 3. 研析行動化資料保全或裝置遭竊風險。	1. 103 年完成行動化安全防護管理規範之訂定。 2. 104 年起落實行動裝置及可攜式媒體管理機制。	資通安全辦公室(研考會)

行動方案	執行要點	績效指標	主（協）辦單位
3.5.3.提升政府無線網路安全措施	1. 規劃無線網路新型態身份認證及可集中管理的安全性架構。 2. 研究無線網路設備之組態安全設定及管理。	1. 103 年完成身份認證及可集中管理的安全性架構規劃。 2. 104 年完成無線網路組態安全設定規範及安全指引。	資通安全辦公室(研考會)
4.1.1.辦理資安推廣活動	1. 辦理大專院校資安技能、動畫、海報及金句競賽等活動。 2. 利用網路、電子及平面媒體，結合資安廠商、公協會及入口網站業者辦理資安推廣活動。	1. 每年辦理各類資安推廣活動。 2. 每年辦理各類資安競賽活動。	教育部、資通安全辦公室(各機關)
4.1.2.推廣全民資安認知及個資保護	加強宣導，提升民眾對資安認知及個資保護程度。	1. 辦理資安素養認知宣導推廣活動，至少 1 萬人次以上參與。 2. 製作資安及個資保護廣宣資料，提供全民資安認知學習使用。	資通安全辦公室(各機關)
4.2.1.培訓資安種子師資及專業人才	1. 規劃資安種子師資養成體系。 2. 培育資安專業人才登錄及訓用。	資通安全辦公室： 每年培訓政府資安專業人才 80 名。 教育部： 1. 103 年完成資安種子師資養成體系規劃。 2. 104 年起每年培訓資安種子師資 50 名。 內政部、法務部： 每年培育及訓用資安鑑識專業人才。	資通安全辦公室、教育部、內政部、法務部
4.2.2.推動資安專業訓練認證機制	1. 規劃建立資安專業人員能力登錄機制。 2. 規劃建立資安專業人員認證機制。	1. 103 年完成資安專業人員登錄平台建置。 2. 104 年完成資安專業人員能力認證規劃。 3. 105 年起資安專業人員經認證合格，授與資安專業證書(照)。	資通安全辦公室(教育部)
4.3.1.資安納入各級學校課程或學程	1. 鼓勵各級學校資安訓練納入通識教育。 2. 建構我國教育體系資安訓練科普課程，並提供資安先備課程及教材。 3. 落實大專院校設立資安學程及資安系所。	1. 每年辦理至少 2 場涵蓋資安人才培育議題之研討會。 2. 103 年起發展資安先備(基礎)課程教材。 3. 103 年起推動大專院校設立資安學程及資安系所至少達 20%以上。 4. 推動資安素養議題納入中小學課程。	教育部(資通安全辦公室)

行動方案	執行要點	績效指標	主（協）辦單位
4.3.2.規劃多元資安學習管道	1. 規劃資安多元(行動化、雲端、實體及數位)學習管道。 2. 推動民間擴大資安教育訓練能量。	教育部： 1. 103 年完成數位化資安課程分級、分類規劃。 2. 104 年結合資安多元學習環境，提供課程相關內容。 資通安全辦公室： 103 年完成資安多元學習管道之規劃與評估。	教育部、資通安全辦公室
4.4.1.規劃各類職務應具備資安知識及技能	1. 規劃各類職務應具備之資安知識與技能。 2. 定期檢討各類職務應具有之技能項目及專業證照。 3. 建立人員回流培訓機制。	1. 103 年完成資安專業人員類別與能力規劃。 2. 每年定期檢討各類職務應具有之技能項目及專業證照。 3. 103 年起資安專業人員回流培訓比率達 40%以上，以後每年增加 5%。	資通安全辦公室
4.4.2.訂定職能課程開發與評量相關規範	1. 訂定開發資安職能課程所依循之規範。 2. 建立執行資安職能評量之標準化作業流程。	1. 以一綱多本的原則，103 年完成課程發展所需文件、訓練課程上課天數及課程先備條件之制定。 2. 103 年完成學習評量標準與制度、評量對象通過要件、各科目評量基準。 3. 104 年完成題庫規範與評量模式。	資通安全辦公室
4.4.3.發展資安職能數位及實體課程教材	1. 檢討資安職能之訓練課程。 2. 收集國外資安職能課程資訊做為發展課程之參考。	1. 102 年起針對新興資安議題，規劃實體及數位課程。 2. 每年定期檢討與修訂已開發之訓練課程(實體及數位課程)。	資通安全辦公室
4.4.4.建立資安職能評量制度	定期針對一般人員與專業人員，建置不同程度之資安職能評量。	1. 102 年起一般人員與主管至少須通過 3 門資安數位課程評量。 2. 103 年起 A、B 級機關資訊人員與資安人員每年至少須維持一項資安專業證書(照)有效性。	資通安全辦公室
4.5.1. 參與國內、外資安組織相關會議及活動	1. 參與國內、外資安組織相關會議或活動，交流分享資安訊息與經驗。 2. 爭取國際資安會議或活動於我國召開。 3. 鼓勵國內資安組織積極參與國	1. 每年派員參與國際資安會議至少 4 次，並積極爭取主辦權或於我國召開。 2. 維護 APCERT、APWG、AVAR、FIRST 等組織會員身分，每年爭取於會議中分享我	資通安全辦公室(外交部)

行動方案	執行要點	績效指標	主（協）辦單位
	際會議或活動。 4. 積極爭取成為國際資安組織正式會員或參與會議資格。	國資安推動經驗。	
4.5.2. 參與國際性網路犯罪偵防相關活動	1. 積極爭取參加網路犯罪偵防跨國或區域聯防機制(體系)。 2. 主動參與執法專業國際會議，促進國際合作共同打擊電腦網路犯罪。	法務部： 每年定期派員參與相關國際會議或活動。 內政部： 1. 每年定期參與相關國際會議（如執法專業國際會議、高科技犯罪研討會等），加強國際組織聯繫互動。 2. 積極建立國際合作交流窗口，交換網路犯罪情資與趨勢等情報。	法務部、內政部(資通安全辦公室)
4.5.3. 加強國際資安學術發表	1. 鼓勵國內學研機構與國際知名資通安全研究機構進行資安技術議題合作研究專案。 2. 參與國際資安學術研討會並發表研究論文。	1. 每年提供國內學研機構科研資源，參與國際資安學術研討會議或活動。 2. 與國際知名資通安全研究機構進行為期 1 至 2 年資安研究議題之學術合作專案。 3. 每年選優至少 2 篇以上資安學術研究論文在國際期刊或研討會上發表。	國科會(資通安全辦公室、教育部)