國家資通訊安全發展方案

（98 年至 101 年）

行政院國家資通安全會報

中華民國98年1月

目　　次

第一章 前言 3
壹、 依據 3
貳、 緣起 3
第二章 現況分析 6
壹、 發展現況 6
貳、 現階段資安問題與挑戰 15
參、 我國之資安發展優勢、弱點、威脅和機會分析 19
第三章 願景與政策目標及發展藍圖 22
壹、 願景與政策目標 22
貳、 發展藍圖 25
第四章 重要措施與行動方案 27
第五章 推動組織、資源需求與計畫管理 30
壹、 推動組織 30
貳、 執行規劃 30
參、 預算來源與執行 30
肆、 資通訊基礎建設相關行動方案之管考 30
伍、 計畫核定與修訂 30
附錄 31
壹、 行政院國家資通安全會報設置要點 32
貳、 行政院國家資通安全會報下各單位職掌 34
參、 行動方案執行要點與績效指標說明表 36

第一章　前言

壹、 依據

一、 建立我國通資訊基礎建設安全機制計畫

中華民國 90 年 1 月 17 日行政院第 2718 次院會通過

中華民國 90 年 4 月 24 日行政院核定修正

中華民國 91 年 6 月 6 日行政院核定修正

二、 建立我國通資訊基礎建設安全機制計畫（94 年至 97 年）

中華民國 93 年 3 月 30 日行政院　核定通過

中華民國 96 年 2 月 15 日行政院　核定修正

三、 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 0940083856 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

貳、 緣起

資通訊科技發展一日千里，受到高度運算能力、網際網路高通透性的支援，全球已逐漸邁入網際網路與資訊普及的數位經濟時代，在創造新法則與新思維模式的同時，資訊也面臨了日趨嚴重與多樣的安全威脅。

我國於 83 年成立跨部會專案小組，推動「國家資訊通信基本建設」，91 年又啟動數位台灣計畫，持續落實資通訊發展方案，促進資通訊科技普及應用於基礎建設、電子化政府、生活、商務等。在公私部門通力合作下，經過多年的努力，我國的資訊化程度已居國際領先地位。96 年 3 月行政院第 3033 次會議通過 96~100 年國家資通訊發展方案，在「發展優質網路化社會」的方向之下，該方案以民眾能夠感受到資通訊科技的好處之觀點出發，期待在不久的將來，隨著「無所不在運算技術」的發展與應用趨勢，任何人在任何時間、任何地點，都可透過多種管道享受優質 e 化生活服務。然而，資訊化程度持續加深的同時，資訊運用流程中所面臨的威脅、衝擊與脆弱點亦不斷地攀升，導致資安事故發生的可能性愈來愈高。因此，各國政府莫不高度重視並積極因應。

90 年 1 月行政院通過「建立我國通資訊基礎建設安全機制計畫（90 年至 93 年，以下簡稱第 1 期機制計畫）」，成立行政院國家資通安全會報（以下簡稱本會報），並於同月召開第 1 次委員會議，從此開啟政府有計畫地推動我國資通訊安全建設之路。

延續第 1 期機制計畫的成果，持續推動資安相關建設，對於提升我國整體資安防護能力至為關鍵，行政院爰於 93 年通過第 2 期機制計畫（94 年至 97 年），復於 96 年 2 月核定修正之。參照上一期計畫以「確保我國擁有安全、可信賴的資訊通訊環境」為願景，第 2 期機制計畫規劃「提升通報應變時效」、「健全資安防護能力」、「深化資安認知及教育」、「促進國際合作」四大政策目標，主要政策包含政府機關資訊安全長（Chief Information Security Officer, CISO）責任制度、資安責任等級分級作業與機密資訊保護等，對強化政府機關之資安能力產生一定的影響。

97 年 3 月行政院科技顧問組發表《2008 資通安全政策白皮書》，揭示「安全信賴的資訊化社會，安心優質的數位化生活」之願景。出版該書，旨在讓社會各界對政府之資通安全政策有較完整的瞭解，並期望在政府與民間充分合作之下，共同推展資通安全建設，齊心營造台灣成為「優質網路化社會」。

第 2 期機制計畫執行 4 年來，在各部、會、署、直轄市及縣市政府的努力之下，已獲致一定的成果，惟面對全球複雜多變的資安環境，我國在發展數位經濟時，除了充分利用資通訊科技所帶來的優勢外，面對日益嚴重的資安威脅，持續落實有效措施，實屬必要。是以，本會報於 96 年委託研究、97 年邀集相關部會組成專案小組，以前 2 期計畫的工作要項為基礎，同時參酌《2008 資通安全政策白皮書》的規劃，研訂「建立我國通資訊基礎建設安全機制計畫」之賡續發展計畫。復考量經過兩期計畫的推動，業建立我國之「通資訊基礎建設安全機制」，且在本會報協調運作之下，已達成「建立整體資安防護體系、健全資安防護能力」之階段目標，並為與院頒「國家資通訊發展方案」之名稱用語一致，將計畫定名為「國家資通訊安全發展方案（98 年至 101 年）」（以下簡稱本方案）。

第二章　現況分析

壹、 發展現況

在兩期機制計畫引領下，搭配數位台灣計畫的推動，我國在資安基礎環境建設與政府機關（構）資安防護能力的提升上已初具成效。

一、 資安基礎環境建設

以下分別從資安法制建構、認知教育與宣導活動、資安人才培育、資安技術研發、數位憑證推廣運用等面向說明我國資安基礎環境建設概況。

(一) 資安法制建構

基於強化資訊應用之初衷，政府持續參照國際間相關立法趨勢，積極整備促進政府資訊應用、打擊網路犯罪、維護民眾通訊隱私與個人資料保護等基礎法制。

90 年 10 月立法院三讀通過電子簽章法，對網路及電子商務市場的發展影響至深。此外，培植評估與驗證國內外資安產品能力，並建立國際互信機制則是政府持續努力的目標。

在打擊網路犯罪方面，我國於 92 年 6 月增訂刑法第 36 章「妨害電腦使用罪」章，讓駭客入侵、病毒散布或植入木馬等行為皆有明確的處罰依據。另為避免兒童或少年接取網路不良資訊，我國於 93 年通過電腦網路內容分級處理辦法，有相同意旨之法令，另見電腦軟體分級辦法、出版品及錄影節目帶分級辦法等。

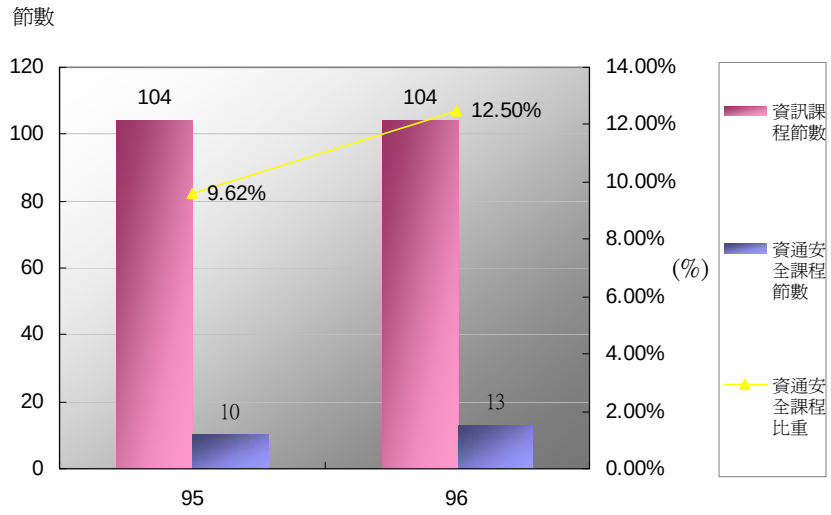
94 年底公布之政府資訊公開法，以便利民眾共享與公平利用政府資訊，增進全民對公共事務之瞭解、信賴及監督，並促進民主參與為目的。惟考量資訊公開之前提仍在於維護機密，我國已先於 92 年制定實施國家機密保護法，以落實公務機密保護、維護國家安全及利益，與確保行政目的之遂行。

有關民眾通訊秘密與個人隱私，我國主要以刑法、通訊保障及監察法與電信法相關法令來加以保護。然而隨著網路科技與各類新興應用的普及，偽造與詐欺犯罪的猖獗已危及民眾對電子交易安全的信心，益發突顯線上身分認證與個人資料保護的重要性。現

行法制因應科技特性而檢討者，包含個人資料保護法草案、濫發商業電子郵件管理條例草案，已由相關機關積極推動立法中；電子簽章法亦在研議修正，並思考擴張電子簽章之適用範圍，新增對電子交易與訂約之規範等。

(二) 認知教育與宣導活動

基於強化資安認知宣導的必要性，教育部積極推動中小學資安認知教育，以「引導學生了解資訊倫理、電腦使用安全及資訊相關法律等議題」。圖 1 顯示 96 年我國中小學資安課程占資訊教育的比重於 95 年上升 2.88%達 12.5%。



資料來源：國民中小學九年一貫課程綱要（教育部全球資訊網 95~96）

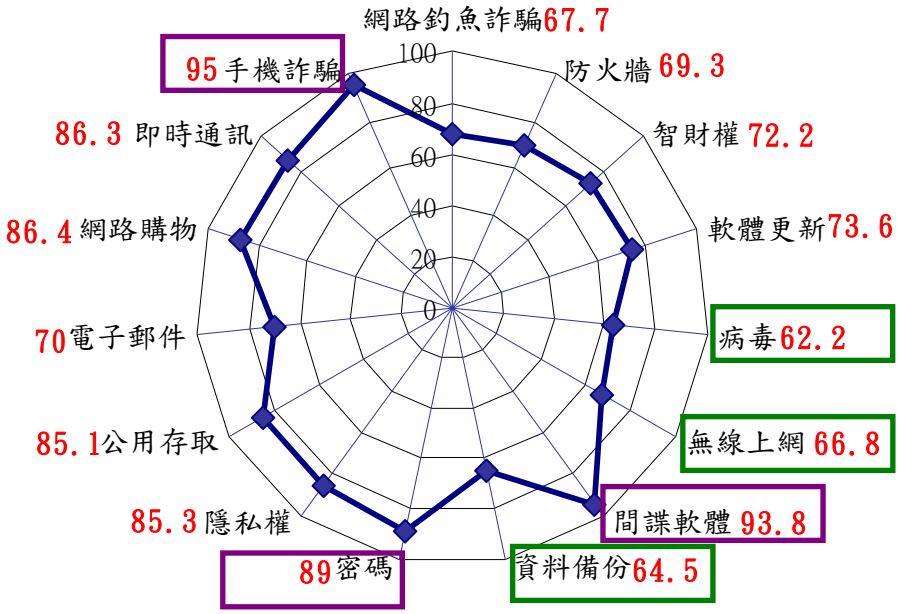
圖 1 我國中小學資安課程占資訊教育比重

政府各主管機關及目的事業主管機關亦已規劃對所屬、一般民眾、所轄民間機構員工等，實施資安認知宣導計畫，藉由系統化的推廣，提升使用者資安認知，以降低資安事件發生頻率或防止損害擴大。

有關國人的資安意識表現，根據 97 年 8 月財團法人中華民國國家資訊基本建設（NII）產業發展協進會委託中央研究院針對台灣地區（含離島）1,079 位 15 歲以上使用電腦網路的民眾所做的資安認知電訪調查[1]，訪查結果每一題的答對比例均超過六成，約略反應經常上網的民眾普遍具有基本的資安認知。反觀受訪者針對「病毒」、「資料備份」及「無線上網」等三項的認知判斷力則

[1] 財團法人中華民國國家資訊基本建設產業發展協進會/財團法人資訊工業策進會「協調推廣全民資通安全認知計畫」，97 年 8 月

略顯不足，有待強化，詳見圖 2 所示。



資料來源：財團法人中華民國國家資訊基本建設產業發展協進會/財團法人資訊工業策進會「協調推廣全民資通安全認知計畫」，97 年 8 月

圖 2 資安認知強弱項目

(三) 資安人才培育

我國資安人才培育可區分為在學培育與在職培訓兩大類。在學培育以教育部自 94 年起推動執行的資通訊安全學程計畫為例，95 年共 15 所、97 年共 27 所大專院校之申請補助計畫獲審核通過，至 97 年 6 月底計有 200 人次取得學程證書。

在職培訓，可區分為基礎培訓與研究發展兩類。基礎培訓目前由經濟部工業局、行政院研考會及其他民間訓練機構辦理，提供職前、在職、轉業訓練，以提高業界專業人力或提升在職人員資安相關知識為目標。在職研發則藉由產學合作，並與國外頂尖學研機構進行人才及技術交流，以達培育專業資安科技研發人才及落實資安核心技術研發為目標，較具代表性的計畫如 94 年正式啟動的資通安全科技跨國研究（International Collaboration for Advancing Security Technology, iCAST）計畫，由政府相關單位與資通安全研究與教學中心（Taiwan Information Security Center, TWISC）及業界相關研究單位共同參與，該計畫於 96 年至 98 年

預計培育資安相關技術人員 33 人、博士生 49 位、碩士研究生 44 位及種子師資 25 位以上。另該計畫已與 3 家民間業者簽署合作備忘錄（Memorandum of Understanding, MoU），共同推動產學合作以提升我國資安產業競爭力。

另有關政府機關人員之資安教育，依行政院第 2993 次院會院長裁示，已由行政院人事行政局通函各單位納入年度訓練計畫實施，而行政院研考會亦已於電子化政府－網路文官學院（http://elearning.nat.gov.tw/）之資訊安全課程類別下，提供多門適用於各職務性質的資安數位課程，供各界上網學習。

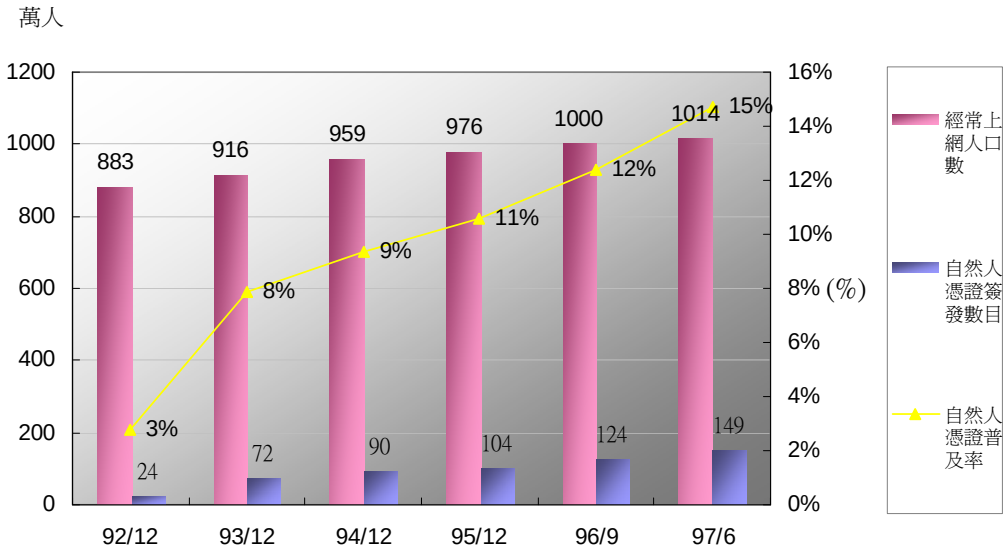
(四) 資安技術研發

為整合國內各大學及研究機構的研究資源，94 年 4 月 1 日資通安全研究與教學中心正式成立，其主要參與團隊包含中央研究院、台灣科技大學、台灣大學、交通大學與成功大學等，主要目的在於透過前瞻議題研究，支援產業應用能量。

近年來我國投入關鍵資安技術研發的主要成果，如發展無線感測網路之密鑰管理技術與適用之安全路由協定、高安全遠端身分鑑別理論研究、安全網路（Secure Cyberspace）核心技術與關鍵系統研發與實作、整合式安全控制（遠程醫療照護）系統實作等，對於協助國內資安產業提升自主研發能力與技術自主性具有一定程度的效益。

(五) 數位憑證推廣運用

圖 3 顯示 97 年 6 月我國自然人憑證簽發數累計約 149 萬人(94~97 年使用人次累計近 2 千萬人次），占經常上網人口比例之 15%，較 96 成長 20%，同時我國自然人憑證簽發比例自 92 年起逐年上升。有鑒於透過數位憑證運用以建立資訊系統安全防護之重要性，推動其應用於電子化網路申辦服務，是政府持續努力之目標。



資料來源：資策會 FIND/經濟部技術處「創新資訊應用研究計畫」、內政部資訊中心

圖 3　我國自然人憑證簽發數目與簽發比例

二、 政府機關（構）資通安全防護能力提升

在本會報各工作組與應變分組的努力之下，第 2 期機制計畫「提升通報應變時效」、「健全資安防護能力」、「深化資安認知及教育」及「促進國際交流合作」四大政策目標之達成情形如次。

(一) 提升通報應變時效

通報應變組

本會報通報應變組自 94 年起由行政院研考會主責，在該會的努力下，業建立 7,486 個政府機關（構）資安聯絡人資料、接獲 2,994 件資安事件通報、提供 226 件資安事件技術服務及 10,467 件資安諮詢服務。

國家資通安全防護管理平台（National Security Operation Center, NSOC）則不僅提供一般監控與預警服務，且將 23 個機關納入防護範圍，依機關業務需求，配置不同監控設施，如佈署入侵偵測系統（29 個）、DNS 警示系統（20 個）、內部網路警示系統（16 個）、使用者端警示系統（12 個）（機關）等。而除了強化通報應變網站功能、定期進行通報演練外，資安警訊發布亦已結合通報聯絡人資料庫，可適時針對資安聯絡人，發布系統漏洞、駭客訊息等，確已有效提升整體通報應變時效。

(二) 健全資安防護能力

法規偵防組

目前國內因應網路犯罪所成立之任務編組，包括台灣高等法院檢察署之「電腦犯罪防制中心」與各級檢察署之專股/專組辦案機制、內政部警政署刑事警察局之「科技犯罪防制中心」、國家通訊傳播委員會之「電信警察隊」、法務部調查局資訊室、各縣市警察局刑警隊所成立之「電腦犯罪偵防小組」等。而為跨國合作打擊網路犯罪，檢警機關亦已積極建立與他國執法單位聯繫管道（如我國於 92 年正式入會之 G8 24/7 Network（八大工業國家高峰會「防制高科技犯罪各國連繫窗口全天候聯防組織」），共同合作處理駭客入侵事件，並派員赴國外研習。

在強化偵辦電腦與網路犯罪之技術與效能上，本會報法規偵防組（法務部）完成「精進檢察官電腦/網路犯罪執法能力與資安法制建構計畫」、在 95 年建置完成資通安全鑑識實驗室，並持續朝制定數位證據蒐證標準作業程序、建置實體設備、加強實驗室及人員的認證與訓練等三個方向努力。此外，「犯罪現場及網路環境之數位證據保全及鑑識分析能量提升計畫」等三案亦獲行政院國家科學技術發展基金補助執行。另 97 年計支援外勤單位現場搜索共 49 案、109 人次、送鑑案件 65 案，較 96 年現場搜索 29 案，69 人次，送鑑案件 36 案，大幅增加。97 年度內協助搜索包含「特偵組調查相關洗錢案」、「某職棒簽賭案」、「O 縣長下水道工程涉嫌不法案」、「東 O 公司涉嫌違反公司法、反武器擴散案」等涉及犯防、貪瀆、國家安全等重大案件。此外，亦協助桃園地檢署「大潤發公司購買大陸三鹿奶粉案」、台灣高等法院「實密科技有限公司之資料磁帶復原案」等各地方法院及地檢署之鑑識案件。

標準規範組

本會報標準規範組（經濟部標準檢驗局）自 91 年起陸續完成 CNS27001 等 59 種國家標準，持續推動重要核心政府機關援引與採用，並每年舉辦資安稽核相關訓練 4 場次。另行政院研考會於 94 年完成「行政院及所屬各機關資訊安全管理規範」（修訂草案）「資通安全規範整體發展藍圖」等文件，預計於 4 年內發展完成防火牆安全參考指引等 37 份文件，陸續提供各政府機關（構）參照、遵循。97 年完成「資通安全共通規範發展藍圖」修訂、「資訊系統風險評鑑參考指引」等 14 項資安規範或參考指引、並選定 5 項參考指引及遴選試行機關辦理實務導入、辦理 3 項資安參

考指引實務導入及 3 項資安參考指引修訂。

政府近年來於公務體系中亦積極推動導入資訊安全管理系統（Information Security Management, ISMS）驗證，採用規劃－執行－檢查－行動（Plan-Do-Check-Act, PDCA）過程模型，藉以提升政府機關（構）資訊安全管理水準，降低相關作業風險。

有關推動機關（構）核心業務系統導入資訊安全管理系統，迄 97 年 12 月我國已有 202 個政府機關構與民間企業通過國際驗證（ISO27001（國內 CNS27001）），居全球第 4。

通報應變組

通報應變組在本項目標上所達成的績效指標包含在 94 年完成警訊發布系統，95~97 年共發佈 3,892 則警訊通告、79 則資安訊息、4 則緊急事件、443 則網頁攻擊、2,605 則資安預警及 761 則入侵事件；辦理地方政府網站 SQL Injection 及 Cross Site Scripting 等重要弱點檢測及協助修復，並辦理 73 場說明會；推動各部會規劃建置虛擬私有網路（VPN），整合成單一資訊網路，強化網路防衛縱深；訂定 NSOC 資安事件資料交換格式（Security Incident Data Exhchange, SIDEx），建立 NSOC 與政府自建或民間 SOC 資安事件訊息交換模式，通過 NSOC 資安事件資料交換連通測試驗證廠商共 12 家；96 年 5 月起與 GSN 維運小組合作，建立駭客中繼站攔阻機制，自骨幹網路阻擋駭客嘗試性連線共 3,416 萬次等。

從表 1 歷年資安攻防演練結果：手法精進而模擬入侵成功比例逐年降低（由 93 年 1.2%降至 0.84%、0.56%再精進至 96 年 0.3%）顯示，政府機關整體資安防護能力提升。

表 1　93~96 年資安攻防演練攻入比例

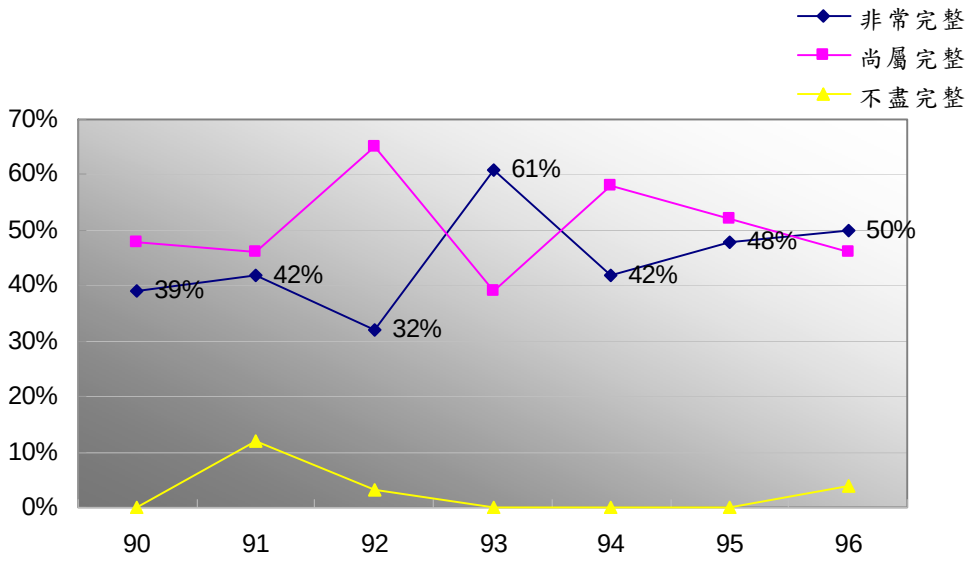
年度 / 項目	93	94	95	96
攻擊 IP 數	18,960	13,954	21,888	21,888
攻入 IP 數	228	117	123	65
攻入比例（%）	1.2	0.84	0.56	0.3

資料來源：本會報，97 年 2 月，資安演練成果及通報執行情形

稽核服務組

本會報稽核服務組（行政院主計處電子處理資料中心）自 90 年起每年選擇 30 餘重要核心機關進行資安外部稽核，並於 94 年起

推動主管機關進行內部稽核。迄今該中心已對 303 個公民營單位進行資安外部稽核（主要以政府機關為主），提供稽核建議，協助受稽單位落實資安防護工作之完整性與有效性。圖 4 顯示歷年受稽單位外部稽核被評為非常完整之比例呈上升趨勢，自 90 年 39%至 96 年達 50%。



資料來源：主計處電子處理資料中心

圖 4　90~96 年政府資通安全準備情形統計

綜合規劃組

延續上一期計畫，第 2 期機制計畫（94 年至 97 年）持續推動政府機關資訊安全長責任制度並藉由資通安全責任等級分級作業，以充分運用有限的資源，達到強化政府機關資通安全防護能力的目標。

目前本院、37 部會、25 直轄市及縣市政府均已設立 CISO，並成立資通安全處理小組，負責推動執行單位內之資通訊安全相關計畫，另重要涉密機關均已依需求採用適當的實體隔離作法與加密保護措施，俾有效保護機密資訊安全。

95 年 10 月涵蓋 80%以上的政府機關（計 6,979 個）納入資安分級，執行本會報所律定之資安應辦事項。不僅各等級均須於一定期限內達到應有的防禦機制強度及縱深，A、B 級機關並將陸續通過資訊安全管理系統驗證。

而為防止 P2P 分享軟體所衍生之資安問題，本會報推動 A 級機關

於 96 年 9 月底前訂定點對點（P2P）分享軟體使用規範，並清查移除不當 P2P 軟體。前項作為且已於 97 年由主管機關推動 B 級機關執行，俾擴大政策效益。

另本會報 96 年亦積極推動「防範惡意電子郵件社交工程施行方案」，各機關已依規劃自 96 年 10 月起推動執行相關防制措施。96 年度電子郵件社交工程演練結果與上一年度相較，開啟郵件人數比自 43%降至 24.17%；點閱連結人數比自 23.9%降至 16.29%，顯示相關人員之警覺性已大幅提升。

本會報尚政策引導資安科技跨國研究計畫於 96 年納入優先推動計畫，目前有 50 餘位教授，約百名碩博士生參與，另工研院與資策會亦參與研發資安相關技術。該計畫並已與 3 家民間業者簽署 MoU，推動產學合作以提升我國資安產業競爭力。

通報應變分組

在關鍵資訊基礎建設保護上，本會報自 90 年起即針對足以影響國家安全與社會安定之 20 個重要作業系統（94 年增至 24 個），制定包括建置 ISMS、SOC 與人員訓練等資安管制方案，初期由本會報集中管制，96 年起已由各領域主管機關自行督導目的事業機構落實執行保護措施。而國防部、外交部、經濟部及交通部亦於 96 年起規劃或建立國防、外交、能源（水、天然氣）及交通運輸等領域資安資訊分享與分析中心，俾逐步導引各領域關鍵基礎建設在資通安全事件發生時，能迅速而確實的應變，並透過群策群力的方式構築周密無漏洞的資通安全防護網。

此外，經濟部推動「網路商店雙向身分認證機制」、「電子商務交易保障機制」、「線上選擇性爭議處理機制」等 8 項電子商務信賴機制（94~96 年 2,794 家次商店運用）；國家通訊傳播委員會亦已促使中華電信公司於契約服務第 46 條訂定資安規範，並透過「台灣網際網路協會（TWIA）」建立各業者橫向連絡網，且於網站上設置檢舉信箱。以上，對於保護個人資料皆具有積極、正面作用。

(三) 深化資安認知及教育

除了本章壹、一之（二）與（三）教育部、行政院人事行政局等機關在資安認知教育與宣導活動及人才培育上所獲致的成果之外，行政院國家科學委員會負責本會報資訊服務組工作，為加強最新資通安全技術發展與政策資訊之提供，自 94 年起於所建置之資通安全資訊網刊登資通安全分析專論，除提供下載及專題選

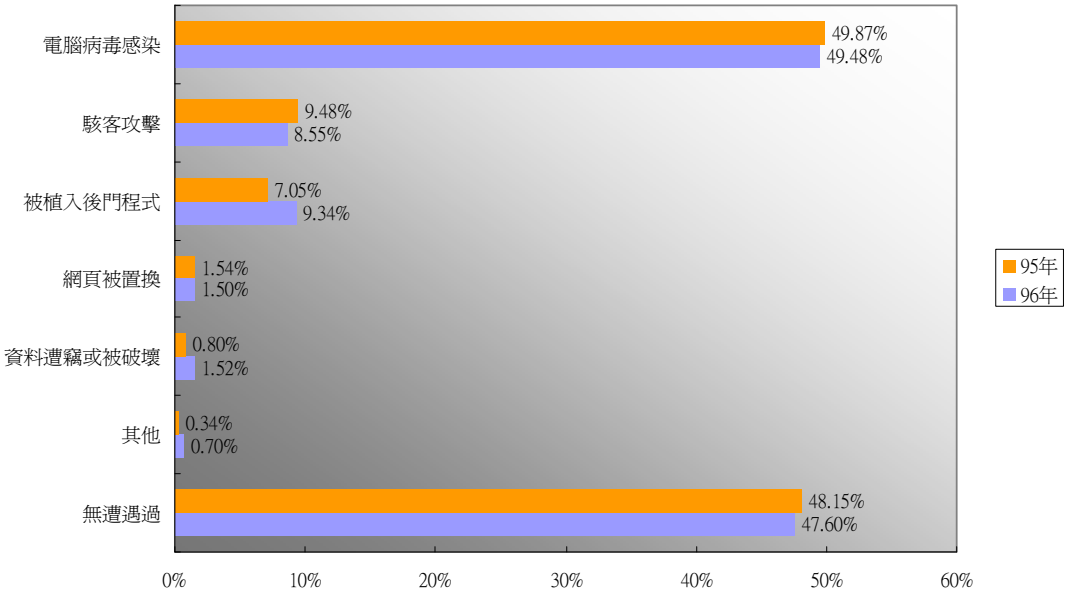
粹訂閱服務外並將之彙集成冊，以方便各界人士閱讀（該組全年蒐集資料 16,400 筆、網站點擊數 391 萬人次、完成國內外資通安全報告摘要 31 篇、資通安分析專論 25 篇）。此外亦委由國家實驗研究院科技政策研究與資訊中心（原該會科學技術資料中心）延請國內資通訊安全領域的學者專家規劃編輯三套共 20 冊資通安全專輯，出版以來，普受資安相關專業人士歡迎並已產生廣泛的影響。

而行政院研考會於 94 年至 97 年共完成資安專業證照培訓 440 人次，取得 215 張 ISMS LA、8 張 CEH 及 3 張 CISSP 證照，已達到一定程度提升政府機關（構）資安專業人力的目的。

貳、 現階段資安問題與挑戰

隨著資通訊科技發達，網路應用與服務愈加豐富多元，同時也帶來了不同的資安威脅，其來源包含電子郵件、即時通訊與分享軟體及全球資訊網（World Wide Web, WWW）等，駭客攻擊對象則是從廣泛散播，轉而針對特定目標或區域，攻擊手法與技巧更是不斷翻新－製作潛藏於資通訊設備中的惡意程式已取代刪除檔案、阻絕服務及以癱瘓電腦為目的的惡意程式，一群有組織、有特定目的的個人或團體，不斷創造行蹤更隱匿的惡意程式，伺機對被控制的電腦下達指令，啟動包含濫發垃圾郵件與竊取個人資料或業務機密等各種惡意行為，對於優質網路化社會的發展，已造成相當程度的負面影響。

根據行政院主計處的統計，過去二年內，平均半數以上政府機關（構）與民營企業曾遭遇資安事件的困擾。其中以遭受電腦病毒感染，最為普遍。其餘資安事件類型比率則相對較低。（如圖 5）

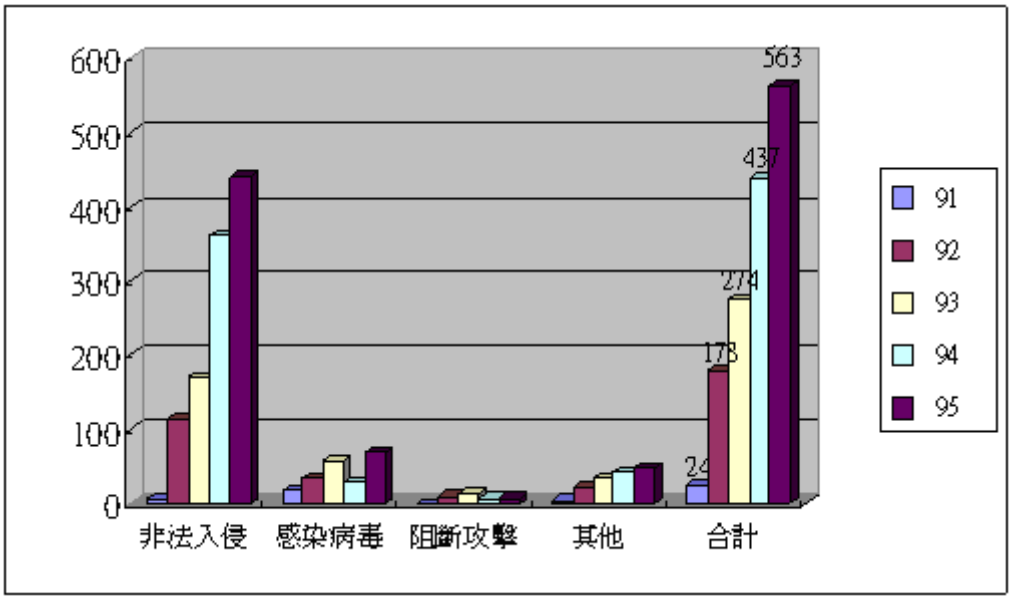


資料來源：行政院主計處，97 年 10 月，96 年電腦應用概況報告

圖 5　遭遇資安事件概況與類型

而在兩岸特殊的情勢之下，政府正面臨日益嚴重的資安威脅。圖 6 顯示政府機關資安事件通報件數於 91~95 年逐年遞增，其中以「非法入侵」占大宗，96 年更一共接獲 1,191 件資安事件通報，較 95 年大幅成長 170%，主動通報率則由 95 年之 5%提升至 51.08%。

另根據本會報技術服務中心的分析，結合零時差與社交工程之攻擊為我政府機關公務內網資訊遭竊之最主要威脅，鎖定目標、假冒身分及發布公務訊息之偽冒電子郵件為必然之發展趨勢，各機關對外服務伺服器之系統安全雖已有顯著進步，但 Web-based 之應用程式（如 SQL Injection ）卻仍存在許多安全漏洞。



資料來源：行政院國家資通安全會報

圖 6　91~95 年政府機關通報情形

技術服務中心 95 年分析 417 封各政府機關使用者通報有問題之電子郵件，信件主旨包含政治新聞、生活議題、公務通告、情色等，其中 287 件經鑑識確定隱藏惡意程式；96 年亦分析 1,558 件惡意電子郵件，其中 729 件具有惡意行為。根據 95 年政府機關社交工程演練結果顯示，開啟惡意郵件及點閱惡意聯結或附件之比率分別高達 43%與 23.9%，可見電子郵件社交工程攻擊的威脅性。因應此一威脅，本會報特別將防範惡意電子郵件社交工程攻擊列為當（95）年重點工作，96 年度電子郵件社交工程演練結果與前一年相較，開啟郵件人數比自 43%降至 24.17%；點閱連結人數比自 23.9%降至 16.29%，顯示相關人員之警覺性已大幅提升。

行政院主計處每年針對政府機關與民營企業(不含家庭面資料)辦理電腦應用概況調查。96 年國內 30 人以上機構資訊總經費約 1,278.04 億元，其中資安支出占 5.40%，為 68.95 億元(詳如表 2)，96 年在資訊總經費成長的情況下，資安經費較 95 年增加 13.90 億元。

表 2　資安經費概況

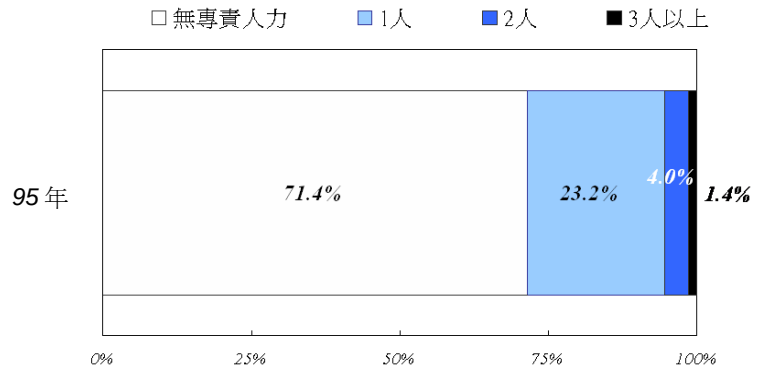
單位：百萬元；%

經費概況 / 機構類別	96 年			95 年		
	資訊總經費	資安經費		資訊總經費	資安經費	
		金額	占資訊總經費（%）		金額	占資訊總經費(%)
總計	127,804	6,895	5.40	120,774	5,505	4.56
民營企業	88,716	4,374	4.93	80,917	3,168	3.91
政府行政機關	17,640	1,334	7.56	17,907	1,237	6.91
公營事業機構	10,205	651	6.38	11,136	511	4.59
公立學校	4,281	203	4.74	4,316	243	5.62
公立研究機構	449	21	4.75	592	32	5.41
私立學校	5,035	256	5.09	4,064	253	6.23
私立研究機構	1,478	57	3.84	1,842	61	3.30

註：針對 30 人以上機構調查

資料來源：行政院主計處，97 年 10 月，96 年電腦應用概況報告

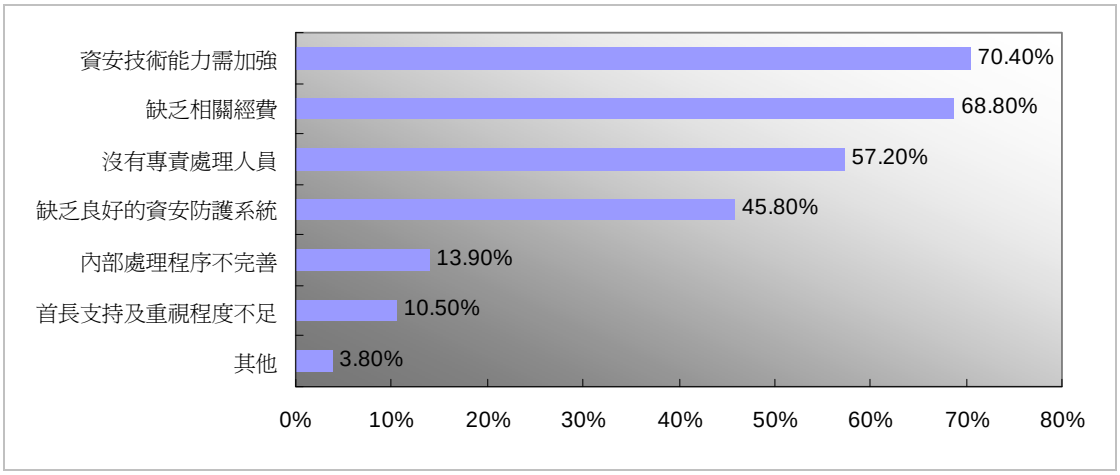
行政院研考會於 95 年 9 月至 10 月間，針對各級政府機關（構）5,075 位資訊部門主管或資通安全聯絡人進行資安人力現況調查。95 年我國政府機關（構）平均僅擁有 0.4 位專責與 1.3 位兼辦資安業務人力，其中高達 7 成未設置專責資安人員（詳如圖 7）。而以資安等級別區分，A 級機關與 B 級機關仍分別有 45.7%與 60.9%尚未設置專責資通安全人員。



資料來源：行政院研考會，96 年 6 月，資安人力調查及需求推估報告

圖 7　95 年政府資安人力統計圖

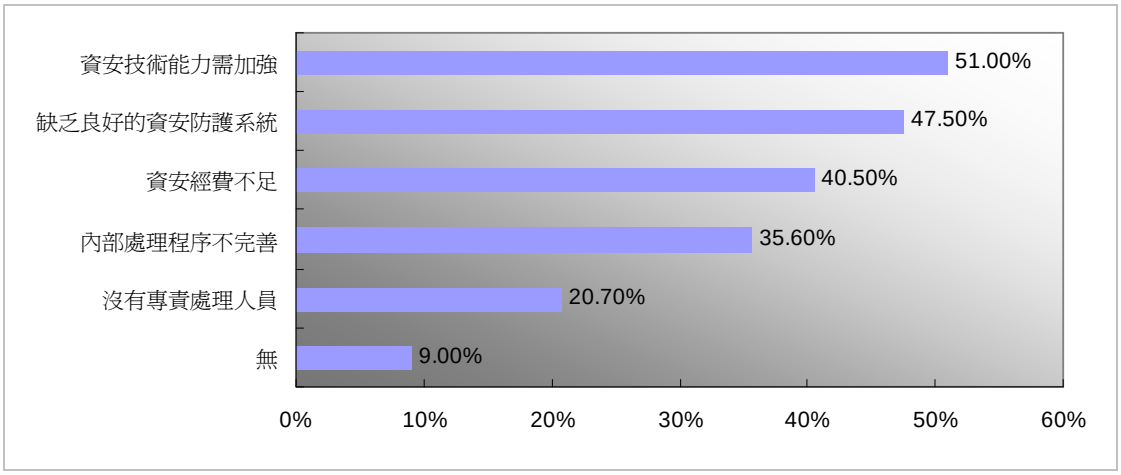
綜上所述，根據 95 年我國政府資通安全應用調查報告，9 成以上政府機關表示在落實資通安全管理及防護時遭遇困難，其中又以資安技術能力需加強、缺乏相關經費、沒有專責處理人員等三項困難亟需克服。（詳如圖 8）



資料來源：行政院研考會，95 年 11 月

圖 8　政府機關（構）落實資安管理及防護所遭遇困難

有關資通安全技術能力與經費不足的問題，我國大型企業在處理資安事件時，亦遭遇同樣的困難。因應新興多變的資安威脅，資安技術漸趨複雜且日新月異，51.0%大型企業坦承自身技術能力需再加強，同時 4 成以上大型企業表示資安經費不足。（詳如圖 9）



資料來源：資策會 MIC；95 年 4 月

圖 9　大型企業處理資安事件所遭遇困難

參、 我國之資安發展優勢、弱點、威脅和機會分析

經過兩期機制計畫的推動，透過政府與民間共同努力，我國的整體資安環境已有長足的進步，惟距離「安全信賴的智慧台灣、安心優質的數位生活」，仍有一段距離。以目前的狀況而言，欲實踐

前述願景，各有內部環境之優劣勢與外部環境之機會與威脅，如表 3 所示。

表 3　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強。 3. 擁有豐富的資安防護經驗與駭客行為模式資料。	1. 使用者在行為面並未落實資安，認知與警覺性仍待進一步提升。 2. 資安相關法制立法推動不易，未設資安專責主管機關，無法充分發揮事權統一之效。 3. 資安治理知易行難，亟待宣導推廣。 4. 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。 5. 資安資訊分享不易。 6. 關鍵資安科技為先進國家所掌握且不易突破以及資安產業發展條件受限。 7. 資安國際合作空間受限。
機會（Opportunities; O）	**威脅（Threats; T）**
1. 政府持續發展資通訊應用及建設，可充分掌握行政院組織改造契機，優化政府資訊架構並提升整體網路安全。 2. 隱私權與智慧財產權保護議題受重視。 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. 資通訊安全無國界，在國際社會中，各國皆須強化國際地位與影響力並積極拓展資安合作機會。	1. 資安績效評量不易，潛在效益經常被忽略，致令資安資源投入不足。 2. 因應資安發展趨勢，各先進國家均已陸續推動資安相關管理機關的組織調整，並進行必要的立法改革。 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. 國外積極投入資安科技研發，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之作為。

在當前的情況下，我國之資通安全發展環境實不容樂觀。我國目前所擁有的優秀資通訊、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

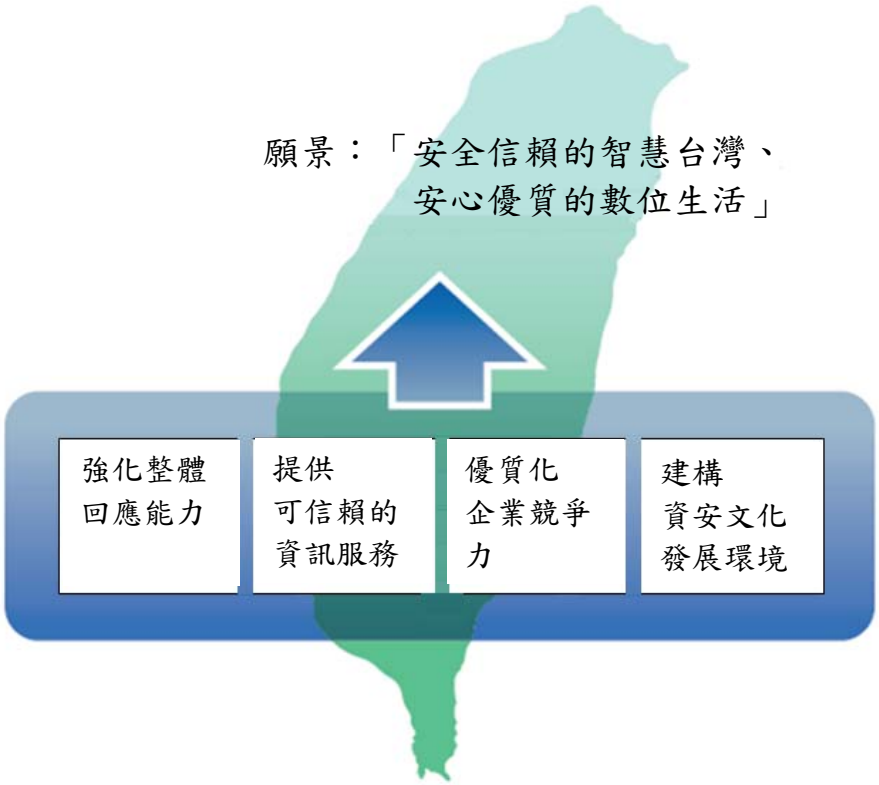
用。因此，如何積極看待、處理和充分利用目前的優勢，使其朝向正向發展，至關重要。

反觀我國目前所面臨的資安問題，在資通訊安全的重要性已不容忽視的情況下，卻因為整體資源投入有限，不僅無法正確評估資安風險，更可能無法有效的將其控制在可接受的範圍內。透過 SWOT 分析所反映出來的情況，政府必須清楚地意識到現階段所面臨的資安問題和可能遇到的威脅與挑戰，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，確立本方案願景與政策目標，針對現階段我國發展資通訊安全所面對問題，制定有效的解決對策，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。

第三章　願景與政策目標及發展藍圖

壹、 願景與政策目標

本方案之願景旨在達成「安全信賴的智慧台灣，安心優質的數位生活」（如圖 10 所示），期經由前瞻政策的引導，在政府與民間的通力合作之下，透過國家整體力量，逐步推動並落實充分考量我國特性的資安行動方案。



資料來源：本會報綜合規劃組整理

圖 10　願景與政策目標

透過實踐各項行動方案，本方案將達成「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：

一、 強化整體回應能力

當重大資安事件發生時，必須具備能在有限的時間內，採取緊急應變行動的能力，方能使災害損失降至可接受的程度，並確保核心業務的持續運作。整體回應能力包含通報、應變及復原等能力，每年由通報應變組辦理一次資安演練加以驗證，各機關亦須配合進行內部演練，並執行改善計畫。

二、 提供可信賴的資訊服務

高度資訊化社會，民眾對於政府與關鍵基礎建設的最基本期待在於兩者所提供的資訊服務是可以讓人安心且可信賴的。基於此，A、B 級機關須分別於 100、101 年底前導入資安治理、資訊與資訊系統之分類分級至 101 年已可由主管機關自行列管所屬機關，以達基本資安防護需求，同年各機關亦已依需求配置資安人力。在持續強化資安稽核上，各機關每年至少辦理一次內部稽核，同時稽核服務組仍將選定重要單位進行外部稽核。至於，關鍵資訊基礎建設的保護，係以建立各領域資安預防與早期預警、偵測、反應、危機管理能力為要，在 97 年建置完成重要民生基礎建設資安資訊分析與分享中心（電力、油氣及自來水部分）基礎之上，預期於 98 年再由教育部、國家通訊傳播委員會完成區網中心資安資訊分析與分享中心，以及電信網路「資訊安全通報處理平台」之建置。

三、 優質化企業競爭力

在支援策略所需的資訊資本日益重要、各行各業相繼投入資源以強化資訊力作為組織要務之際，資安的重要性尤其不應該被忽視。是以透過資安來為組織的核心業務創造價值，並協助企業達成未來的競爭優勢，亦為推動本方案的目標之一。在強化企業資訊安全上，經濟部預計於 101 年底前輔導網路 200 家商店應用線上身分認證機制、建立 20 個商業交易安全認證示範應用體系，完成 10 種不同行業之輔導。金融監督管理委員會亦將於 101 年底前推動證券期貨交易網路下單作業使用 CA 憑證進行身分安全認證率達 90%。至於發展資安服務業，經濟部標準檢驗局每年將制定完成 5 種資安相關標準，國家通訊傳播委員會將於資安共同準則規範新版公布 2

年內完成中文版公告。此外，研發關鍵資安技術，推廣研發成果，帶動產業發展，與建構資安人才培育體系，亦為推動重點。

四、 建構資安文化發展環境

推動「個人資料保護法」儘速完成立法，是本會報法規偵防組持續努力的目標之一，該法通過後，相關主管機關可依前揭修正法規授權指定保有大量且重要之個人資料檔案的非公務機關，訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。在提升全民資安認知上，除透過教育體系資安計畫讓資安觀念從小紮根外，本會報資訊服務組將持續提供資安資訊服務、每年出版 25 篇資安專論與舉辦 2 次研討會。此外，亦將透過標竿學習以鼓勵讓資源發揮最佳效益的創新作法，自 99 年起舉辦的政府機關（構）資安最佳實務競賽，預期將成為資安年度盛會。而由於資安所涉及的層面相當廣泛，因此必須透過團隊合作的方式來推動。包含各機關之間的聯繫與合作、政府與民間的合作夥伴關係及與國際間友好國家的合作等，均應大力加以促進。

最後，透過資安關鍵指標的量化資訊、定性分析，可概略瞭解我國資安政策發展狀況、實施成效及趨勢。是以，本會報將持續每年調查、維護及發布指標數據，並以改善各項數據為努力方向。我國資安關鍵指標共分為 3 大類：資安認知與環境、整體資安防護能力及緊急應變功能；此 3 大類再細分為 18 個細項指標，以清晰呈現我國在某項目上的表現。95~97 年我國資安關鍵指標的總表現如表 4 所示。

表 4　95~97 年我國資安關鍵指標表現總表

大類	小類	指標名稱（單位）	數據			資料來源
			95	96	97	
資通安全認知與環境	資安資源投入程度	組織資安經費占資訊經費比例（%）	5.08	4.56	5.4	行政院主計處
		組織具有資安教育訓練之比例（%）	-	38.0	39.9	台經院
		組織設置資安專責主管之比例（%）	-	16.2	9.6	台經院
	資通安全法規整備度	資通安全法規建立之整備度（%）	72.7	72.7	72.7	台經院
	民眾資安素養	民眾具資安素養之比例（%）	*75.3	*65.5	*70.8	NII
整體資通安全防護能力	資安防護裝置完備度	防毒產品使用普及率（%）	86.4	90.7	86.7	行政院主計處
		防火牆普及率（%）	67.5	76.9	76.4	行政院主計處
		入侵偵測系統（IDS）普及率（%）	17.6	21.9	28.4	行政院主計處
		漏洞修補程式管理普及率（%）	-	38.8	46.0	台經院
	資安認驗證情形	政府及上市櫃企業通過資安驗證之比例（%）	-	5.3	6.7	台經院彙整
		人員取得資安專業證照數（張/每百萬人）	-	196	248	台經院彙整
	安全網路伺服器普及率	擁有安全網路伺服器（SSL 伺服器）數（台/每百萬住民）	*169	*298	*312	台經院
	資安事件發生率	組織遭受資安事件侵害之比例（%）	40.5	51.8	52.4	行政院主計處
		資料遭竊或被破壞之比例（%）	0.65	0.8	1.5	行政院主計處
		組織遭遇病毒侵害之比例（%）	38.8	49.9	49.5	行政院主計處
		組織遭遇傀儡程式感染之比例（%）	5.0	7.1	9.3	行政院主計處
緊急應變功能	資通安全演練	組織舉辦資安演練之比例（%）	-	33.8	42.7	台經院
	資安事件損害	資安事件危害與復原時間（小時）	-	11.35	12.34	台經院

說明：標示*數據表示當年度調查結果，其餘數據表示調查前一年狀況；部分指標項目於 95 年未進行調查，故無數據。

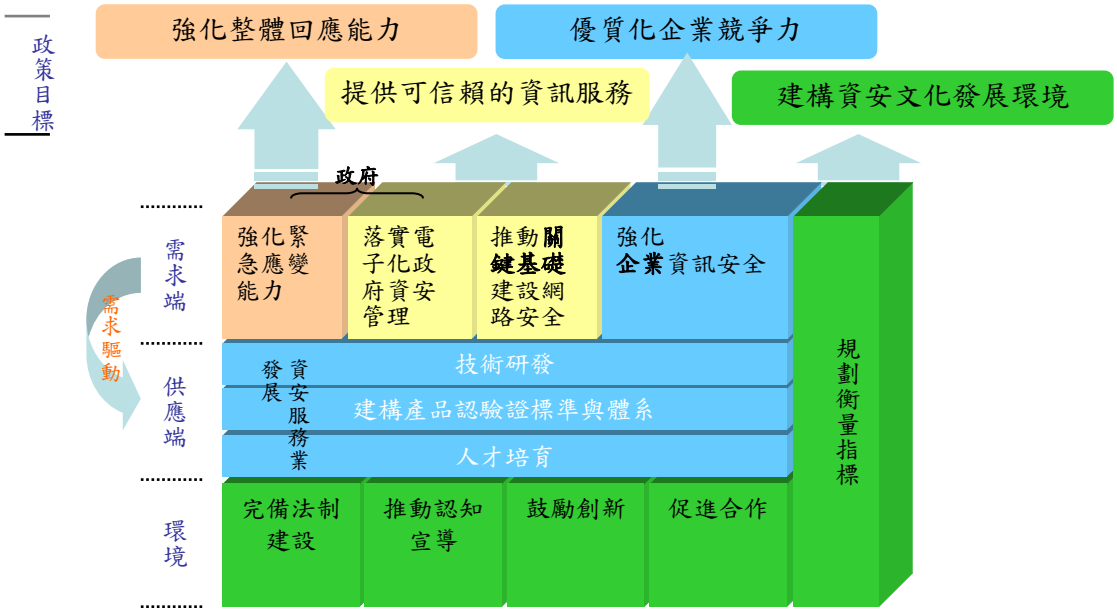
資料整理：台灣經濟研究院

貳、 發展藍圖

本方案之發展藍圖（如圖 11）可從「需求端」、「供應端」及「環境」三個面向加以考量。需求端包含政府、關鍵基礎建設、企業三個主體，分別透過強化緊急應變能力、落實電子化政府資安管理、推動關鍵基礎建設網路安全及強化企業資訊安全等措施，預期可達成強化整體回應能力、提供可信賴的資訊服務及部分優質化企業競爭力的目標。

有關優質化企業競爭力，還需要供應端的支持，途徑是透過建構資安服務業發展環境，包含技術、標準、人才等，並藉由需求趨動，進而發展資安服務業。

環境面，則包含完備法制建設、推動認知宣導、鼓勵創新與合作及規劃衡量指標等，亦分別設計相對應的行動方案，以達「建構資安文化發展環境」的目標。



資料來源：本會報綜合規劃組整理

圖 11　發展藍圖

第四章　重要措施與行動方案

為使各項資安工作能順利推展並落實，本方案分別依據 4 大政策目標規劃 11 項重要措施（30 個行動方案）如表 5，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 5　重要措施與行動方案（分工）

目標	重要措施	行動方案		主（協）辦單位
強化整體回應能力	提升通報應變及復原能力	1.	提升通報時效	行政院研考會（各機關）
		2.	建立資安事件管理與回應程序	行政院研考會（各機關）
		3.	持續發展緊急應變及復原能力	行政院研考會（各機關）
		4.	訓練資安事件回應人力	行政院研考會（各機關）
提供可信賴的資訊服務	落實電子化政府資安管理	5.	發展與維護政府機關資安作業規範與參考指引	行政院研考會（各機關）
		6.	推動資安治理	行政院科技顧問組（行政院研考會、行政院主計處、各機關）
		7.	推動資訊與資訊系統分類分級	行政院科技顧問組（行政院研考會、各機關）
		8.	強化電子化政府資通安全，落實公務資料保護	行政院研考會（法務部、各機關）
		9.	推動政府機關（構）採購符合安全驗證之資通訊設備	國家通訊傳播委員會（行政院研考會、公共工程委員會、各機關）
		10.	充實資安人力	行政院人事行政局、行政院研考會（銓敘部、考選部、各機關）
		11.	提升資安防護技術與服務品質	行政院研考會
		12.	強化資安素養與能力培訓	行政院研考會
		13.	加強資安稽核與推動資訊安全管	各機關（行政院主計

目標	重要措施	行動方案		主（協）辦單位
			理系統驗證	處）
	推動關鍵基礎建設網路安全	14.	發展關鍵資訊基礎建設保護策略	金管會、經濟部、教育部、交通部、衛生署、國家通訊傳播委員會、行政院研考會
優質化企業競爭力	強化企業資訊安全	15.	強化電子商務信賴安全	經濟部、行政院金管會（行政院公平會、行政院消保會、內政部、國家通訊傳播委員會、法務部）
		16.	依法規授權，促進事業機構運用第三方評鑑	金管會、衛生署、國家通訊傳播委員會、經濟部、教育部
		17.	促使業者發揮自律精神，善盡資安社會責任	經濟部、金管會、交通部、衛生署
	發展資安服務業	18.	發展資通安全產品及管理系統認驗證標準及體系	經濟部標檢局、國家通訊傳播委員會（相關部會及目的事業主管機關）
		19.	強化國家資安研究能量	國科會(基礎研究)、經濟部（產業技術與推動）、國防部（國防資安科技研發）
		20.	建構資安人才培育體系	教育部
建構資安文化發展環境	完備法制建設	21.	檢討修訂國家資通安全相關法規	法務部、國家通訊傳播管理委員會
		22.	持續發展數位鑑識能量	內政部（警政署）、法務部、國防部
	推動認知宣導	23.	推動教育體系資通安全計畫	教育部
		24.	提供全方位資安資訊服務	國科會
		25.	整合資安資源之訊息，分眾加強宣導	行政院科技顧問組、行政院研考會、各機關
	鼓勵創新合作	26.	規劃依資安策略需要而運作的新型組織	行政院科技顧問組、行政院研考會
		27.	鼓勵讓資源發揮最佳效益的創新作法	行政院科技顧問組、各機關

目標	重要措施	行動方案		主（協）辦單位
		28.	促進有效的團隊合作	行政院科技顧問組、行政院研考會（各機關）
		29.	促進國際合作	行政院科技顧問組、行政院研考會、法務部、內政部（警政署）、國家通訊傳播委員會、各機關
	規劃衡量指標	30.	調查與發布資安關鍵指標	行政院科技顧問組、行政院主計處

第五章　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（附錄壹），本會報為資通訊安全相關工作推動單位，負責整合本方案範圍內各承辦單位對資通訊安全環境之需求，並規劃、推動及落實本方案。（本會報下各單位職掌如附錄貳）

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貳，細部執行規劃由各主辦單位依政府施政計畫編審相關作業規定制定年度計畫。

參、 預算來源與執行

各主辦單位所提年度計畫之預算來源，由各單位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、 資通訊基礎建設相關行動方案之管考

本方案與電子化政府、產業電子化、網路化社會及資通訊基本建設等國家資訊通訊發展相關之行動方案，由行政院國家資訊通信發展推動小組運用既有督導機制，落實執行。

伍、 計畫核定與修訂

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 年中程方案，並視需要於期中進行檢視修訂。

附錄

壹、 行政院國家資通安全會報設置要點

貳、 行政院國家資通安全會報下各單位職掌

參、 行動方案執行要點與績效指標說明表

壹、 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

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、 本會報設綜合規劃組（本院科技顧問組負責）、標準規範組（經濟部負責）、稽核服務組（本院主計處電子處理資料中心負責）、資訊服務組（本院國家科學委員會負責）、法規偵防組（法務部負責）及通報應變組（本院研究發展考核委員會負責），負責下列事項之政策研究、協調、聯繫、策劃、整合及推動：

(一) 提高資通安全決策層次，強化政府資通安全防護能量。
(二) 積極防衛國家資通設施，確保電子化政府之服務效能。
(三) 建立資通安全預警機制，主動偵防降低實質危害因素。
(四) 研析資通安全相關資訊，加強資通安全專業人力培訓。
(五) 推廣全民資通安全認知，提高資通安全全民防護能量。
(六) 策訂相關資通安全規範，增修訂相關法令及技術標準。
(七) 推動資通安全技術研發，促進資通安全相關產業發展。
(八) 提升執法機關偵防能力，建立跨國及區域性合作機制。

三、 本會報置總召集人一人，由本院主管科技之政務委員兼任；協同總召集人一人，由本院研究發展考核委員會主任委員兼任；委員十八人至三十人，除總召集人及協同總召集人為當然委員外，其餘委員，由總召集人就推動資通安全有關機關之副首長及學者、專家聘兼之。

四、 本會報置執行長一人，由本院科技顧問組執行秘書兼任，承總召集人之命，綜理本會報有關業務；置副執行長三人，分別由本院主計處電子處理資料中心主任、國防部派員及本院研究發展考核委員會資訊管理處處長兼任，襄助執行長綜理本會報有關業務；本會報幕僚作業，由綜合規劃組負責。

五、 各工作組得置召集人一人，由主責機關之委員擔任之，並依需要訂定各組作業規範。

六、 本會報為廣徵產學研各界學者專家意見，得設國家資通安全諮詢小組，以有效推動資通安全相關工作，其作業注意

事項另定之。

七、 本會報總召集人、協同總召集人、執行長、副執行長、委員及各組召集人，均為無給職。

八、 本會報應定期（每半年至少一次）召開會議，審核及評估資通安全政策；有重大議題時，得視業務需要召開臨時會議。

貳、 行政院國家資通安全會報下各單位職掌

一、 綜合規劃組（辦理單位：本院科技顧問組主責、本會報下各工作組配合協辦）

(一)國家層級資通安全基礎建設政策規劃作業。

(二)負責資通安全會報相關行政協調作業綜合業務。

(三)統合推動通資訊安全基礎建設工作及協調組織運作業務。

(四)負責資通安全計劃管理與考核。

二、 通報應變組（辦理單位：本院研考會主責、各機關配合協辦）

(一)建立資通安全事件通報處理程序。

(二)建置資通安全事件通報網站。

(三)建立資通安全事件各安全等級之有關緊急應變程序。

(四)處理資通安全通報事件及緊急應變。

(五)建立事前、事中及事後各項資通安全事項通報預警及應變復原機制。

(六)統計發布我國資通安全事件及應變程序。

三、 資訊服務組（辦理單位：本院國科會主責、中科院、工研院、資策會、相關公協會及民間業者配合協辦）

(一) 蒐集、分析國內外資通安全相關資訊。

(二) 建置資通安全資料庫。

(三) 傳布及推廣資通安全資訊並主動提供服務。

四、 法規偵防組（辦理單位：法務部主責、內政部、國防部、國家通訊傳播委員會配合協辦）

(一) 指派人員負責資通安全犯罪事件偵查工作。

(二) 培訓執法人員辦理資通安全有關偵防能力。

(三) 建立跨國及區域性合作偵防機制。

(四) 配合研修網路犯罪相關法規。

五、 稽核服務組（辦理單位：本院主計處電子處理資料中心主責、國防部、交通部、經濟部、財政部配合協辦）

(一) 培訓資通安全稽核人力。

(二) 協助各機關訂定作業系統安全等級。

(三) 選定資通安全等級高之作業系統。

(四) 每年對重要系統不定期辦理資通安全稽核作業。

(五) 彙編重要系統資通安全稽核報告。

六、 標準規範組（辦理單位：經濟部主責、本院研考會、國防部、交通部、國家通訊傳播委員會、財政部配合協辦）

(一) 訂定資通安全技術標準。

(二) 訂定各機關辦理資通安全有關作業規範。

(三) 規劃建置資通安全驗證方法。

(四) 規劃建置資通安全認證程序。

參、 行動方案執行要點與績效指標說明表

行動方案	執行要點	績效指標	主（協）辦單位
1. 提升通報時效	(1) 檢視通報與應變架構，強化緊急應變機制，落實分級分工原則。 (2) 對資安防護人員強化即時資安資訊分享。	每年檢討資安事件通報與應變機制。	行政院研考會（各機關）
2. 建立資安事件管理與回應程序	建立應變作業相關程序（含事件偵測、識別及分析與回應等）。	99 年底前完成應變作業相關程序。	行政院研考會（各機關）
3. 持續發展緊急應變及復原能力	(1) 強化國家資安防護管理平台功能。 (2) 建立資安事件研究能力。 (3) 掌握緊急資安事件發生趨勢。 (4) 探究資安事件發生原因，建立改善計畫並重新評估風險。 (5) 落實資安演練計畫，定期測試並精進資安事件管理與回應程序。	(1) 每年辦理 1 次資安演練。 (2) 各機關配合資安演練，每年至少辦理一次內部演練，並執行改善計畫。	行政院研考會（各機關）
4. 訓練資安事件回應人力	(1) 組織、訓練與整備資通安全處理小組，並視需要成立資安服務團，協助因應資安事件。 (2) 加強緊急應變教育訓練、講習活動及研討會。	每季辦理 1 次通報應變會議，加強緊急應變教育訓練。	行政院研考會（各機關）
5. 發展與維護政府機關資安作業規範與參考指引	(1) 檢視修正發展藍圖。 (2) 依優先順序逐年訂定資安作業規範與參考指引，並積極推廣運用與評估成效。	(1) 98 年底前完成政府資安作業共通規範發展藍圖檢討及修正。 (2) 依據修正之政府資安作業共通規範發展藍圖，逐年訂定資安作業規範與參考指引。 (3) 每年辦理 6 場次資安作業參考指引訓練。	行政院研考會（各機關）
6. 推動資安治理	(1) 由副首長擔任 CISO。 (2) 強化資安組織功能。 (3) 明確資安預算。 (4) 強化政風聯繫協調機制，發揮資安稽核人員功能。 (5) 定期評估與陳報執行成效 a. 評估資安治理成熟度。 b. 研訂具體改進措施。 c. 分級訂定資安治理績效評估準則，擇績效良好單位給予獎勵。 (6) 依機關資安等級分期推動實	(1) A 級機關導入資安治理比例：98 年達 30%；99 年 70%；100 年 100%。 (2) B 級機關導入資安治理比例：99 年達 30%；100 年 70%；101 年 100%。 (3) 資安治理成熟度提升比率。（導入機關自訂） (4) 資安演練防禦成功率上升比率。	行政院科技顧問組（行政院研考會、行政院主計處、各機關）

行動方案	執行要點	績效指標	主（協）辦單位
	施。 備註：導入資安治理參考原則： (1) 由 CISO 每年主導進行一次資安治理成熟度評估，與資安處理小組共同檢視資安計畫成果，並向首長陳報績效。 (2) 組織應落實資安計畫，包含： a. 將資訊資產風險評估視為整體風險管理專案之一部分，定期加以評估，並根據評估結果制定資安政策與程序，且據以實施。 b. 建構內部資安管理架構，明確賦予每個人相對應的權責。 c. 將資安視為系統正常運作要素，針對網路、設施、系統、資訊等發展資安保護行動計畫，建立業務持續運作計畫、事件回應程序，並進行演練。 d. 對員工進行資安認知宣導與教育訓練。 e. 定期測試與評估資安政策與程序之有效性，並針對資安缺失提出矯正措施。 (3) 採用最佳資安實務指引（如 ISO27002（CNS27002））衡量資安成果。		
7. 推動資訊與資訊系統分類分級	(1) 整合機關、資訊及資訊系統之分類分級作法。 (2) 建立分類分級標準，設定基本資安防護需求水準。 (3) 對資訊與資訊系統進行分類分級鑑別，並要求達到最基本的資安防護需求。	(1) 98 年建立分類分級標準，99 年設定基本資安防護需求水準。 (2) 99 年 A 級機關完成資訊與資訊系統鑑別。 (3) 100 年 B 級機關完成資訊與資訊系統鑑別。 (4) 101 年由主管機關自行列管所屬各級資訊系統達到基本資安防護需求。	行政院科技顧問組（行政院研考會、各機關）

行動方案	執行要點	績效指標	主（協）辦單位
8. 強化電子化政府資通安全，落實公務資料保護	(1) 優化政府資安組織與架構。 (2) 強化電子化政府資訊通信技術之平台與應用安全。 (3) 建立政府安全資訊網路，強化骨幹網路系統安全。 (4) 訂定公務資料保護管理規定，強化蒐集於各機關之個人資料資料庫的安全維護，及資訊系統管理，含在作業流程上、資料經手人員的訓練管控及資訊委外管理上，皆訂有嚴謹的作業準則與稽核方式。 (5) 協助各機關有關保護個人資料之法制作業與提供法律諮詢。 (6) 公務涉及蒐集、處理、利用個人資料之機關，由專責人員或單位，負責個資保護之教育宣導、投訴處理及主動督察的工作。	(1) 98 年底前完成政府機關推動電子識別證-結合自然人憑證及識別證作為公務系統使用之規劃。 (2) 每年完成 4 個重要電子化政府資訊系統滲透測試。 (3) 98 年底前相關機關訂定保護個人資料之管理規則，且由專人或專責單位加以落實。前揭規則並配合「個人資料保護法」立法進程，於一定時間內完成修正。	行政院研考會（法務部、各機關）
9. 推動政府機關（構）採購符合安全驗證之資通訊設備	(1) 建立資通安全之機敏裝備項目。 (2) 辦理資通安全驗證作業訓練。	(1) 建立政府機關優先採購經驗證之資通設備項目。 (2) 資通設備驗證審驗作業訓練每年兩場次。	國家通訊傳播委員會（行政院研考會、公共工程委員會、各機關）
10. 充實資安人力	(1) 各機關依需求配置資安人力。（參考原則：A 級單位設置資安專責 2 人（含以上），B 級單位設置資安專責 1~2 人（含以上），C 級單位設置資安兼辦 2 人（含以上），D 級單位設置資安兼辦 1 人（含以上）。） (2) 研議資安人才進用之配套措施（考量於公務人員考試「資訊處理」類科增設資訊安全相關應試科目/專技人員轉任）。	98 年底前資安等級列為 A 級之中央部會配置資安專責人力 2 人。	行政院人事行政局、行政院研考會（銓敘部、考選部、各機關）
11. 提升資安防護技術與服務品質	(1) 依需求提供政府機關資安技術服務。 (2) 定期或視需要彙整與發布資安警訊。	(1) 每年執行 1 次服務需求改善調查。 (2) 每年至少發布 500 則資安警訊。	行政院研考會

行動方案	執行要點	績效指標	主（協）辦單位
12. 強化資安素養與能力培訓	(1) 充實資安（管理/技術）課程，開辦資安教育訓練。 (2) 推動資通安全專業證照培訓工作。 (3) 辦理資安技能競賽。	(1) 每年辦理 12 場次資安巡迴講習、4 場次資安專業技術訓練。 (2) 每年辦理 4 場次資安專業證照訓練。 (3) 每年辦理 1 次資安技能競賽。	行政院研考會
13. 加強資安稽核與推動資訊安全管理系統驗證	(1) 各機關定期進行資安內部稽核。 (2) 選定政府機關實施資安外部稽核，評估檢討受稽單位落實程度且進行持續改善。 (3) 推動各機關依需求建置資訊安全管理系統，並選定核心業務為驗證範圍。	(1) 各機關於年度內擇期辦理資安內稽至少一次。 (2) 於年度內選定27個重要單位實施資安外部稽核。	各機關（行政院主計處）
14. 發展關鍵資訊基礎建設保護策略	(1) 建立各關鍵基礎建設領域資安預防與早期預警、偵測、反應、危機管理能力。 (2) 規劃與設計網際網路接取服務提供業者（IASP）聯盟與通報處理作業機制，並建置電信網路「資訊安全通報處理平台」，包括通報資訊共享平台、資訊分享介面及入口網站。	金管會： (1) 定期進行證券期貨市場集中交易系統關鍵基礎建設資安風險評鑑。（每年 1 次）。 (2) 定期執行證券期貨市場集中交易系統關鍵基礎建設異地備援演練。（每半年 1 次）。 (3) 推動證券期貨市場集中交易系統關鍵基礎建設資訊安全監控中心（SOC） 與國家資訊安全監控中心（NSOC）連線分享資安資訊。(每年至少測試 1 次)。 經濟部（國營會）： (4) 97 年底完成重要民生基礎建設資安資訊分享與分析中心（電力、油氣、自來水部分）建置作業。 (5) 98 年起逐年編列管理與維護預算，持續維運資安資訊分享與分析中心。 教育部： (6) 區網中心於 98 年完成 ISAC 建置。 國家通訊傳播委員會： (7) 於 98 年建置完成電信網路「資訊安全通報處理平台」；99 年起逐年編列管理與維護預算。	金管會、經濟部、交通部、衛生署、教育部、國家通訊傳播委員會、行政院研考會

行動方案	執行要點	績效指標	主（協）辦單位
15. 強化電子商務信賴安全	(1) 加強線上交易安全身分認證機制。 (2) 推動運用公開金鑰基礎建設（PKI）憑證服務。 (3) 建立信賴驗證服務機制（資訊透明化、隱私權保護）。	經濟部（商業司）： (1) 輔導網路 200 家商店應用線上身分認證機制。 (2) 建立20個商業交易安全認證示範應用體系，完成10種不同行業（如流通業、網購業等）之輔導。 (3) 預計99年完成非公務機關線上隱私權保護標章或認證機制資料蒐集與研究。 金管會： (4) 執行信用卡電子商務特約店網路弱點掃描（98年完成網路弱點掃瞄規劃，99年起每季進行一次掃瞄）。 (5) 推動證券商及期貨商與證券期貨集中交易系統使用公開金鑰基礎建設（PKI）憑證服務（證券期貨交易網路下單作業使用CA 憑證進行身分安全認證）（98 年運用率 30%、99 年50%、100 年 70%、101 年 90%） (6) 設置證券期貨市場投資人服務專線，辦理客服及接受投資人申訴，並每月製作客訴處理表陳報簽核。（98年完成專線建置，99年起每月至少辦理1次客訴處理表）	經濟部、行政院金管會（行政院公平會、行政院消保會、內政部、國家通訊傳播委員會、法務部）
16. 依法規授權，促進事業機構運用第三方評鑑	(1) 對目的事業加強資安查核措施，促使業者研擬強化個資保護作為。 (2) 推動各目的事業單位建立資安內部稽核制度並落實執行。 (3) 推動資通安全成為企業內稽內控循環之一。 (4) 指導各目的事業單位委由公正第三者進行資通安全外部稽核。	金管會： (1) 持續推動銀行跨行交易系統、證券期貨集中交易系統關鍵基礎建設 ISO27001 認證之有效性。（每年1次） (2) 辦理聯合信用卡處理中心、金融聯合徵信中心 ISMS 第三方驗證。（信用卡處理中心98年完成驗證、聯合徵信中心 100年完成驗證） (3) 定期檢查證券商及期貨商資通安全實際執行、追蹤、改善情形。（每年1次） 衛生署、國家通訊傳播委員會： (4) 已建立內部稽核制度並落實執行之事業機構數量。 (5) 事業機構委由公正第三者通過	金管會、衛生署、國家通訊傳播委員會、經濟部（指標併方案17）、教育部（指標併方案23）

行動方案	執行要點	績效指標	主（協）辦單位
		資安驗證之數量。 國家通訊傳播委員會： (6) 於 98 年度辦理所有固網業者「個人資料保護辦理情形檢查」。	
17. 促使業者發揮自律精神，善盡資安社會責任	(1) 鼓勵業者訂定資安自律準則。 (2) 促使業者重視資通安全。	經濟部： (1) 印製資通安全自我檢核表 5,000 份發送予流通業，促使業者重視自身資訊安全。（商業司） (2) 每年對製造業內廠商舉辦資通訊安全認知宣導 3 場次。（工業局） (3) 印製資通安全自我檢核表，發送製造業或置於局網站供其下載，以促使業者重視本身資訊安全。（工業局） (4) 經濟部能源局每年輔導至少 3 家業者建立及完善資安制度。（能源局） (5) 印製發送中小企業資通安全自我檢核表 5,000 份，促使業者重視自身資訊資產安全。（中小企業處） (6) 每年至少辦理 2 場宣導會並做問卷調查。（加工口區管理處） 金管會： (7) 辦理證券期貨市場資通安全之宣導教育之場次及人次。（每半年 1 場次） 交通部： (8) 輔導「待檢廠」及「駕訓班」，每年辦理 2 次資安宣導。（公路總局） (9) 輔導轄區航商貨主，每年至少辦理 1 次資安宣導。（港務局） (10) 印製有關網站、資料及資訊安全維護管理相關注意事項 5,000 份，發送各旅行業者，宣導業者重視自身資訊安全及建立完善資安制度。（觀光局） 衛生署： (11) 辦理業者資安防護推廣研討會之場次數量。	經濟部、金管會、交通部、衛生署

行動方案	執行要點	績效指標	主（協）辦單位
18. 發展資通安全產品與管理系統之認驗證標準及體系	(1) 研擬、訂定及推廣有關標準。 (2) 積極參與並申請加入國際組織、掌握國際趨勢，與國際認驗證體系相互承認。 (3) 訂定國內急迫需要之資通安全技術規範。 (4) 與國際接軌，訂定資通安全共同準則（Common Criteria）相關技術規範中文版。 (5) 建立驗證機構的組織與人員管理規範。	經濟部（標檢局）： (1) 每年制定完成資通安全相關標準 5 種。 國家通訊傳播委員會： (2) 資通安全共同準則規範新版公布後二年內完成中文版公告。	經濟部標檢局、國家通訊傳播委員會（相關部會及目的事業主管機關）
19. 強化國家資安研究能量	(1) 研發關鍵資通安全技術，推廣研發成果，帶動產業發展。 (2) 建立資安科技研發合作與成果擴散平台。 (3) 吸引與凝聚國內外優秀人才。 (4) 利用全球資源提高資安科技自主研發創新能力。	國科會： (1) 論文篇數（資訊安全優良論文期刊發表篇數增長） (2) 人才培育 （培育資訊安全博、碩士生人數） 經濟部（技術處）： (3) 研發關鍵資通安全技術，提供產業加值應用，每年達成技術移轉 2 件。 (4) 掌握重要核心技術智財權，每年提出專利申請 2 件。 (5) 研發資安監控與偵測防護關鍵技術，完成相關系統及平台 2 個。 (6) 協助運作資安廠商結盟 1 件。 (7) 服務重點資安廠商 5 家。 (8) 合作參與/協辦資安技術研討會或成果發表會 5 場次。 (9) 與國際知名資通安全研究機構進行技術合作交流，預計每年 2 案。 國防部： (10) 研發國防資安科技。 (11) 參與產官學界資安科技關鍵技術研究。 (12) 資安人才培育（博、碩、學士）。 (13) 發表國際資安論文。 (14) 參與國家（際）級資安研討會。	國科會（基礎研究）、經濟部（產業技術與推動）、國防部（國防資安科技研發）
20. 建構資安人才培育體系	(1) 鼓勵高教體系培育資安專業研究人力。 (2) 建構技職體系資安人才培育課程，培育高級資安技術人才。	(1) 鼓勵技專校院辦理 1 場資安人才培育研討會。 (2) 大學校院相關科系資安課程開設數達 10%。	教育部

行動方案	執行要點	績效指標	主（協）辦單位
21. 檢討修訂國家資通安全相關法規	(1) 推動「個人資料保護法」完成立法。 (2) 依上開新修法規授權指定保有大量且重要之個人資料檔案的非公務機關，訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 (3) 訂定前項計畫及處理方法之標準等相關事項之辦法。 (4) 檢討修訂國家資通安全執法工作相關法規。（含數位證據的相關法令） (5) 訂定電信業者資通安全管理之相關法規或行政配套措施。	(1) 積極推動「個人資料保護法」儘速完成立法，並配合修正施行細則。 (2) 配合「個人資料保護法」立法進程，訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法之標準等相關事項之辦法。 (3) 法規完備度。	法務部、目的事業主管機關、國家通訊傳播管理委員會
22. 持續發展數位鑑識能量	(1) 訂定電腦鑑識程序與標準。 (2) 培訓專業鑑識人員，加強鑑識科學之學習（軍、檢、警、調偵查人員具備足夠的鑑識能力）。 (3) 進行國際交流合作。	內政部： (1) 研訂警察機關電腦數位證據現場處理標準程序。 (2) 每年協助破獲各類刑案 20 件。 (3) 每年至少辦理 2 場次電腦鑑識專業講習。 法務部： (4) 訂定電腦鑑識程序與標準，完成現場搜索電腦鑑識程序。 (5) 每年辦理專業鑑識工具講習兩次，如 Encase、FTK，由職司鑑識人員參加，受訓人數 10 人。 (6) 委託或自行開發適合現場簡易蒐證之工具乙套並辦理講習，受訓人數 40 人以上。 (7) 每年協助各類刑案資安鑑識報告 50 件。 (8) 每年協助各類刑案現場搜索 40 件。 (9) 每年派員參加相關國際研討會 4 人次。 (10) 邀訪外國學者專家來台講習 2 次，以利與國際接軌。 國防部： (11) 人員參與基礎/專業數位鑑識課程。 (12) 建置數位鑑識實驗室（人力、設備（軟、硬體））。 (13) 參與法務部（調查局）或內政部（警政署）數位鑑識科技（課程）交流。 (14) 參與國家（際）級數位鑑識研	內政部（警政署）、法務部、國防部

行動方案	執行要點	績效指標	主（協）辦單位
		討會。	
23. 推動教育體系資通安全計畫	(1) 推動教育體系資安分級計畫。 (2) 推動各級學校資訊倫理教育與資通安全認知推廣活動。 (3) 健全教育部資通安全推動組織。 (4) 輔導教育機構建置資訊安全管理制度。 (5) 強化教育機構資安專業技術及管理能力。	(1) 推動各縣市辦理中小學教師資訊素養（網路倫理、智慧財產權、資訊應用安全）培訓，每年培訓 3 萬人次。 (2) 規劃推動學術機構專屬資訊安全管理規範及驗證制度。 (3) 培訓學術機構資安主導稽核員及資安專業證照數 4 年 400 人次。	教育部
24. 提供全方位資安資訊服務	(1) 蒐集、分析與傳布國內外資通安全相關資訊，擴充資安資料庫，主動提供政府機關及民間機構各項資安資訊服務。 (2) 出版資通安全專論，並舉辦相關研討會。	國科會（政策研究中心）： (1) 資料蒐集每年 10,000 筆。 (2) 網站點擊數每年 4,000,000 人次。 (3) 資安專論每年 25 篇。 (4) 每年舉辦 2 次研討會。	國科會
25. 整合資安資源之訊息，分眾加強宣導	(1) 結合民間力量，針對特定主題（個人資料保護、資安法律...），分眾加強宣導。 (2) 運用創新作法，強化宣傳綜效。（網站、活動）	(1) 每年辦理一次全民資安健檢活動，達成 10,000 人次健檢。 (2) 提升民眾對資安認知程度。	行政院科技顧問組、行政院研考會、各機關
26. 規劃依資安策略需要而運作的新型組織。	(1) 依功能彈性調整行政院國家資通安全會報組織架構。 (2) 配合行政院組織改造，規劃設置資安專責主管機關。		行政院科技顧問組、行政院研考會
27. 鼓勵讓資源發揮最佳效益的創新作法	(1) 辦理政府機關（構）資安最佳實務競賽。 (2) 鼓勵各機關針對資安提供創新作法，經評選優良者給予獎勵。	(1) 98 年完成資安最佳實務競賽辦法。 (2) 99~101 年每年辦理一次政府機關（構）資安最佳實務競賽。	行政院科技顧問組、各機關
28. 促進有效的團隊合作	(1) 加強各機關彼此間的聯繫與合作，發展跨部會合作專案。 (2) 建立政府與民間合作夥伴關係。	(1) 視議題需要召開跨工作組談話會議。 (2) 定期（原則每 2 個月）召開工作小組會議。	行政院科技顧問組、行政院研考會（各機關）
29. 促進國際合作	(1) 參與國際會議，交流分享最新資安訊息與經驗。 (2) 積極爭取參加跨國或區域偵防機制，適時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。 (3) 積極參與國際合作，防制垃圾	法務部： (1) 每年定期參與資安相關國際會議（如執法專業國際會議），加強與資安相關國際組織聯繫互動。 (2) 積極爭取參加跨國或區域偵防，建立中繼站通報，促進國	行政院科技顧問組、行政院研考會、法務部、內政部（警政

行動方案	執行要點	績效指標	主（協）辦單位
	郵件氾濫。	際合作，共同打擊電腦／網路犯罪。 (3) 積極建立國際合作交流窗口，交換駭客偵查、網路犯罪趨勢等情報。 內政部警政署： (4) 每年定期參與資安相關國際會議（如執法專業國際會議1場次等），加強與資安相關國際組織聯繫互動。 國家通訊傳播委員會： (5) 每年定期參與國際會議（倫敦行動計畫）以了解國際於防制垃圾郵件之趨勢。	署）、國家通訊傳播委員會、各機關
30. 調查與發布資安關鍵指標	(1) 發布年度資安關鍵指標報告。 (2) 持續發展資安關鍵指標系統與國際接軌。	每年一次調查與發布資安關鍵指標	行政院科技顧問組、行政院主計處