國家資通安全發展方案
(106 年至 109 年)

行政院國家資通安全會報

中華民國 108 年 4 月修正

目錄

壹、 緣起

我國自 90 年開始推動資通安全(簡稱資安)基礎建設工作，迄今歷經四個推動階段，已完成諸多階段性里程碑，包括：完成政府機關資安責任等級分級機制、推動行政機關資訊安全長制度、成立國家級資安監控中心、建立資安事件通報應變機制、建立政府資安聯防監控與資安情報分享機制等，已有效提升我國資安完備度。第四期國家資通安全發展方案(102 年至 105 年)業於 105 年屆期。

近年來，數位經濟帶動產業朝跨世代、跨境、跨領域、跨虛實等趨勢發展，促使全球產業格局翻轉，加上隨著數位經濟與物聯網(Internet of Things, IoT)時代的來臨，為建構完善的產業生態體系(ecosystem)及加速產業創新與優化產業結構，行政院提出「數位國家・創新經濟發展方案(2017-2025 年)」(簡稱 DiGi^{+})。爰下一階段國家資通安全發展方案之推動，需從資通安全的角度，確保數位國家安全，推動 DiGi^{+}方案「友善法制環境」、「跨域數位人才」、「先進數位科技」等三項數位國家基磐配套措施，進而打造安全可信賴的「數位創新基礎環境」及「網路社會數位政府」。

綜上，行政院國家資通安全會報(簡稱資安會報)提出「國家資通安全發展方案(106-109 年)」(簡稱本方案)，期透過前瞻、宏觀的視野，提出國家級的資通安全上位政策，以因應我國特殊的政經情勢及全球複雜多元的資通訊變革，並作為國家推動資安防護策略與計畫之重要依據。

貳、 全球資安威脅與國際政策趨勢

一、 全球資安威脅趨勢

依據世界經濟論壇(World Economic Forum, WEF)「全球風險報告」顯示，在106年全球可能風險排名中，資料欺詐或盜竊名列第5名，大規模網路攻擊則名列第6名，可見資安風險已深深影響人類的生活。

（一）資料欺詐或盜竊

根據身分竊盜資源中心(Identity Theft Resource Center, ITRC)的統計數據顯示，截至106年6月30日美國年度資料外洩事件已高達791筆，與105年同期相較增加了29%，創歷史新高。ITRC並預測，106年底資料外洩筆數將高達1,500筆，較105年的1,093起(累計多達3,660萬筆資料遭竊)增幅37%。而資料外洩之主因為駭客攻擊，包括勒索軟體(Ransomware attack)、網路釣魚(Phishing attempt)、員工疏失及意外曝露(employee error and accidental exposure)等。

近年資安外洩最嚴重的案例為102年美國知名入口網站系統遭駭客入侵，累計個資外洩筆數達30億筆，這其中包含我國人的個資在內。根據賽門鐵克(Symantec)106年4月的網路資安報告顯示，我國資料外洩程度居全球第5名，更高居亞洲榜首，且5月份亦發生史上最大宗個資外洩案，資料外洩筆數高達1.7億筆，顯示資料欺詐或盜竊威脅，已成為維護個人安全及社會安全不容忽視的嚴峻課題。

（二）大規模網路攻擊

根據卡巴斯基(Kaspersky)105 年第 4 季釋出的報告指出，有 80 個國家的殭屍網路參與分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)，其中發起攻擊的多為 IoT 設備組成的殭屍網路，且攻擊強度有持續提高的趨勢，攻擊規模甚至提升到 Tb 級。隨著 Mirai 攻擊程式釋出，預料 IoT 設備將發起更複雜的 DDoS 攻擊，包含應用層與加密類型的攻擊。

值得注意的是，許多 DDoS 攻擊背後真正的目的，是為了發動進階持續性滲透攻擊(Advanced Persistent Threat, APT)，以竊取公務或商業機密，因此，遭到 DDoS 攻擊同時，也需留意其他資安告警。此外，106 年農曆春節期間，我國若干券商遭勒索比特幣並發動 DDoS 攻擊事件，經由此案例也凸顯駭客攻擊模式已朝向產業化方向發展。

（三）關鍵資訊基礎設施無法正常運作

越來越多關鍵基礎設施(Critical Infrastructure, CI)的監視控制與資料擷取系統(Supervisory Control And Data Acquisition, SCADA)因有遠端操控系統的需求，紛紛採用開放的連網架構，徜本身的安全性未提升到足以抵禦駭客攻擊的程度，一旦遭到入侵或破壞，可能會對民生經濟甚至國人生命安全造成相當程度的損害。例如：104 年烏克蘭伊萬諾-弗蘭科夫斯克州的電網控制中心遭利用魚叉式網路釣魚(Spear Phishing)方式入侵，造成大停電事件。

行政院國土安全辦公室現階段定義攸關國家安全與民眾

福祉的關鍵基礎設施包括：中央與地方政府、能源、水資源、高科技園區、通訊傳播、交通運輸、銀行與金融、緊急救援與醫院等 8 大領域。根據 105 年，卡巴斯基實驗室專家針對工業控制威脅進行調查，發現全球有數千臺主機暴露在網際網路上，其中更有高達 91.1%的主機存在遠端控制的漏洞。此資訊對廣泛使用工業控制系統(Industrial Control System, ICS)的關鍵基礎設施提供者，無疑是一大隱憂，尤須加強防範機制。

（四）科技進步的負面效應

隨著新興資訊科技的快速變革，駭客的攻擊手法也因應這些轉變做調整。未來，需加強新興資訊科技的安全防護機制，例如：

1. IoT 設備：從近期的 DDoS 攻擊案例中發現，攻擊手法多為混合式攻擊，發動來源以 IoT 設備為主。據 Gartner 公司預測，105 年有 64 億個 IoT 設備連網，109 年將高達 208 億個 IoT 設備連網。一旦疏忽考量 IoT 的安全設計與威脅，將使得這些設備為駭客所利用，對全球資安產生更嚴峻的威脅。
2. 行動裝置：軟體公司 Check Point 發現，由行動裝置衍生的資料外洩事件，將成為重要的安全問題。尤其是受國家支援的組織型駭客，將使得這類攻擊手法在全球蔓延。
3. 雲端運算：隨著越來越多的政府機關與企業組織採用公有雲或私有雲等雲端運算架構，儲存更多資料，這類資訊架構也將成為駭客攻擊的目標，藉由加密檔案在不同的雲間

傳播，把雲端運算架構當成是擴大攻擊效果與範圍的工具。

4. 無人載具：近年，隨著各種新興智慧科技的蓬勃發展，無人載具也被廣泛應用，包括：常見的智慧機器人載具、無人飛行載具（UAV)、無人地面載具（UGV）與無人水域載具（UMV）等類型，其資安議題也被密切關注。以 UAV 為例，兼負全國供電重任的電力公司近年為避免飛航事故，開始推動運用無人機於清掃電塔礙子用途，惟這些無人機雖為國內廠商所製造，但可接收北斗衛星導航系統訊號，此現象對國家安全具高度風險，不容忽視。

另一項令各國政府及社會高度關注的議題為會影響社會秩序及安全的暗網(Darknet)與深網(Deep web)，其為許多不法份子的溫床，凡舉駭客工具、槍支販賣、毒品交易等非法訊息都會出現，因此各國檢調單位都相當注意。106 年 7 月，美國、加拿大及泰國即曾聯手攻破全球最大的暗網黑市「AlphaBay」。

二、 國際資安政策發展趨勢

資訊科技改變了世界，也打破了國土的界線，成為國際間重要的科技議題。本節綜整研析世界主要國家針對網路攻擊模式演變所提出的因應對策，以作為未來四年研提我國資安上位政策之參考。

（一）美國之資安政策發展

美國於 2002 年成立「國土安全部(Department of Homeland Security, DHS)」，以回應恐怖主義的威脅並強化

關鍵基礎設施的保護，並通過「聯邦資訊安全管理法」(Federal Information Security Management Act of 2002, FISMA)，要求各聯邦政府機關都必須發展、制定及執行全機關的資訊安全計劃,每年也要針對資訊安全控管政策、程序、實務等面向進行測試與評估，以提供組織與其利害關係人資訊安全保障。

2013 年歐巴馬總統為強化關鍵基礎設施的復原能力，簽署「改善關鍵基礎設施之網路安行政命令」行政命令(Executive Order 13636—Improving Critical Infrastructure Cybersecurity)，要求美國商務部「國家標準技術研究所」(National Institute of Standard and Technology, NIST)，研議提升關鍵基礎設施資通訊安全之架構（Framework to Improve Critical Infrastructure Cybersecurity)，將美國聯邦憲法所保障的企業商業機密、個人隱私權和公民自由等法益納入考量。

2014 年調修 FISMA 並更名為「美國聯邦資訊安全現代化法」(Federal Information Security Modernization Act of 2014, FISMA 2014)，修法重點有：(1)要求對資安事件進行通報，(2)授權給國土安全部部長，使其協助預算局局長共同進行各機關之監督管理，(3)要求資訊系統內之資料實際受到侵害時應有相關處置，(4) 調整各機關提出年度報告之內容。此調修顯示美國資通安全政策重點由電子化政府之資通安全，擴張至國土安全議題。

2015 年通過「網路安全資訊分享法」(Cybersecurity

Information Sharing Act, CISA)修正案，更名為「網路安全法」(Cybersecurity Act of 2015)。此法著重於資訊分享，鼓勵企業主動分享情資，以獲得早期預警資料。同時允許 ISP 業者，可在資訊安全防護目的下，監控企業的網路系統。該法並指定由國土安全部建置網路威脅情資平臺，蒐集並分享威脅情資與預警訊息，以降低關鍵基礎設施的資安風險。

為了提升政府、民間企業及民眾生活的網路安全，美國於 2016 年提出「國家網路安全行動計畫」(Cybersecurity National Action Plan, CNAP)，其重點包括：

1. 策略性整合近期的資訊安全計劃，以綜合的觀點看待並處理公私部門與個人所面臨的資訊安全議題。
2. 採取短期行動，並制定長期策略來提升網路安全意識和防護、保護隱私、維護公共安全以及經濟和國家安全，並賦權予美國人民，讓他們更能掌控自己的數位安全
3. 以資訊科技現代化基金及聯邦資訊安全總長的設置來改革政府管理資訊安全的方式。
4. 以附加安全工具，如多因子認證等來賦權一般民眾，以增加其線上帳號以及金融交易的安全性。
5. 提供聯邦政府跨部會的既有資訊安全與資訊科技再檢視措施。
6. 投入 190 億美元預算在資訊安全的業務上，這相較 2015 年的資訊安全預算增加了 35%。
7. 重申美國應採取「負責任之國家行為原則」來領導國際資訊安全維護行動。

2016 年亦依第 41 號「美國資安事件協調總統政策指令」(Presidential Policy Directive--United States Cyber Incident Coordination, PPD-41)制定「國家資安事件回應計畫」(The National Cyber Incident Response Plan, NCIRP)，用以清楚說明國家在關鍵基礎設施遇重大資安事件時的回應與復原上所扮演的角色、應負的責任與協調架構。

2017 年川普總統上任後，則公布「強化聯邦網路與關鍵基礎設施網路安全」總統命令(Presidential Executive Order: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure)，要求各聯邦機關首長應使用改善關鍵基礎設施網路安全框架，管理該機構的網路安全風險。關鍵基礎設施威脅資訊分享框架指南是用來協助關鍵基礎設施的所有者與營運者、其他私部門、聯邦政府、州政府與地方政府等合作夥伴，分享人為攻擊的威脅情資，並學習接收與報告威脅情資。

（二）日本之資安政策發展

日本於 2005 年通過「關鍵基礎設施資訊安全策略行動計畫」，計畫中規劃關鍵基礎設施[1]資訊安全確保的安全基準指導指南、強化資訊共享機制、分析各領域關鍵基礎設施相依性、跨關鍵基礎設施領域的演習，以及資訊安全基礎的建構與國際合作等五大項目，目的在於當關鍵基礎設施遭受攻擊而發生運作障礙時，盡可能繼續提供服務，並從事故中迅速恢復，避免對國民生活與社會經濟造成重大影響。

[1] 2005 年日本關鍵基礎設施領域為：資通訊電信、金融、航空、鐵路、電力、天然氣、政府與行政服務(包含地方自治團體)、醫療、水資源與運輸等。

2009 年，日本政府曾提出「關鍵基礎設施資訊安全策略第 2 次行動計畫」，用於持續活用與發展新公私協力模式。但由於該行動計劃策定後，2011 年發生東日本大地震且針對日本政府與重要關鍵基礎設施 IT 系統(含工業控制系統)的網路攻擊持續發生，因此在 2012 年提出第 2 次行動計畫改定版，以回應整體環境變化，主要增加處理 IT 事故與 IT 功能不完全的對策，以避免關鍵基礎設施的 IT 事故影響國民生活與社會經濟活動。

2014 年，通過「網路安全基本法」，針對關鍵基礎設施提供者的資訊安全維護相關事項，要求其訂定安全標準、進行跨領域演練，並推動各部會、地方政府、關鍵基礎設施提供者及網路安全產業間進行資訊共享與相關合作。

2015 年制定「關鍵基礎設施資訊安全策略第 3 次行動計畫改訂版」，增加維持關鍵基礎設施服務持續提供的目的，讓防護目的更加明確化，並增加化工、信用卡與石油 3 類新領域，及提出五大對策，包括：安全基準的整備與提升、資訊共享框架的強化、事故應變框架的強化、風險管理，及防護基礎的強化。

2015 年公布「網路安全策略」，其重點包括：(1)強化社會經濟活力與持續性發展，(2)為民眾建立安全的社會，(3)確保國際社群與國家安全的和平與穩定性，(4)強化網路安全相關的研發以及人力發展。

2016 年則通過「物聯網系統安全之一般架構」，旨在確保物聯網系統的安全性、機密性、整全性，以及可得性，並

就所有物聯網的設計、發展與營運提出一般要求；另就個別部門的特性提出相應的要求。並提出以下政策：(1)在加入物聯網前，應先確認相關的法規明文之要求、或其他非明文但屬於不可或缺要求，以及業界認為重要的其它要求，並且對其加以妥善執行；(2)分析每一物聯網階層，進行模組化，並以這些模組為基礎進行安全評估；(3)進行常規風險評估，並提出因應相關風險的對策；(4)釐清相關人的角色並促進其合作。

為了持續維持日本國內以及與東京奧運舉辦相關的關鍵基礎設施服務的安全性，日本內閣網路中心於 2017 年 4 月 19 日公布「關鍵基礎設施資訊安全對策第 4 次行動計畫」，除持續檢討並改善第 3 次行動計畫原有政策外，較重要的變革為 OT(Operation Technology)的重視與風險對應機制整備。在安全基準整備與落實情況方面，要求關鍵基礎設施產業須將 OT 的觀點融入人才培育。在資訊分享制度方面，分享的資訊範圍應包含 IT、OT 與 IoT 的資訊，並排除資訊分享的障礙。而在風險管理部分，日本從功能保證的觀點出發，新增風險情況對應準備的要求，包含事業持續計畫的提出與緊急應變措施的制定等。而在防護基礎強化上，該行動計畫認為關鍵基礎設施產業的 IT、OT 人員及法務部門必須依其內部資訊安全策略共同為關鍵基礎設施安全而跨組織合作。

（三）新加坡之資安政策發展

新加坡有若干與網路安全有關的法規，如：「電腦濫用與網路安全法」(Computer Misuse and Cybersecurity Act,

CMCA)、「通訊法」(Telecommunications Act)、「垃圾信件控制法」(Spam Control Act)、「電子交易法」(Electronic Transactions Act）等，並於 2016 年公布「網路安全策略」(Singapore’s Cyber security Strategy)，主要內容包括：(1)強化關鍵資訊基礎設施的韌性。(2)藉由動員企業與社區、面對網路威脅、打擊網路犯罪，及保護個人資料來創造更安全的網路空間。(3)發展包含技術勞力、具備先進技術的企業以及強大研究能量之網路安全生態系統（Cyber security ecosystem)，以支持新加坡的網路安全需求，同時也帶動經濟成長。(4)由於網路威脅沒有國界之分，因此致力於強化國際夥伴關係。

2017 年通過「電腦濫用與網路安全法」修訂案，主要是為了因應電腦犯罪本質的改變，及跨國性與網路犯罪手法的變化，防範電腦不受未經允許的存取及修改，亦授權政府在需要偵測、辨認，或應對網路威脅時得以強制關鍵基礎設施業者提供關於其網路之資訊。

2018 年並通過「網路安全法」(Cybersecurity Act)，主要目的在建立與維護國家網路安全架構、有效降低網路威脅風險及確保關鍵資訊基礎設施受到保護，使國家能更有效率及完善地因應網路攻擊。該法並要求各關鍵基礎設施提供者通報網路安全事件，並採取防護措施以確保其系統的復原力（resilience)；此外也將賦與 2015 年成立的新加坡網路安全局（Singapore’s Cybersecurity Agency, CSA）管理網路安全事件及提升網路安全標準的權力。

新加坡最新的五年期資通安全精進計畫為「2018 年國家網路安全精進計畫」(Infocomm Security Masterplan, ISMP)。本計畫在前兩期精進計畫的基礎上，藉由政府、關鍵資通基礎設施、企業與個人的努力來強化新加坡的網路安全。其計畫包含三項重點：(1)強化關鍵資通基礎設施 (Critical Infocomm Infrastructure, CII) 的安全以及復原力來應付高度發展的網路攻擊。(2)提升企業與個人對於資通安全措施的採取。(3)發展新加坡的資通安全專家庫(Pool of Infocomm Security Experts)。

（四）德國之資安政策發展

德國在 2009 年通過「聯邦資訊科技安全局法」(Act on the Federal Office for Information Security 2009)，指定聯邦資訊科技安全局(German Federal Office for Information Security, BSI)為網路安全之聯邦層級主管機關，並規範其任務職責。在 2011 年頒布「德國網路安全策略」(Cyber-Sicherheitsstrategie für Deutschland)，其目標為：(1)保護關鍵基礎設施，(2)強化德國公民與企業的 IT 系統，(3)加強公共行政系統內的資訊安全，(3)建立「國家資訊回應中心」(National cyber Response centre)，(4)建立「國家資訊安全理事會」(National Cyber Security Council)，(5)提升資訊空間的犯罪控制效率，(6)進行資訊安全之歐洲區域以及全球合作，(7)使用可靠的資訊科技，(8)聯邦機構當中的人力發展，(9)採取資訊攻擊之回應措施。

2015 修訂「聯邦資訊科技安全局法」(BSI Act)，要求

關鍵基礎設施提供者，在其施行後 2 年內，應採行適當之組織與技術管理措施，以保護其所營運設施之必要系統、零件或作業程序，免於其在可用性、完整性、可鑑別性及機密性方面遭受瓦解，且關鍵基礎設施提供者與其產業協會可透過推動相關安全標準，以確保其措施符合前述要求，且每 2 年內須透過稽核或驗證等方式，持續證明其符合安全措施之要求。

2015 年亦通過「資訊科技安全法」，該法為一綜合性(包裹式)立法，整併並修正既有的網路安全法規，並且賦與 BSI 更多的權責。目的在增加對於德國公民、企業及政府機關的保護，降低其網路安全風險。該法要求關建基礎設施提供者採取檢視措施，並且向 BSI 報告網路安全事件；此外也要求 ISP 通報其可能的網路安全風險之義務。

2016 年，德國制定了三項與資安有關的政策如下：

1. 「德國資訊安全策略」(Cyber Security Strategy for Germany)

強調對關鍵基礎設施的保護，同時要求公私部門建立更廣泛的網路威脅資訊分享機制，及協助私部門與公眾強化面對網路威脅的能力。此外也提出在聯邦資訊安全局內設立行動快速回應軍團 (Quick Reaction Force)，以針對政府機構與關鍵基礎設施面對的網路安全威脅做出回應。該策略將德國網路安全分為在數位環境中採取安全而自主的行動、國家與經濟體間的共同任務、強大而永保先進的網路安全架構、德國於歐洲及國際網路安全政策的積

極定位的四大行動領域。

2.「關鍵基礎設施條例」(BSI-Kritisverordnung)

本條例係為補充 2015 年資訊科技安全法而提出。由於資訊科技安全法要求關鍵基礎設施營運者有義務執行最小化安全標準，且必須回報資安事件給聯邦資訊安全局。因此，該條例允許能源、水資源、食物與資通訊關鍵基礎設施的營運者透過該條例附件所提出的準則與計算公式，判斷其是否落入不適用資訊科技安全法的範圍內。此外，該條例修正關鍵基礎設施領域的適用範圍，將判斷準則擴大到金融、保險、運輸與交通及醫療關鍵基礎設施提供者的規定，並已於 2017 年 6 月 30 日正式生效。

3.「德國國防與安全政策白皮書」(White Paper on German Security Policy and the Future of the Bundeswehr)

該白皮書提出應透過強化國家復原能力的方式，以對抗日益增加的混合式威脅。其作法包含加強各級政府、關鍵基礎設施提供者及網路與媒體提供者的合作，降低能源部門的脆弱性、進行有效的邊界控制與發展公民保護與災難控制的議題。

參、 我國資安推動現況

一、 組織架構

資安會報成立於 90 年 1 月，負責國家資通安全政策、通報應變機制、重大計畫之諮詢審議及跨部會資通安全事務之協調及督導。為貫徹「資安即國安」戰略—提高資安主導層級之重要策略，行政院於 105 年 8 月 1 日成立資安專責單位—

資通安全處(簡稱資安處)取代原任務編組之資通安全辦公室，擔任資安會報的幕僚單位。

資安會報目前下設網際防護及網際犯罪偵防等二體系。依據105年8月修正之「行政院國家資通安全會報設置要點」，資安會報組織架構如下圖 1。

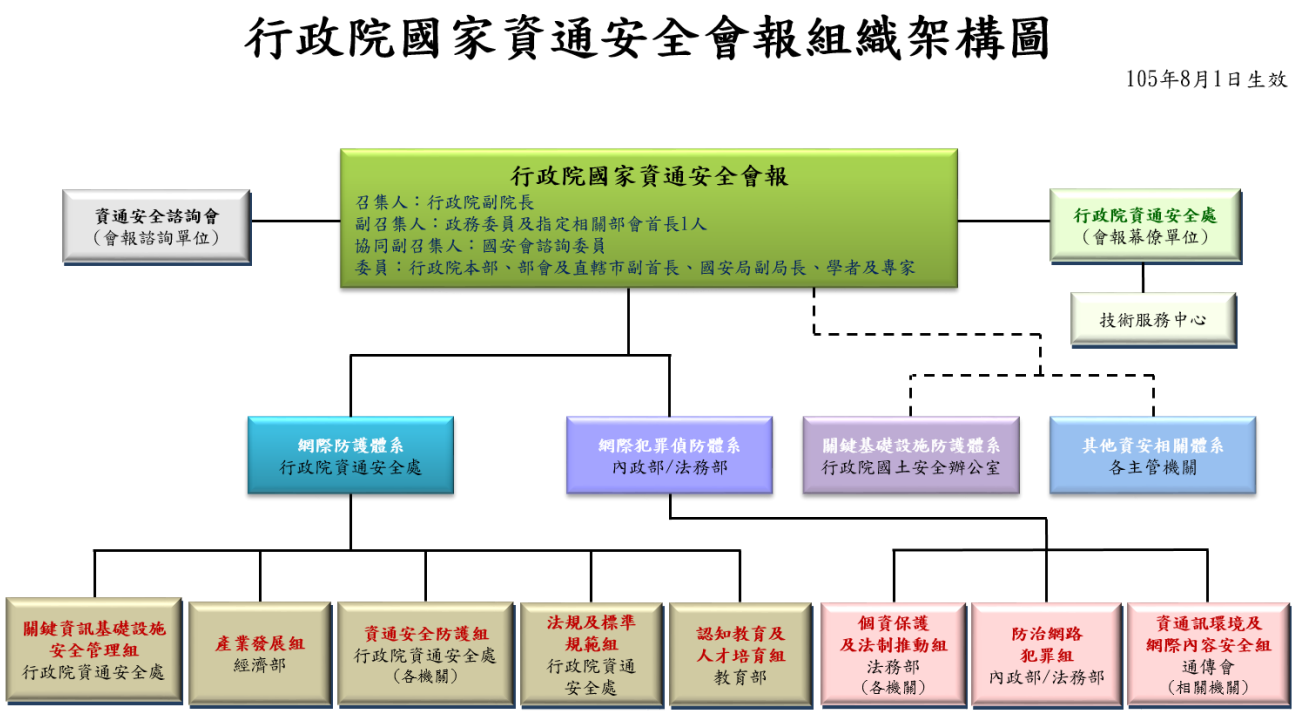

圖 1、行政院國家資通安全會報組織架構圖

1. 網際防護體系：由資安處主辦，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)及任務如下：

- 關鍵資訊基礎設施安全管理組：資安處主辦，負責規劃推動關鍵資訊基礎設施安全管理機制，並督導各領域落實安全防護及辦理稽核、演練等作業。
- 產業發展組：經濟部主辦，負責推動資安產業發展，整合產官學研資源，並發展相關創新應用。

- 資通安全防護組：資安處主辦，負責規劃、推動政府各項資通訊應用服務之安全機制，提供資安技術服務，督導政府機關落實資安防護及通報應變，辦理資安稽核及網路攻防演練，協助各機關強化資安防護工作之完整性及有效性。
- 法規及標準規範組：資安處主辦，負責研訂(修)資安相關法令規章，發展資安相關國家標準，訂定、維護政府機關資安作業規範及參考指引。
- 認知教育及人才培育組：教育部主辦，負責推動資安基礎教育，強化教育體系資安，提升全民資安素養，提供資安資訊服務，建構全功能之整合平臺，辦理國際級資安競賽，促進產學交流，加強資安人才培育。

2. 網際犯罪偵防體系：由內政部及法務部共同主辦，負責防範網路犯罪、維護民眾隱私、促進資通訊環境及網際內容安全等工作，並設下列各組，其主辦機關及任務如下：

- 個資保護及法制推動組：法務部主辦，負責個資保護之宣導推廣，檢討修正維護民眾隱私及防制網路犯罪相關法令規章。
- 防治網路犯罪組：內政部及法務部共同主辦，負責網路犯罪查察、電腦犯罪防治及數位鑑識等工作。
- 資通訊環境及網際內容安全組：國家通訊傳播委員會主辦，負責促進資通訊環境及網際內容安全，協助防治網路犯罪等工作。

行政院國家資通安全會報技術服務中心(簡稱技服中心)

成立於 90 年 3 月，協助資安會報逐步建置政府資通安全防護機制，並提供各政府機關事前安全防護、事中預警應變、事後復原鑑識等資安技術服務。此外，為積極研議國家資安政策及推動策略，強化產官學研資安技術、情資與經驗之交流及分享，充實資安作業能量，資安會報亦設置「資通安全諮詢會」，聘請資安領域有關之傑出人士及學者、專家擔任委員，就國家資安政策、管理及技術各面向提供建言。

另在民間資安推動的部分，主要由台灣電腦網路危機處理暨協調中心(TWCERT/CC)擔任主要窗口，除協助國內民間業者進行相關資安事件通報應變外，也肩負起和各個國際資安組織的聯繫和合作事宜，透過互惠合作及情資共享，加速事件通報應變與協調處理，以提升國家整體資安聯防的能量。

二、 推動進程

資安會報自 90 年迄今，陸續推動四個階段、各為期四年之重大資通安全計畫或方案，已有效提升我國資安完備度，各期計畫或方案重點說明如下圖 2。

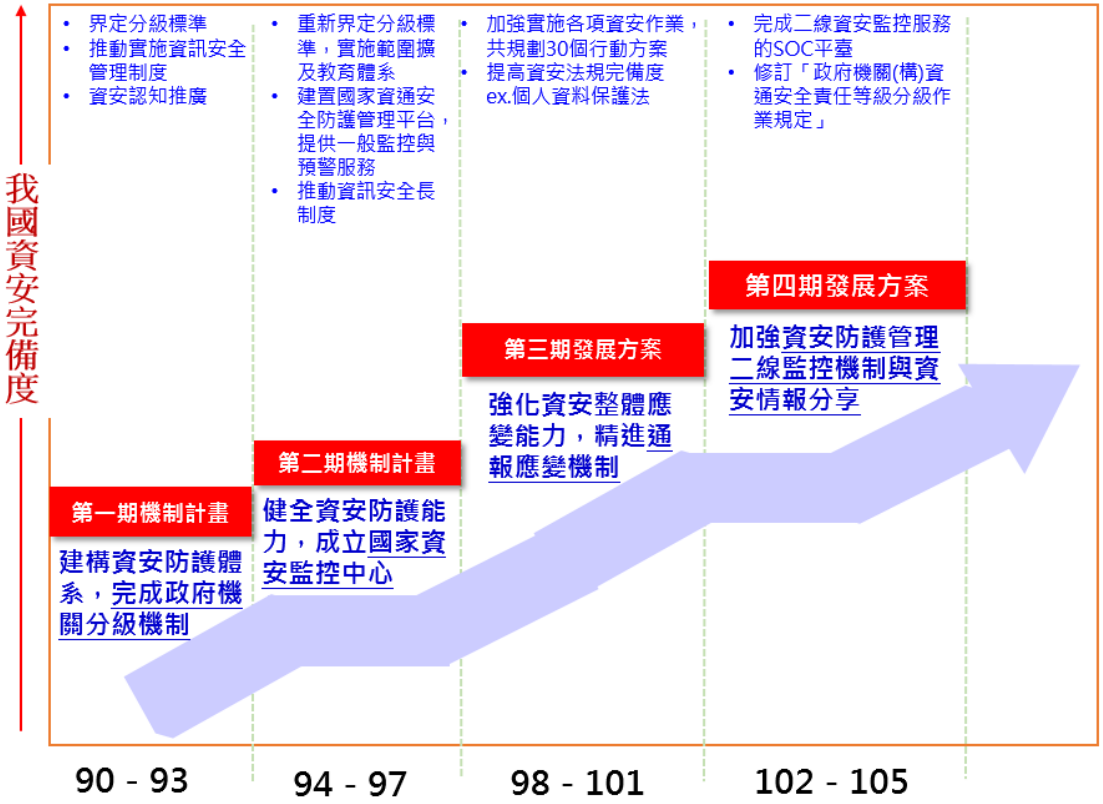

圖 2、我國資安推動進程

(一) 第一期機制計畫(90-93 年)

建構資安防護體系，完成政府機關分級機制

90 年 1 月 17 日行政院第 2718 次會議通過「建立我國通資訊基礎建設安全機制計畫」(簡稱第一期機制計畫)，成立資安會報，開啟政府有計畫地推動我國資通安全建設之路。第一期機制計畫主要工作：

1. 界定分級標準：

致力於推動全國 3,713 個政府機關(構)建立整體資

安防護體系，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，期在有限資源下，做好全面的資安防護工作。

2. 推動實施資訊安全管理制度：

針對20多個關鍵基礎設施的資訊系統實施資安管理方案，以推動實施資訊安全管理制度為首要工作，要求限期完成異地備援系統及通過國際資訊安全管理系統驗證。

3. 資安認知推廣：

訂定資訊人員及主管人員應接受必要之資安技術或管理課程訓練。

(二) 第二期機制計畫(94-97年)

健全資安防護能力，成立國家資安監控中心

第一期機制計畫對建立我國整體資安防護能力至為關鍵，行政院爰於93年核定「建立我國通資訊基礎建設安全機制計畫(94年至97年)」(簡稱第二期機制計畫)，旨在落實各項資安作業。主要工作包括：

1. 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。

2. 建置國家資通安全防護管理平臺(National Security Operation Center, NSOC)，以提升通報應變時效，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，對強化政府機關之資安能力產生一定的影響。

3. 建立並推動政府機關資訊安全長(CISO)責任制度、加強資安責任等級分級作業與機密資訊保護等。

(三) 第三期發展方案(98-101年)

強化資安整體應變能力，精進通報應變機制

一、二期機制計畫之推動，對於促使各機關重視資安與帶動民間投入具一定成效。鑒於大環境因素及資安問題仍層出不窮，實有訂定資安賡續發展計畫、加強實施各項資安作業之必要，爰行政院於98年1月訂頒「國家資通訊安全發展方案(98年至101年)」(簡稱第三期發展方案)。第三期發展方案以「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」作為四大政策目標，透過落實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。

（四） 第四期發展方案(102-105 年)

加強資安防護管理二線監控機制與資安情報分享

行政院於 102 年核定「國家資通訊安全發展方案(102 年至 105 年)」(簡稱第四期發展方案)，作為我國推動資安防護計畫之依據，及貫通政府、產業與民眾資安防護之價值樞紐。主要工作有：

1. 完成二線資安監控服務 SOC 平臺

在每個政府機關的內部網路，安裝不同類型的資安設備，負責蒐集第一層防線的資安事件，並經由自動化管道將問題單送給第二層防線的 G-SOC，進行 24x7 跨機關、跨部會的的關聯分析，以掌握政府機關遭受資安攻擊的全貌。

2. 辦理資安外部稽核及擴大規模網路攻防演練

每年至少選定 20 個機關辦理資安外部稽核，了解各機關(構)資安防護措施與資安管理政策之有效性與完整性，並針對受稽機關提出改善建議。自 102 年起舉辦大規模網路攻防演練，每年均挑選政府機關與關鍵基礎設施參與演練，以了解機關與關鍵基礎設施對資安事件之標準作業程序、通報應變程序及聯防機制的熟悉度，降低整體資安風險。

3. 推動政府組態基準及訂定安全軟體發展生命週期參考指引

自 101 年起推動各部會資通訊終端設備(如：個人電腦)部署政府組態基準(Government Configuration

Baseline, GCB)，105 年起並推廣至各部會所屬三、四級機關及地方政府。另針對軟體安全發展議題，訂定安全軟體發展生命週期(SSDLC)參考指引，以改善政府機關整體資安環境。

4. 建立「個人資料去識別化」的驗證標準規範

於 104 年建立「個人資料去識別化」的驗證標準規範(CNS 29100 與 CNS 29191)，並由政府機關帶頭試用，以回應民眾對於政府推動大數據(Big Data)及開放資料(Open Data)恐侵害個人隱私的顧慮。104 年 11 月 30 日財政部財政資訊中心率先通過驗證，取得財團法人臺灣電子驗證中心核發之證書，成為全國第一個示範案例。

5. 修訂「政府機關(構)資通安全責任等級分級作業規定」

為因應資通安全威脅情勢，進而提升國家資安防護水準，乃參考資通訊科技發展與網路攻防演練、政府機關(構)資安健診、稽核等結果，進行研修並將名稱調整為「政府機關（構）資通安全責任等級分級作業規定」。

三、 資安發展優劣勢分析

因應我國特殊的政經情勢及全球資安威脅趨勢，持續推動並落實國家整體資安防護以回應外界挑戰有其迫切性及必要性。爰透過 SWOT 深入分析我國內部資安環境之優劣勢及外部環境面臨之機會與威脅，作為規劃本方案之重要參考。

優勢(Strengths: S)	劣勢(Weaknesses: W)
1. 完成四階段國家資通安全發展方案，已顯著提升我國資安完備度 2. 政府提高資安主導層級，成立行政院資通安全處，與國家安全會議資通安全辦公室及國家通訊傳播委員會形成政府資安鐵三角，建構國安級資安防護機制 3. 資安會報成立「關鍵資訊基礎設施安全管理組」與「產業發展組」，進一步擴大資安防護範圍 4. 積極推動「資通安全管理法」立法，作為推動國家資安工作之法源依據，並依據母法增修訂相關子法及施行細則，成為建構數位國家的良好基礎	1. 我國尚未制定明確之關鍵資訊基礎設施保護(CIIP)推動政策、防護基準及管理標準，亦無持續監控各 CI 領域資安事件之機制，因此資安預警與事件處理難以有效落實 2. 政府機關、產業及學研界之資安專業人才缺口日益擴大，難以促進關鍵技術研發及國內資安產業發展 3. 資安產業規模及產值過不大，難以和國際大廠競爭，進而造成資安人才培育及研發資源不足
機會(Opportunities: O)	**威脅(Threats: T)**
1. 政府推動「數位國家‧創新經濟發展方案(DiGi^{+})」，帶動五加二產業創新及下一階段資安需求與成長 2. 政府已成立資通電軍及培育產學研菁英人才，人才需求浮現 3. 我國資安情勢特殊，惡意攻擊樣態多元，吸引他國與我國進行國際合作意願	1. APT 攻擊與組織型駭客試圖竊取公務與商業機密之威脅未減 2. DDoS 攻擊頻率與規模持續升高 3. 關鍵資訊基礎設施連網已成趨勢，遭入侵風險遽增，對民生經濟甚至國家安全造成嚴重威脅 4. IoT 等新興資訊技術快速發展，資安威脅與日俱增

肆、 發展藍圖

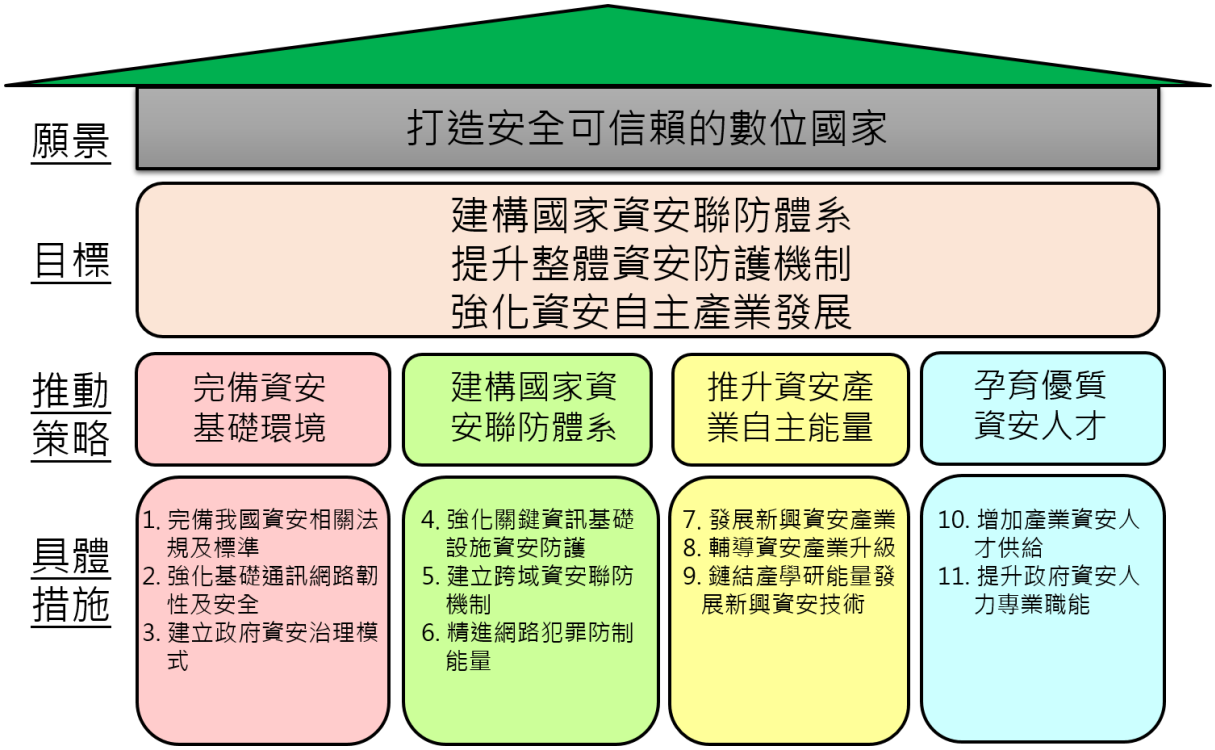

圖 3、方案發展藍圖

一、 願景

我國資安政策推動已歷經前四階段之系統性發展，逐步達成「建立安全資安環境，完備資安防護管理，分享多元資安情報，擴大資安人才培育，加強國際資安交流」之階段性目標，有效提升我國資安完備度。

考量駭客攻擊手法隨資訊科技發展迅速變異，且朝組織化方向演繹，而在推動數位經濟發展的過程中，各基礎建設均會逐漸數位化，倘資安事件層出不窮，不只帶來不便，甚至會影響經濟安定、社會安全及國家安全。因此，以風險管理的角度推動國家整體資安防禦尤其重要。另配合政府「五加二」產業創新及「數位國家・創新經濟發展方案」兩項重要政策，建立安全穩固的基磐配套措施，乃是促進數位國家

經濟更蓬勃發展的關鍵成功因素。爰本方案以「**打造安全可信賴的數位國家**」為願景，期經前瞻政策引導及國家整體資源投入，逐步提升國家整體資安防禦能量。

二、 目標

從「資安即國安」戰略可以看出，我國已將資安提升到國安層次，展現積極捍衛數位國土的決心。此外，為建構國家完整的資安發展策略，並防止駭客攻擊行為，國家安全會議(簡稱國安會)協同資安處及相關部會於105年8月召開「資安即國安策略會議」，並針對建立國家層級資安聯防團隊之作法提出建議：將各關鍵基礎設施如何建立資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)與電腦緊急事故處理小組(Computer Emergency Response Team, CERT)等資安管理機制納入，並請各主管機關據此落實執行。

爰此，為達成「打造安全可信賴的數位國家」願景，本方案以「**建構國家資安聯防體系，提升整體資安防護機制，強化資安自主產業發展**」為目標，期以各關鍵資訊基礎設施領域為基礎，建立國家資安聯防體系，戮力提升事前整體資安防護能量，以降低資安事件發生的頻率與衝擊，並強化事中的緊急應變效能及事後的復原作業機制，進而強固數位國土的資安防線。

惟歷年來我國資安防護機制推動之主要對象為政府機關，甚少涉及其他關鍵基礎設施領域，主因係除政府領域外之關鍵基礎設施為民營業者所營運，尚無法源依據可據以要求各關鍵基礎設施提供者強化資安防禦機制及制定相關資安防護

基準。爰本方案期能藉由資安專法之推動，完善我國資安法制基礎，借以推動各關鍵基礎設施領域主管機關及提供者落實資安防護措施，另方面，亦積極推動相關資安標準規範及政府資安治理制度，提升整體資安防禦機制。

此外，關鍵資訊基礎設施之安全，攸關我國民生經濟甚至國家安全議題，需國內資安自主產業及資安人才之支持，方能建構足夠之資安防護能量，保衛數位國家安全。惟我國資安自主廠商屬中小型企業，無足夠資源及人才開發出符合需求之資安整體解決方案，亦難以承擔國際行銷費用和龐大的在地化服務成本，成為跨足國際市場之主要瓶頸。

三、 推動策略

為建構國家資安聯防體系，提升整體資安防護機制，強化資安自主產業發展，以保衛數位國土安全，本方案具擬四項推動策略，分別從「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」及「孕育優質資安菁英人才」等四個面向著手，逐步推動我國資安縱深防禦及聯防體系，打造安全可信賴的數位國家。

（一） 完備資安基礎環境

為了因應數位時代資訊科技及雲端服務的蓬勃發展，及瞬息萬變的資安攻擊手法，歐美及亞太地區多致力於制訂資安相關法規與政策，以有效控制已知資安風險，並亟力掌握未知風險，以回應內外資安挑戰。

我國因特殊的政經情勢，面臨更為嚴峻的資安威脅與攻擊，必須用更高的標準看待資安，將資安置於國安的架構內。

爰本方案從資安基礎環境著手，由法規、標準及資安治理等層面，設法打造安全的資安基礎環境，作為推動國家資安聯防體系、資安產業自主能量及資安人才培育之根本。

1. 完備我國資安相關法規及標準

1.1 完成「資通安全管理法」立法及進行相關法規調適

(1) 完成我國資安專法—「資通安全管理法」立法，並納入公務機關、關鍵基礎設施提供者及公營事業、政府捐助之財團法人等民營機構。

(2) 完成相關子法及施行細則之增修訂。

(3) 完成資通安全管理法相關法規標準盤點及增修訂。

1.2 因應新興科技發展，研訂資安標準規範

(1) 持續關注新興科技發展，蒐集研析國際資安相關標準規範，以制定與國際接軌之國家標準規範。

(2) 定期檢視並增修訂資安作業規範、國家標準、參考指引等，以因應新興科技發展趨勢，符合數位國家的資安要求。

2. 強化基礎通訊網路韌性及安全

2.1 強化通訊網路資安防禦與應變能量

(1) 加強通訊網路資安防禦與緊急應變措施，增加國家基礎網路之韌性及安全。

(2) 即時掌握重點通訊網路運作狀態，發掘潛在資安威脅，適時啟動應變機制，降低資安風險。

2.2 強化物聯網安全，推動安全驗證標章

(1) 蒐集研析 IoT 設備之國際資安規範及標準，並據以發展我國之技術規範與認證標準。

(2) 建立 IoT 設備之資安檢測環境，推動 IoT 設備之安全驗證標章，並輔導廠商產品進行資安檢測。

2.3 推動政府資料中心整合，優化政府網路防禦架構

(1) 建置以部會為中心的資料中心，資源向上集中並集中安全防護能量。

(2) 配合網路調整集中，加強安全之網路防禦策略及架構。

3. 建立政府資安治理模式

3.1 建立國家層級資安風險管理機制

建立國家層級資安風險識別、評估、處理與監控之框架與方法，俾利國家重要資產及關鍵基礎設施提供者據以落實資安管理機制，提升整體資安韌性與安全。

3.2 推動政府機關導入資安治理制度

(1) 建立資安治理成熟度主導評審員種子師資及培訓機制。

(2) 推動政府機關導入資安治理制度，並進行成熟度自評或評鑑，據以分配國家資安資源。

(二) 建構國家資安聯防體系

資安會報因應我國資安威脅加劇，新增「關鍵資訊基礎設施安全管理組」，讓資安鐵三角—國安會、資安處及國家通

訊傳播委員會(簡稱通傳會)連結 8 大關鍵基礎設施領域之 7 個主管部會，擴大建立國家資安聯防運作機制、建立 8 大關鍵資訊基礎設施領域及國家層級之資訊分享與分析中心(ISAC)、電腦緊急事故處理小組(CERT)及資訊安全監控中心(Security Operation Center, SOC)，期由情報驅動國家政府、關鍵基礎設施主管機關及提供者三大層級，形成資安聯防與合作網路，組成國家資安聯防體系，進行資安聯防及情資分享，並聯結國際。

為了強化地方政府資安防護之最後一哩路，本方案亦推動地方政府資安區域聯防體系，以六都為首結合鄰近縣市資源，建立地方聯合資安防護網，並進一步與國家層級資安聯防團隊合作，使中央及地方政府關鍵資訊基礎設施領域之資安防護更具韌性。而檢調單位對於新型態跨境、跨域之網路犯罪查察能量，亦為本方案之重要工項之一。

4. 強化關鍵資訊基礎設施資安防護

4.1 訂定關鍵資訊基礎設施資安防護政策及風險控管原則

(1) 訂定關鍵資訊基礎設施資安防護政策、風險管理機制及資安防護建議，並定期滾動式檢討修訂。

(2) 訂定關鍵基礎設施領域之 ISAC、CERT 及 SOC 建置指引。

4.2 輔導各關鍵資訊基礎設施落實資安防護基準

(1) 建立各關鍵基礎設施領域之資安防護策略與

防護基準。

(2) 盤點各關鍵基礎設施領域資訊資產、系統及網路，以建置資產資料庫。

(3) 建立各關鍵基礎設施領域風險評估與管理機制，並落實風險控制。

(4) 建置各關鍵基礎設施領域之 ISAC、CERT 及 SOC，以達資安情資分享、早期預警、緊急應變及持續監控之目的，確實掌握資安風險。

(5) 推動各關鍵基礎設施領域主管機關研訂及實施資安防護計畫，以落實資安防護基準。

(6) 定期辦理各關鍵基礎設施領域之通報應變相關演練。

5. 建立跨域資安聯防機制

5.1 建立國家資安情資整合及預警中心

(1) 建置國家層級的 ISAC、CERT 及 SOC，達到跨領域之情資分享、緊急應變及資安監控，強化縱向通報及橫向通知機制，以掌握國家整體資安風險。

(2) 即時分析資安事件樣態及駭侵手法，並部署主動式防禦機制，以建立跨域資安聯防機制。

(3) 定期實施關鍵基礎設施跨領域相關演練。

5.2 結合國內產業與民間社群能量，建立國內外公私協防機制

(1) 持續參與國際重要會議及活動，透過資安威脅

情資互惠交流等方式，以建立雙邊實質合作關係。

(2) 協助建立產業 CERT/CSIRT 機制，落實資安事件通報，並強化國內資安應變組織協同合作，完善資安事件應處作為。

(3) 善用民間社群及網路媒體等資源，發布資安相關訊息與技術文件，以提升民眾資安認知。

5.3 建構地方政府資安區域聯防體系

(1) 以六都為核心，結合鄰近縣市推動資安區域聯防，建立地方聯合資訊安全防護網，並帶動地方政府與臨近學研機構合作，共同培育政府與學界之資安人才。

(2) 推動導入政府組態基準(Government Configuration Baseline, GCB)，並逐步汰換基層地方政府具高風險資訊軟硬體設備，以完善縱深防禦。

6. 精進網路犯罪防制能量

6.1 強化新型態網路科技犯罪偵防能量

(1) 拓展網路安全情蒐網路，研析新型態網路犯罪手法,形成主動式的犯罪偵查網路,即時發掘、檢測、通報與跨機關分享資安情資。

(2) 研析網路犯罪資料及整合相關資訊科技，有效保全網路危安證據、解析駭侵動機與意圖，以提升新型態網路犯罪案件的偵辦效能。

(3) 強化網路駭侵偵查技術，提升網路科技犯罪資訊蒐集廣度及鑑識能量。

6.2 提升網路犯罪取證與鑑識能量

(1) 精進輔助工具，強化第一線人員現場取證能力與簡化作業流程，以確保數位證據的完整性，加強鑑識作業的效率。

(2) 跨域統合鑑識資源，分析歸納情資關聯性，以利即時掌握關鍵數位證據。

6.3 建構網路跨境追查環境

(1) 因應跨境及匿蹤之網路犯罪型態，建構境內與境外中繼站管制、監視及追蹤機制，以即時發現受駭電腦、進行案件調查並阻止網路竊密情形。

(2) 建立公、私部門聯防管道，掌握跨境網路犯罪跡證，即時通報防禦與追蹤查處，提升犯罪偵防效率。

（三） 推升資安產業自主能量

政府及民間企業為建構足夠的資安防護能量，對於資安廠商提供整體性的資安解決方案(Total Solution)需求若渴。然我國資安自主研發廠商屬中小型企業，無足夠資源及機會快速開發出符合市場需求的資安解決方案，長期依賴國外廠商之情形下，不僅弱化國內資安自主防護能量，也讓國內資安業者發展緩步。

為解決我國資安產業發展之瓶頸，資安會報新設「產業發展組」，且為推動「資安即國安」戰略—推動國防資安產業之重要策略，亦增設「國防需求分組」，期透過國防需求帶動國內資安產業發展，並提高臺灣資安產業在全球資安市場之技術優勢。

7. 發展新興資安產業

7.1 連結國家防衛自主需求，發展國內資安產業生態系

(1) 配合新興應用資安技術研發，提供合適之場域進行技術驗證，以提升國內資安產業自主研發比例，降低對國外產品之依賴。

(2) 創造國內資安產品與關鍵場域合作之契機，以提升國內資安產品能見度，帶動整體資安產業發展量能。

(3) 打造有利資安產業發展之環境，輔導具發展潛力之新創廠商或團隊，以促使新興資安產業生態系發展。

8. 輔導資安產業升級

8.1 推動國內廠商資安產品納入共同供應契約

(1) 盤點國內自主研發資安技術，逐年依產業需求重點，建立相對應之資安產業標準，以供相關產品採購參考，並輔以共同供應契約規範，推動政府機關採購國內資安產品，提升國內資安自主產品使用率。

(2) 持續修訂資安產業標準，提升共同供應契約產品安全性，強化政府機關採購優質且高安全性之資安產品。

8.2 建立資安產業標準及檢測認驗證機制

(1) 蒐集研析國際資安產業技術標準，作為增修訂我國資通訊產品之國家標準及產品認驗證機制之參考依據。

(2) 推動我國資安檢測認驗證制度，協助國內資安檢測實驗室建立符合標準之檢測服務能量，輔導廠商產品進行安全性檢測及提供資安修補諮詢，以提升國內資安產品之國際市場競爭力。

9. 鏈結產學研能量發展新興資安技術

9.1 以國內產業技術自主為導向發展關鍵技術

(1) 以前瞻科技及產業需求為導向，推動產學媒合，導引研發成果擴散至產業，提升國內資安關鍵技術自主研發能量。

(2) 盤點資安產業技術缺口，結合產學研能量，發

展資安關鍵核心技術，並導入重點場域試煉，以研發國際級資安產品、新興應用整合技術及整合性方案。

(3) 藉由資安技術研發的過程與成果，進而培育高階資安專業人才，促進產學研資安人才培育之正向循環。

（四） 孕育優質資安人才

我國資安產業自主能量發展需仰賴堅實之資安人力，爰政府當務之急為提升我國資安人才之質與量，積極培育資安高階人才。

10. 增加市場資安人才供給

10.1 投入資源厚植大專校院資安人才培育量能

(1) 調查並推估產業資安技術及人才供需缺口，提供大專校院資安人才培育規劃與布局之參考。

(2) 提出具體措施，以引導大專校院師生鏈結產學研能量，合作布建教學實作資源、環境及養成模式等，將系統化及制度化的資安人才培育模式導入正規教育體系，擴大人才培育量能。

(3) 鼓勵企業與學校合作，研擬符合產業需求之資安人才培育課程或專班。

10.2 拔擢在職人士培育產業所需之資安專業人才

(1) 針對資安實務工作需求，以實習、實訓等方式培養實戰能力，強化資安專業人才培育之質與量。

(2) 建立學習與實際演練之平臺，以強化學員之資安實戰經驗與防護部署能力。

(3) 積極促成國際資安訓練機構協同合作，以利資安人才技能交流。

11. 提升政府資安人力專業職能

11.1 發展政府資安人員職能及領域職能藍圖並辦理培訓

建立政府機關資安人員職能及領域職能藍圖，並規劃相關訓練課程辦理培訓工作，俾利補強政府機關資安人力缺口。

11.2 建立資安訓練單位認證制度

建立政府機關(構)訓練單位資安課程等相關認證制度。通過認證之單位可開設資安專業課程、代訓資安人員，擴大資安人才培育之量能。

11.3 培養公務人員資安基本知能

(1) 中高階主管及公職人員考試錄取人員專業訓練，納入資安認知課程。

(2) 加強推動各機關依資安分級辦理資訊人員及一般人員資安知能相關課程。

11.4 推動政府機關設置資安專職人力

(1) 積極研議政府機關設置資安專職人力推動機

制。

(2) 積極協調各機關依相關法規，就施政優先序、業務消長情形，分階段補足所需資安人力。

四、 部會分工

表 1、部會分工表

具體措施/工作項目	主辦部會
1.完備我國資安相關法規及標準	
1.1 完成「資通安全管理法」立法及進行相關法規調適	行政院資安處、相關部會
1.2 因應新興科技發展，研訂資安標準與規範	行政院資安處、相關部會
2.強化基礎通訊網路韌性及安全	
2.1 強化通訊網路資安防禦與應變能量	通傳會
2.2 強化物聯網安全，推動安全檢測標章	IoT 目的事業主管機關
2.3 推動政府資料中心整合，優化政府網路防禦架構	國發會、各部會
3.建立政府資安治理模式	
3.1 建立國家層級資安風險管理機制	行政院資安處
3.2 推動政府機關導入資安治理制度	行政院資安處、各部會
4.強化關鍵資訊基設施資安防護	
4.1 訂定關鍵資訊基礎設施資安防護政策及風險控管原則	行政院資安處
4.2 輔導各關鍵資訊基礎設施落實資安防護基準	各 CI 主管機關
5.建立跨域資安聯防機制	
5.1 建立國家資安情資整合及預警中心	行政院資安處
5.2 結合國內產業與民間社群能量，建立國內外公私協防機制	行政院資安處 通傳會
5.3 建構地方政府資安區域聯防體系	各地方政府

具體措施/工作項目	主辦部會
6.精進網路犯罪防制能量	
6.1 強化新型態網路科技犯罪偵防能量	內政部、法務部
6.2 提升網路犯罪取證與鑑識能量	內政部、法務部
6.3 建構網路跨境追查環境	內政部、法務部
7. 發展新興資安產業	
7.1 連結國家防衛需求，發展國內資安產業生態系	經濟部
8. 輔導資安產業升級	
8.1 推動國內廠商資安產品納入共同供應契約	經濟部
8.2 建立資安產業標準及檢測認驗證機制	經濟部
9. 鏈結產學研能量發展新興資安技術	
9.1 以國內產業技術自主為導向發展關鍵技術	科技部、經濟部
10. 增加產業資安人才供給	
10.1 投入資源厚植大專校院資安人才培育量能	教育部
10.2 拔擢在職人士培育產業所需之資安專業人才	經濟部
11. 提升政府資安人力專業職能	
11.1 發展政府資安人員職能及領域訓練地圖並辦理培訓	行政院資安處
11.2 建立資安訓練單位認證制度	行政院資安處
11.3 培養公務人員資安基本知能	國發會
11.4 推動政府機關設置資安專職人力	行政院資安處、人事行政總處

五、 重要績效指標

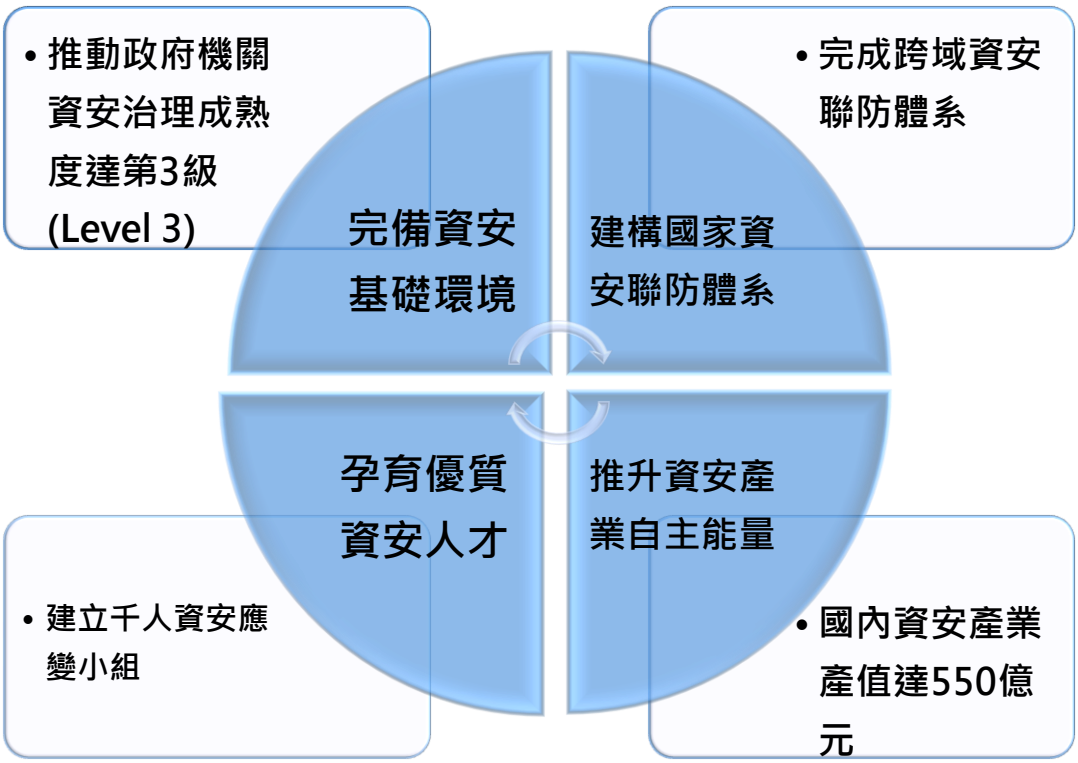

圖 4、重要績效指標

本方案依據願景、目標及推動策略，訂定四項重要績效指標(如圖 4)，分述如下：

(一) 推動政府機關資安治理成熟度達第 3 級(Level 3)

根據趨勢科技 2016 年度資訊安全總評報告，顯示 2016 年網路威脅屢創新高，勒索病毒造成全球企業損失金額高達 10 億美元（相當於新台幣 300 億元），且勒索病毒新家族數量較 2015 年相比成長 7 倍，而臺灣遭受此攻擊次數更排名全球前 20%，屬高資安風險國家。

為有效降低並控管政府機關資安風險，落實資安治理制度是必要的措施。我國自 103 年起開始輔導政府機關試行導入資安治理成熟度評估模式，以衡量組織之資安治理成效，截止 105 年底止，累計有 10 家政府機關推動試行。未來除了積極推動各政府機關全面導入資安治理成熟度評估模式，將透過定期辦理自評方式，引導各機關強化資安治理作為，朝制度化型(Established)、可預測型(Predictable)，甚至是創新型(Innovating)組織邁進，使 A、B 級政府機關資安治理成熟度達第 3 級(含以上)，健全各政府機關之資安體質。

值得一提的是，「資通安全管理法」係推動資安治理法制化的第一步。為了回應日益嚴峻的資訊安全威脅同時健全數位時代的法制基礎，行政院資安處積極推動「資通安全管理法」之立法，及完成資通安全管理法施行細則與相關子法之訂立；藉由資安專法之訂立，賦予各機關資通安全維護義務之法律基礎，以利各關鍵基礎設施領域主管機關完成業管領域法規或標準之盤點與增修訂作業，並作為後續推動國家資

通安全工作之基石，進而有效提昇我國資通安全防禦能量。

（二） 完成跨域資安聯防體系

106 年 5 月 Wanna Cry 病毒在全球肆虐，我國政府機關在資安工作長期推動的成效下，所幸影響層面不大，但仍有若干醫院及電廠等關鍵基礎設施之行政電腦遭受感染，幸未影響運作。因此，從保護資訊安全角度出發，推動關鍵資訊基礎設施防護(CIIP)將是本方案之重點工作之一。

CIIP 的推動將分三層級，分由行政院、CII 主管機關、CII 透過 SOC（事前監控）、CERT（事中通報），及 ISAC（事後分享）等平臺之建置，落實風險管理、資訊共享與合作、通報應變等工作。另外，在中央與地方政府聯防方面，為使地方政府之資安防禦能量提升，與中央政府之資安防禦網有效鏈結，本方案同時推動以六都為首之地方政府區域聯防，期藉由鄰近縣市資安資源整合與運用，加速地方政府回應外界資安挑戰之應變能量，並帶動區域學研機構人才培育之成效。

本方案預期 109 年將完成我國跨域區域資安聯防體系之建構，從基層機關至中央建構縱深防禦體系，由 CI 領域提供者擴及國家層次，強化跨域資安聯防以有效抵禦外界的資安威脅與挑戰。

（三） 國內資安產業產值達550億元

根據IDC(International Data Corporation)105年10月公布的全球安全支出指南半年報，預測資安相關的硬體、軟體與服務的市場規模，將由105年的737億美元(約合新台幣2.34兆元)，增長至109年的1016億美元(約合新台幣3.22兆元)，年複合增長率8.3%。

然我國105年資安產業產值約新台幣344億元，規模不大，且年營收逾5億元者以系統整合業者居多，顯見創新研發能量待提升。爰為推升我國資安自主能量，本方案以政府需求為出發，期望藉由推動符合安全標準之國內資安產品納入共同供應契約，推動政府機關優先採用國內資安產品，提升國內資安產業之產值。政府機關同時可作為國內資安產品之實驗場域，回饋產品之使用建議，進而促進關鍵資安技術及產品研發品質之提升。

本方案以109年國內資安產業總產值達550億元新台幣為目標，透過資安產業環境整備、安全檢測機制建立及輔導國內廠商於國際露出等措施，來推升國內資安產業的發展能量，進軍國際資安市場，並為未來國內資安產業產值跳躍式成長打造良好的基礎。

（四） 建立千人資安應變小組

優秀的資安人才是建構國家防護體系之重要關鍵。經資安處調查發現，現階段在A、B、C^{+}等政府機關中，資安專職人力尚有不足；此現象對政府推動縱深防禦體系實屬不易。為滿足國家資安人力需求，本方案規劃透過多元、系統化管

道，從產學研等領域積極培育資安專業人才，並以 109 年底前政府機關建立千人資安應變小組為目標。此千人資安專職人力，於資安事件發生前，執行所屬單位資安防護任務，事中則跨部會快速組成緊急應變小組，即時處理資安事件，事後則協助復原與處置等任務。

短期內，為了快速培訓政府機關資安人才，讓政府體系之資安防護網更趨縝密、應變更具彈性，除藉由資安服務團外，透過符合資格的培訓單位進行代訓工作是刻不容緩的任務。長遠來看，前揭資安應變小組成員未來將成為培訓資安專才之種子教師，將實務經驗轉化為教材，以精進我國資安專才之質量，進而保衛數位國家安全。

表 2、分年里程碑

重要績效指標	106 年	107 年	108 年	109 年
推動政府機關資安治理成熟度達第 3 級 (Level 3)	• 完成「資通安全管理法」立法 • 推動 A、B 級政府機關試行導入資安治理成熟度	• 精進資安治理成熟度評審機制 • 完成 3 個 A 級政府機關導入資安治理成熟度自評作業	推動 30 個 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 2 級以上	推動所有 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 3 級以上
完成跨域資安聯防體系	建構整體(含政府機	建構整體通報應變體	建構整體資安聯防監控	建構國家資安威脅風險

重要績效指標	106 年	107 年	108 年	109 年
	關、關鍵基礎設施領域、教育體系及民間）資訊分享與分析中心	系，成立國家層級電腦緊急應變小組	機制，成立國家資安情資整合及預警中心	燈號，完成跨域資安聯防體系
國內資安產業產值達 550 億元	盤點國內自主研發資安技術，推動 1 個資安模擬場域	輔導 1 家資安產業廠商於國際露出	推動 1 個資安試煉場域，並輔導廠商於試煉場域進行驗證	帶動資安新創團隊或輔導營業額 1 億元以下廠商，計 30 家；帶動國內資安產業值達 550 億元
建立千人資安應變小組	成立資安服務團，輔導部會機關落實資安防護及管理	擴大資安服務團輔導範圍至各關鍵基礎設施領域主管機關	累計達 4 家(含以上)訓練單位通過資安培訓單位認證	政府機關(構)資安專職人力達千人

伍、 預期效益

一、 完備數位時代的法制基礎，建構安全可信賴的網際生態體系。

二、 完成關鍵資訊基礎設施領域及六都區域聯防體系，厚植國家防禦能量。

三、 提升國內資安產業自主研發能量，帶動國內資安產業產值達 550 億元。

四、 建立政府機關千人資安應變小組，整備國家資安人力資源、保衛數位國家安全。

陸、 推動組織、資源需求及計畫管理

一、 推動組織

依據「行政院國家資通安全會報設置要點」，行政院資通安全處為資通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。

二、 執行規劃

本方案工作項目之主責部會應召集相關部會，提出行動計畫與績效指標。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。

三、 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。

四、 相關行動方案之管考

本方案之工作項目與績效指標，由行政院資通安全處運用既有督導機制，落實執行管考。

五、 方案核定與修訂

本方案經行政院核定後實施，修正時亦同。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。

柒、 附件

附件 1、分年重要進程

工作項目	分年重要進程	主(協)辦部會
1.完備我國資安相關法規及標準		
1.1 推動「資通安全管理法」立法及進行相關法規調適	1. 106 年底前完成「資通安全管理法」立法及相關子法與施行細則。 2. 立法通過後 18 個月內，分階段推動實施「資通安全管理法」；立法通過後 2 年，檢討適用範圍。	行政院資安處、相關部會
1.2 因應新興科技發展，研訂資安標準規範	每年至少完成 2 項資安作業規範、國家標準、參考指引等之檢視及增修訂。	行政院資安處、相關部會
2.強化基礎通訊網路韌性及安全		
2.1 強化通訊網路資安防禦與應變能量	1. 107 年底前完成國家通訊暨網際安全中心(NCCSC)建置。 2. 106 年至 109 年，逐步完成與國內 30 家重要 IASP 業者介接，即時交換資安威脅情資。	通傳會
2.2 強化物聯網路安全，推動安全驗證標章	1. 106 年底前完成重要 IoT 項目資安驗證標準之盤點,每年並視研析成果增修訂 IoT 相關資安驗證標準。 2. 107 年底前建立 IoT 設備之資安檢測環境，並輔導廠商落實 IoT 設備與產品之資安檢測。	IoT 目的事業主管機關
2.3 推動政府資料中心整合，優化政府網路防禦架構	1. 108 年底前擴大骨幹網路閘口惡意 IP 及 DNS 阻擋	國發會、各部會

工作項目	分年重要進程	主(協)辦部會
	服務，機關內部接取電路納入資安防護服務。 2. 109 年底前完成 GSN 北、中、南三大機房電路備援機制。	
3.建立政府資安治理模式		
3.1 建立數位國家資安風險管理機制	1. 106 年底前完成國家資安風險評估框架與方法。 2. 107 至 109 年推動關鍵基礎設施領域落實資安風險評估及管理。	行政院資安處
3.2 推動政府機關導入資安治理制度	1. 106 年推動 A、B 級政府機關試行導入資安治理成熟度自評作業。 2. 107 年精進資安治理成熟度評審機制，並推動 3 個 A 級政府機關完成資安治理成熟度自評作業。 3. 108 年推動 30 個 A 級政府機關落實資安治理成熟度自評，成熟度達第 2 級以上。 4. 109 年推動所有 A 級政府機關落實資安治理成熟度自評，成熟度達第 3 級以上。	行政院資安處、各部會
4.強化關鍵資訊基礎設施資安防護		
4.1 訂定關鍵資訊基礎設施資安防護政策及風險控制原則	1. 106 年底前完成關鍵資訊基礎設施資安防護政策與防護原則。 2. 106 年底前完成關鍵基礎設施領域 ISAC、CERT 及 SOC 建置參考指引。	行政院資安處
4.2 輔導各關鍵資訊基礎設施落實資安防護基準	1. 106 年底前完成各關鍵基礎設施領域資訊分享與	各 CI 主管機關

工作項目	分年重要進程	主(協)辦部會
	分析中心(ISAC)建置，107 年底前擴大納管範圍。 2. 108 年底前完成： (1) 建立各關鍵基礎設施領域電腦緊急應變小組(CERT)。 (2) 建立各關鍵基礎設施領域資安防護策略與防護基準。 (3) 完成各關鍵基礎設施領域資訊資產盤點及風險評估。 3. 109 年底前建置各關鍵基礎設施領域資訊安全監控中心(SOC)。	
5.建立跨域資安聯防機制		
5.1 建立國家資安情資整合及預警中心	1. 106 年底前建立國家層級資訊分享與分析中心(N-ISAC) 建置。 2. 107 年建立國家層級電腦緊急應變小組(N-CERT)。 3. 108 年建立國家層級資安聯防監控中心(N-SOC)建置。 4. 每年實施關鍵基礎設施跨領域相關演練。	行政院資安處
5.2 結合國內產業與民間社群能量，建立國內外公私協防機制	1. 每年參與國內、外重要資安聯防活動或會議，並爭取國內、外資安聯防合作專案，建立互惠機制。 2. 持續建立國內、外資安組織聯繫管道，以促進資安情資交流與合作。	行政院資安處、通傳會

工作項目	分年重要進程	主(協)辦部會
5.3 建構地方政府資安區域聯防體系	1. 基層機關導入政府組態基準(GCB)，達 95%。 2. 逐步汰換基層機關具高風險之資訊設備，109 年底前達申請汰換數之 95%。 3. 109 年底前建立六都區域聯防體系。	各地方政府
6.精進網路犯罪防制能量		
6.1 強化新型態網路科技犯罪偵防能量	107 年底前建立新型態網路威脅與攻擊之蒐研與通報防禦機制，並加強犯罪偵查技能之實務訓練，以強化新型態網路犯罪偵防能量。	內政部、法務部
6.2 提升網路犯罪取證與鑑識能量	108 年底前逐步統合全國網路犯罪取證與鑑識服務資源，並持續精進數位鑑識知能，以即時掌握關鍵數位證據、強化鑑識效率。	內政部、法務部
6.3 建構網路跨境追查環境	109 年底前逐步完成網路犯罪跨境追蹤與防制機制，建立公私聯防管道，以持續建構潛在安全威脅及犯罪目標追蹤機制。	內政部、法務部
7.發展新興資安產業		
7.1 連結國家防衛需求，發展國內資安產業生態系	1. 106 年底前完成資安產業需求及現況盤點。 2. 109 年底前輔導資安新創團隊達 20 家，協助媒合新創團隊與創投基金。 3. 輔導新興應用資安技術於關鍵基礎設施進行技術驗證，每年至少 2 項。	經濟部
8.1 推動國內廠商資安產品納入共同供應契約	逐年依產業需求重點，建立相對應之資安產業標準，以	經濟部

工作項目	分年重要進程	主(協)辦部會
	供相關產品採購參考，並輔以共同供應契約規範，推動政府機關採購國內資安產品。	
8.2 建立資安產業標準及檢測認驗證機制	1. 每年增修訂 3 種資安相關國家標準。 2. 109 年底建立資安產業標準認驗證自主營運制度，並輔導廠商通過資安檢測認驗證。	經濟部
9.鏈結產學研能量發展新興資安技術		
9.1 以國內產業技術自主為導向發展關鍵技術	1. 106 年底前完成資安關鍵技術 POC 及初步場域模擬實測；107 年導入重點場域進行實證。 2. 109 年底前完成發展資安新興應用整合技術，催化相關應用與產品。	科技部、經濟部
10.增加產業資安人才供給		
10.1 投入資源厚植大專校院資安人才培育量能	1. 107 年底前建立選派資安種子師資赴外研習機制。 2. 109 年底前建立大專院校系統化培育資安專業人才之機制。	教育部
10.2 拔擢在職人士培育產業所需之資安專業人才	1. 定期辦理國際資安競賽，培育資安競賽實戰選手。 2. 107 年底前引進國外符合產業需求之資安先進課程並試行。 3. 109 年底前進行資安先進課程本土化及產業擴散。 4. 109 年底前培訓產業資安人才達 2,000 人。	經濟部
11.提升政府資安人力專業職能		
11.1 發展政府資安人員職能及領域職能藍圖並辦理培	1. 106 年底前完成政府資安人員職能及領域職能藍	行政院資安處

工作項目	分年重要進程	主(協)辦部會
訓	圖。 2. 每年持續推動政府資安人員培訓作業。	
11.2 建立資安訓練單位認證制度	1. 106 年底前完成資安訓練單位認證制度規劃。 2. 107 年至 108 年,每年輔導 2 個訓練機構通過認證。	行政院資安處
11.3 培養公務人員資安基本知能	1. 106 年底前將中高階主管及高普考資訊類科錄取人員專業訓練納入資安課程。 2. 109 年底前，協同相關部會及地方各級機關，逐步推動資訊安全基本課程及數位學習課程,以提升資訊人員及一般公務人員資安基本知能。	國發會
11.4 推動政府機關設置資安專職人力	協助各主管機關以資訊(安)人力向上集中及持續推動現有資訊(安)業務四化原則，及依「中央政府機關總員額法」檢討員額配置，將節餘人力適度支應資安人力需求。	行政院資安處、行政院人事行政總處

附件 2、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，並自 102 年 1 月 1 日生效
中華民國 103 年 3 月 24 日行政院院臺護字第 1030128738 號函修正發布，並自 103 年 3 月 3 日生效
中華民國 103 年 12 月 29 日行政院院臺護字第 1030157519 號函修正發布，並自 103 年 12 月 29 日生效
中華民國 104 年 3 月 13 日行政院院臺護字第 1040126086 號函修正發布，並自 104 年 3 月 13 日生效
中華民國 105 年 1 月 19 日行政院院臺護字第 1050150599 號函修正發布，並自 105 年 1 月 20 日生效
中華民國 105 年 8 月 24 日行政院院臺護字第 1050173756 號函修正發布，並自 105 年 8 月 1 日生效

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

二、資安會報任務如下：

(一)國家資通安全政策之諮詢審議。

(二)國家資通安全通報應變機制之諮詢審議。

(三)國家資通安全重大計畫之諮詢審議。

(四)跨部會資通安全事務之協調及督導。

(五)其他本院交辦國家資通安全相關事項。

三、資安會報置召集人一人，由本院副院長兼任；副召集人二人，由本院院長指派之政務委員及相關部會首長兼任;協同副召集人一人，由國家安全會議諮詢委員兼任；委員十八人至三十五人，除召集人、副召集人及協同副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；非由機關代表兼任之委員得隨同召集人異動改聘之。

四、資安會報之幕僚作業，由本院資通安全處辦理。

五、資安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：由本院資通安全處主辦，負責整合資通安全（以下簡稱資安）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）及任務如下：

1.關鍵資訊基礎設施安全管理組：本院資通安全處主辦，負責規劃推動關鍵資訊基礎設施安全管理機制，並督導各領域落實安全防護及辦理稽核、演練等作業。

2.產業發展組：經濟部主辦，負責推動資安產業發展，整合產官學研資源，並發展相關創新應用。

3.資通安全防護組：本院資通安全處主辦，負責規劃、推動政府各項資通訊應用服務之安全機制，提供資安技術服務，督導政府機關落實資安防護及通報應變，辦理資安稽核及網路攻防演練，協助各機關強化資安防護工作之完整性及有效性。

4.法規及標準規範組：本院資通安全處主辦，負責研訂(修)資安相關法令規章，發展資安相關國家標準，訂定、維護政府機關資安作業規範及參考指引。

5.認知教育及人才培育組：教育部主辦，負責推動資安基礎教育，強化教育體系資安，提升全民資安素養，提供資安資訊服務，建構全功能之整合平臺，辦理國際級資安競賽，促進產學交流，加強資安人才培育。

(二)網際犯罪偵防體系：由內政部及法務部共同主辦，負責防範網路犯罪、維護民眾隱私、促進資通訊環境及網際內容安全等工作，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：法務部主辦，負責個資保護之宣導推廣，檢討修正維護民眾隱私及防制網路犯罪相關法令規章。

2.防治網路犯罪組：內政部及法務部共同主辦，負責網路犯罪查察、電腦犯罪防治及數位鑑識等工作。

3.資通訊環境及網際內容安全組：國家通訊傳播委員會主辦，負責促進資通訊環境及網際內容安全，協助防治網路犯罪等工作。

為積極研議國家資安政策及推動策略，強化產官學研資安經驗之交流及分享，充實資安作業能量，資安會報得設資通安全諮詢會。

六、前點第一項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。

資通安全諮詢會置委員十七人至二十一人，由資安會報召集人聘請資安領域有關之傑出人士及學者、專家擔任，任期二年，期滿得續聘之。

七、資安會報及資通安全諮詢會原則上每半年召開會議一次；必要時，得召開臨時會議，均由資安會報召集人主持。

八、資安會報及資通安全諮詢會委員、各組召集人，均為無給職。