國家資通安全發展方案

(114 年至 117 年)

行政院國家資通安全會報

中華民國 114 年 5 月

目　錄

壹、緣起.....1
貳、全球資安威脅與國際政策趨勢.....3
一、全球資安威脅趨勢.....3
(一) 新局面.....4
(二) 護關鍵.....4
(三) 新社會.....5
(四) 新科技.....5
二、國際資安政策發展趨勢.....5
(一) 美國.....6
(二) 歐盟.....8
(三) 英國.....9
(四) 日本.....9
(五) 韓國.....10
(六) 新加坡.....12
(七) 澳洲.....12
(八) 以色列.....13
參、我國資安推動現況.....15
一、組織架構.....15
(一) 網際防護體系.....16
(二) 網際犯罪偵防體系.....17
二、推動進程.....18
(一) 第一期機制計畫(90-93 年).....19
(二) 第二期機制計畫(94-97 年).....20
(三) 第三期發展方案(98-101 年).....21
(四) 第四期發展方案(102-105 年).....22

(五) 第五期發展方案(106-109 年) 23
(六) 第六期發展方案(110-113 年).....24
三、資安發展問題評析及應對策略 28
(一) 全球資安風險趨勢 28
(二) 臺灣資安發展評析與對策 29
肆、發展藍圖 32
一、願景 32
二、目標 33
三、推動策略 33
四、機關(單位)分工.....44
伍、預期效益 47
陸、推動組織、資源需求及計畫管理 50
一、推動組織 50
二、執行規劃 50
三、預算來源與執行 51
四、相關行動方案之管考 51
(一) 管考目的.....51
(二) 管考架構.....52
(三) 管考時程與執行程序.....52
(四) 績效指標設計原則.....53
(五) 持續改善與協調機制.....53
五、方案核定與修訂 54
柒、附件.....56
附件 1、各措施之工作項目 56
附件 2、行政院國家資通安全會報設置要點 65

圖目錄

圖 1　資安會報組織架構圖 16
圖 2　我國資安推動進程 19
圖 3　第七期國家資通安全發展方案架構 32
圖 4　第七期國家資通安全發展方案推動循環機制（PDCA） 55

表目錄

表 1　現階段資安發展 SWOT 分析 29
表 2　TOWS 分析矩陣 31
表 3　機關(單位)分工表 44
表 4　重要績效指標 49

壹、緣起

現今數位時代中，資訊傳播科技早已融入日常生活的各種面向，如物聯網(Internet of Things, IoT)、人工智慧(Artificial Intelligence, AI)以及第五代行動通訊網路(5th generation mobile networks, 5G)等技術。在享受科技便利的同時，亦伴隨著各類資安威脅，如進階持續性威脅(Advanced Persistent Threat, APT)攻擊、分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊、關鍵基礎設施(Critical Infrastructure, CI)攻擊等。資通安全(Cyber Security)對國家安全、公共利益、國民生活或經濟活動具有重大影響，必須提升國家資安防護能量，強化基礎通訊網路韌性及安全。

我國近年陸續推動「5+2 產業創新計畫」及「數位國家創新經濟發展方案(106 至 114 年)」(DIGI+方案)，並在奠基於 5+2 產業創新基礎上，打造「六大核心戰略產業」。賴清德總統上任後，推動「國家發展計畫(114 至 117 年)」落實「國家希望工程」之國政願景，與資通安全相關部分，包含打造「五大信賴產業」、可信任的資料流通機制、國土與數位安全；另外，113 年 7 月，行政院通過資通安全管理法修正草案送立法院審議，強化國家整體資通安全規範。

國家安全會議亦於 114 年 4 月 8 日公布《國家資通安全戰略 2025—資安即國安》，以「打造堅韌、安全、可信賴的智慧國家」為願景，提出以「全社會防衛韌性」、「國土防衛與關鍵基礎設施」、「關鍵產業與供應鏈」，以及「人工智慧應用與安全」等「四大支柱」為核心的策略佈局，包括零信任架構推行、主動防禦能力建構、國際聯防深化、人工智慧應用安全等關鍵措施。

鑒於資通訊服務應用廣泛，以及我國重大科技創新政策，對於國家安全，甚至是社會經濟活動各種應用層面，資通安全皆扮演關鍵角色，為能因應國際趨勢與新型態資安攻擊與威脅，在既有的防禦基礎

及面向上延續我國的資安防護能量與優勢，除持續落實第六期國家資通安全發展方案(110 年至 113 年)，行政院國家資通安全會報(以下簡稱資安會報)為逐步提升我國資通安全防護能量，爰據以提出「國家資通安全發展方案(114 年至 117 年)」(以下簡稱本方案)，作為我國推動資安防護策略與計畫之依循目標。

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)《2024 全球風險報告》等報告指出，科技發展加速、氣候變遷、地緣政治結構轉變及人口結構分歧，影響了全球風險，AI 技術的進步，使得假訊息與錯誤訊息成為未來兩年內首要風險；同時，AI 發展的假消息和社會極化、國際衝突等地緣政治問題密不可分，可能引起跨域網路犯罪或是關鍵基礎設施資訊系統的癱瘓；同樣列為五大風險之一的網路攻擊，因為 AI 將變得更加快速發展而嚴重。

隨著數位系統廣泛使用及日漸複雜化，不斷擴大的網路威脅也正在「超過社會有效預防及管理的能力」，也因為系統安全漏洞不斷增加，網路上的惡意活動也出現激增。根據 Check Point 資料，在 2024 年下半年，全球網路攻擊次數較去年同期增加 75%，而我國每週遭受攻擊次數年增 44%，位居亞太地區第一。網路威脅在數量和強度上都顯著增加，而教育與研究機構、政府與軍事機構和醫療保健機構則成為三大最易遭受攻擊的目標。

網路攻擊引發的資通安全事件，在地緣政治和科技發展下，成為重要的議題，參考 113 年全球資安威脅與相關研究案例，歸納出四大面向資安威脅趨勢，包含「新局面」、「護關鍵」、「新社會」、「新科技」，茲說明如下：

(一) 新局面

Google Cloud 2024 年網路安全預測報告顯示三大國際網路安全相關趨勢，包含鎖定大選的網路活動、干擾性攻擊的駭客行動主義興起，以及清除程式將成為國家網路軍火庫標配。Check Point 2024 年八大網路安全趨勢預測亦表示，由國家支持的駭客激進主義恐將延續，來自全球地緣政治緊張局勢，國家安全、企業全球營運、實體與數位安全風險，都帶來新挑戰。

(二) 護關鍵

根據 Check Point 2024 年八大網路安全趨勢預測，供應鏈和關鍵基礎建設攻擊將加劇。物聯網設備與硬體部分，針對物聯網設備網路攻擊急遽增加，2023 年與 2022 年相比，物聯網設備平均每週攻擊次數增加 41%，平均每週有 54%組織遭受攻擊。網路犯罪組織意識到，物聯網設備是網路中最脆弱的部分之一，多未有適當的保護或管理，駭客可以利用易受攻擊的應用程式權限，將命令注入到程式中，物聯網設備的廣泛採用使此類漏洞成為網路犯罪分子的主要目標。

軟體供應鏈部分，Gartner 預測，到 2025 年全球 45%組織將遭受軟體供應鏈攻擊，將比 2021 年增加三倍。供應鏈攻擊以第三方供應商與服務提供者為目標，以取得對其客戶系統與資料存取權限。包括：零時差/軟體漏洞，針對供應商使用韌體、軟體進行攻擊；憑證竊取，透過網路釣魚或系統漏洞等攻擊取得供應商系統存取憑證；資料竊取，入侵供應商系統取得營運或客戶機敏資料。

(三) 新社會

數位不平等是自疫情以來嚴重風險之一，新社會需要努力提供數位基礎設施、數位技能培訓、數位服務等，以實現數位包容和數位公民權。同樣情形發生在資通安全領域，Gartner 2024 年網路安全主要趨勢調查，資安人才供需存在差距、企業內部數位能力分散，有待投入人力之培訓。

(四) 新科技

隨著人工智慧與新興技術發展，多份報告均指出生成式 AI 的出現將成為風險，且有利於網路釣魚與虛假資訊傳播。CISA 曾表示 90%以上網路攻擊都是從網路釣魚開始，網路釣魚仍是最主要攻擊媒介。Cloudflare 報告指出，欺騙性連結占網路釣魚威脅 35.6%，寄發看似合法 URL，使用者點擊該 URL 可能會導向惡意網站或開啟應用程式，使得駭客可以植入惡意程式或竊取資訊。

除了 AI 之外，雲端科技的發展將改變數位生態系的組成，Google Cloud 2024 年網路安全預測報告，攻擊者仰賴雲端無伺服器服務，針對混合雲和多雲攻擊日益成熟且破壞性大。

二、國際資安政策發展趨勢

本節綜整研析世界主要國家或國際組織之重要資通安全政策與規範，如美國、歐盟、英國、日本、韓國、新加坡、澳洲及以色列，並整理其針對網路攻擊模式演變所提出的因應對策，作為本方案之參考。

(一) 美國

1. 網際安全框架 2.0

美國國家標準技術研究院(National Institute of Standards and Technology, NIST)於 2024 年 2 月 26 日正式公布《網路安全框架 2.0》(Cybersecurity Framework, CSF)。相較 2014 年的 1.0 版本，CSF2.0 適用範圍不僅是關鍵基礎設施安全，更進一步全面性協助所有組織應對各種規模的網路安全挑戰。

CSF 2.0 框架，除了延續「識別(Identify)」、「保護(Protect)」、「偵測(Detect)」、「回應(Respond)」、「復原(Recover)」等五大核心，新增「治理(Govern)」強調網路安全風險是企業風險的主要來源之一，高階管理者應將企業治理相關風險一起考慮，適時調整組織的風險管理策略。

2. AI 風險管理框架

美國國家標準技術研究院(National Institute of Standards and Technology, NIST)於 2023 年 1 月 26 日發布《人工智慧風險管理框架 1.0》(Artificial Intelligence Risk Management Framework, AI RMF)版，提供靈活、結構化和可衡量的流程，幫助設計、開發、佈署或使用人工智慧系統的組織管理 AI 風險。

3. 國家資通安全戰略

2023 年 3 月 2 日，美國公布新版《國家資通安全戰略》為拜登之資通安全政策。其中，以建立「可防禦、有韌性的數位生態系統」為目標，有其 5 大支柱共 27 項措施。

五大支柱如下：支柱一保護關鍵基礎設施。支柱二：破壞並摧毀威脅行為者。支柱三：塑造市場力量以推動安全與韌性。支柱四：投資於韌性未來。支柱五：建立國際夥伴關係以追求共同目標。

4. 拜登行政命令

為因應美國軟體開發商 SolarWinds 產品遭駭客組織入侵、微軟 Exchange Server 爆發零時差攻擊行動，以及美國最大燃油供應業者 Colonial Pipeline 遭勒索軟體攻擊等資安事件，美國總統拜登於 2021 年 5 月 12 日簽署行政命令，要求改善美國網路安全並保護聯邦政府網路，內容包括推動美國聯邦政府網路安全現代化，要求導入零信任架構之網路安全策略，改善軟體供應鏈安全，以及建立安全審查委員會等。此外，美國國家標準技術研究所(National Institute of Standards and Technology, NIST)宣布與產業合作，共同開發新技術框架，以提升軟體供應鏈安全性與完整性。

2023 年，美國前總統拜登簽署行政命令，要求 AI 開發者與政府分享安全測試結果，並且頒布指示建立國家 AI 安全機構：美國 AI 安全研究院(AI Safety Institute)。但是 2025 年 1 月份美國總統川普上任後，隨即裁撤這項命令。

2025 年 1 月，拜登政府簽署另一項行政命令，針對聯邦政府軟體供應商設定安全要求，並要求雲端服務供應商針對安全營運資訊保持公開透明，聯邦政府內部加強安全措施，並由 NIST 提供指引補強供應鏈安全與漏洞，以避免更多針對政府的網路攻擊事件發生。此項行政明令未遭到裁撤。

(二) 歐盟

1. 網路韌性法案

歐盟執委會於 2022 年 9 月中公布《網路韌性法案》(Cyber Resilience Act)草案，2024 年 10 月 10 日經歐盟理事會通過，強化數位產品安全性，包括物聯網產品設備及服務的網路安全要求，預估 2027 年底前提供相關軟硬體服務的廠商需要合規。一旦發現違規情事，歐盟監管單位會召回產品，或者強迫退出歐洲市場。《網路韌性法案》指出，聯網裝置的網路安全性低漏洞無所不在，缺乏安全更新亦無向用戶提供足夠的安全防護資訊。在萬物聯網的環境中，一旦某個產品爆發資安事件，即可能波及整體供應鏈安全，加深企業對於操作系統、網路設備和軟體存在漏洞的隱憂。

歐盟物聯網設備製造商必須在為期 5 年或是產品預期壽命期間，評估產品的網路安全風險，並採取適當的步驟來解決問題。企業必須在發現問題 24 小時內將資安事件通知歐盟網路與資訊安全局，並採取相關措施解決問題。而進口商和經銷商亦會被要求驗證產品是否符合歐盟網路安全規範。未來凡是連網裝置，都必須符合各項網路規定，才能獲得認證標章在歐洲地區販售。

2. 網路與資訊系統安全指令

作為歐盟網路安全管理規定法律化首要部分的《網路與資訊系統安全指令》(Security of Network and Information Systems, NIS)，在 2016 年正式公布實施。2020 年底為因應日益嚴重的網路威脅，歐盟執行委員會提出修正提案 NIS 2，目的是增修 NIS 指令以適應未來需求。2023 年 1 月 16 日正式生效，納入公共電子通訊網路或服務供應、特定關鍵產品(如藥品、醫療器材)製造、社交網路平台與資料中心相關數位

服務、太空及公共行政等類型，並以企業規模區分，所有中大型企業須遵守，而具高度風險小型企業由成員國自行規範。

(三) 英國

英國政府提出產品安全與電信基礎設施(Product Security and Telecommunications Infrastructure, PSTI)法案於 2024 年 4 月生效，目的為提升聯網設備的安全性。第 1 部分針對智慧設備提出資安防護措施，旨在保護消費者避免遭受資安攻擊事件；第 2 部分則屬於電信基礎設施指南，以加速設備之安裝、使用及升級。參與消費性物聯網產品供應鏈的企業都需遵守法案，違反將面臨罰款。

(四) 日本

1. 經濟安全保障推進法

日本於 2022 年 5 月 18 日公布《經濟安全保障推進法》，為了確保、防止經濟相關活動危害國家安全，該法自公布後 2 年內(至 2024 年 5 月 17 日)分階段施行。日本已於 8 月 1 日設立「經濟安全保障推進室」承擔與相關省廳調整作業、制定基本方針及公共評論等，將與日本國家安全保障局共同完成經濟安全保障政策。

《經濟安全保障推進法》的核心目標為，確保關鍵基礎設施安全、半導體供應、確保戰略技術和物資、防止技術外流等。該法適用於 14 個產業，包括：電力、天然氣、石油、水資源、電信、廣播、郵政、金融、信用卡、鐵路、貨運、海運、航空與機場等。有關電力、天然氣、石油與其他關鍵基礎設施的營運商在採購設備前必須取得政府核准，此舉在保護網路安全，以避免受到網路攻擊。日本政府認為相關

風險主要來自中國製造的產品，因此，企業必須充分揭露設備的製造商與產地國，若存在被駭的合理風險，日本政府有權阻止相關設備之採用，該舉措的目的是保護關鍵基礎設施系統，避免因網路攻擊而導致重大社會事件與經濟劇變。

2. ICT 網際安全綜合對策

日本總務省於 2022 年 8 月 12 日發布《2022 年 ICT 網際安全綜合對策》，將著重實施「確保資通訊網路安全與信賴性」、「提升網路攻擊自主應對能力」、「推動國際合作」與「推動普及與啟蒙」。

(五) 韓國

1. 2024 年版《資安標準化技術戰略藍圖》實施計畫

2023 年 10 月，韓國情報通信技術協會(Telecommunications Technology Association, TTA)發布 2024 年版《資安標準化技術戰略藍圖》實施計畫，將資安國際標準化戰略地圖作為推進技術前瞻及應用技術發展的具體規劃。戰略藍圖以(1)新興資安技術(如，虛擬實境和人工智慧等)的開發與推動標準化、(2)資訊安全應用的標準化、(3)持續優化既有技術，以確保標準化領先地位為目標，選取了「安全多方運算技術」、「量子安全加解密技術」、「元宇宙話者辨識技術」、「去識別化驗證技術」、「Host based 侵害行為評估技術」、「網路基因組核酸萃取分析技術」、「密碼模組篡改回應技術」、「雲端 IT 產品資安評估技術」、「寵物用生物辨識身分認證技術」、「自動駕駛辨識生物學生技術」、「嵌入式開放型影像資安平台技術」、「智慧城市影像異常預測技術」等 12 個新興及重要的資安技術推動國際技術標準。TTA 考量個

別技術的成熟階段與韓國技術優勢，進行了專家的系統化評估與細緻分析，確認韓國 2028 年資安技術標準化藍圖。

2.《國家資安戰略》

2024 年 2 月 1 日，韓國發佈新版《國家資安戰略》，本次策略由總統府國家安保室發布，同時在執行國家資安戰略目標的過程中，必須堅持以下三大原則；(1)須平衡國家核心價值和人民經濟利益、(2)所有產官學研利益相關者須認識到資安的重要性，共同應對威脅、(3)將基於合法目的與規範，推展維護公民隱私等基本權利，以免權益受到侵害。國家資安戰略主要以「加強防禦進攻性資安」、「積極建構國際合作體系」、「強化國家核心設施的資安韌性」、「掌握新興技術的競爭優勢」、「強化服務執行基盤」等五大議題。國家資安戰略以每五年修訂一次為原則，因依內外部環境變化對國家資安的影響程度，可以經國家資安委員會審議決定後進行修改。

3. 資安產業確保全球競爭力策略

2023 年 9 月，韓國科學技術情報通信部發布《資安產業確保全球競爭力策略》規劃，設定在 2027 年，期望促成培育一家資安獨角獸企業，以帶動韓國資安產業市場達到 30 兆韓元(約新臺幣 7,247 億元)的規模，為此，還研擬提出四大核心策略：策略一掌握資安轉型關鍵創造新興市場、策略二建立業界合作基礎以迎新興市場、策略三以建構強韌生態鏈攻略國際市場，及策略四確保新一代資安技術競爭力。

(六) 新加坡

1. 資通安全策略

有鑑於網路攻擊行為日益複雜及頻繁，CSA 召集產學界利益相關者，共同制定 2021 年《資通安全策略》(Singapore Cybersecurity Strategy)，延續 2016 年《資通安全策略》進行更新，加強數位基礎建設的安全及韌性，使網路空間更加安全，展開與關鍵資訊基礎設施(Critical Information Infrastructures, CII)的合作，支持新加坡的數位生活。

2. 工控職能框架

新加坡政府積極重視推動 OT 資安，發布搭配人才發展策略，與 Mercer Singapore 聯合開發《OT 職能框架》，描繪各個角色的職能指南，並列出相關核心技能。

3. 網路安全(修正)法案

新加坡國會於 2024 年 5 月 7 日三讀通過《網路安全(修正)法案》(Cybersecurity Amendment Bill)，該法主要針對國家安全、國防、外交、經濟、公共衛生等重要方面的資訊設備與機構加強監管，不致影響多數企業。修正法案賦予新加坡網路安全局審查權力，可要求受監管機構提供紀錄、賬目及文件。

(七) 澳洲

2023 年 11 月，澳洲政府發布《2023-2030 資通安全戰略》(2023-2030 Australian Cyber Security Strategy)，為產學界、各州、領地政府以及國際社群共同制定，提出實現國家級網路安全的藍圖，包括公私合

作夥伴、關鍵基礎設施的韌性、數位素養(Digital Literacy)、產學合作以及加強相關政策框架等面向，改善澳洲資通安全與保護網路環境。

《2023-2030 資通安全戰略》的六個網路盾牌如下：強壯的企業和公民、安全技術、世界級威脅分享與防禦、保護關鍵基礎設施、主權能力、區域與全球韌性領導力。

戰略目標包含加強資安人才培育，與全球合作夥伴共同支持和捍衛網路空間國際秩序。澳洲外貿部制定政策吸引外國專業人才，以及來自工程人才大國的投資。藉由此類交流，澳洲盼能推廣澳洲研究、支持產業主導的貿易代表團和監控國際技術市場。

(八) 以色列

以色列國家資通安全局(Israel National Cyber Directorate, INCD)曾於 2021 年發布《以色列國際網路策略(Israel International Cyber Strategy)》，顯示出政府對於國際合作的重視，該報告指出，以色列國際網路策略之核心為建立全球網路韌性，包括網路防禦合作、能力與信心建立措施、新興科技的前置準備等三部份。此策略不僅有助於建立國際合作關係，亦可藉此同步提升以色列國內資通安全水準。

2022 年 2 月 28 日，以色列宣布透過國家資通安全局及財政部捐 2 百萬新謝克爾予美洲開發銀行(Inter-American Development Bank, IDB)，以幫助拉丁美洲及加勒比海地區提升資通安全能力。於 3 月 2 日再度宣布，將與美國國土安全部擴大有關資通安全及新興技術領域的合作，具體內容包括推動採用成熟的資通安全技術、加強資通安全訊息共享及相關能力，以及促進雙邊專家交流。另外，美、以兩國亦簽署一份備忘錄推動交通運輸產業的關鍵資通安全合作。

以色列已與數十個國家及組織簽訂網路防禦合作協議，舉辦國際網路會議，透過經驗分享促進全球網路韌性及合作。

參、我國資安推動現況

一、組織架構

行政院資通安全會報(以下稱資安會報)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，107 年 6 月 6 日公告資通安全管理法，統整國家資通安全機制，將國家整體資安工作正式法制化。111 年 1 月 19 日總統令公告數位發展部組織法，數位發展部於 111 年 8 月 27 日正式掛牌成立，擔任資安會報的幕僚單位，並研擬國家資通安全基本方針、政策及重大計畫，以及制定相關法規及規範。

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 112 年 7 月 20 日修正之「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。

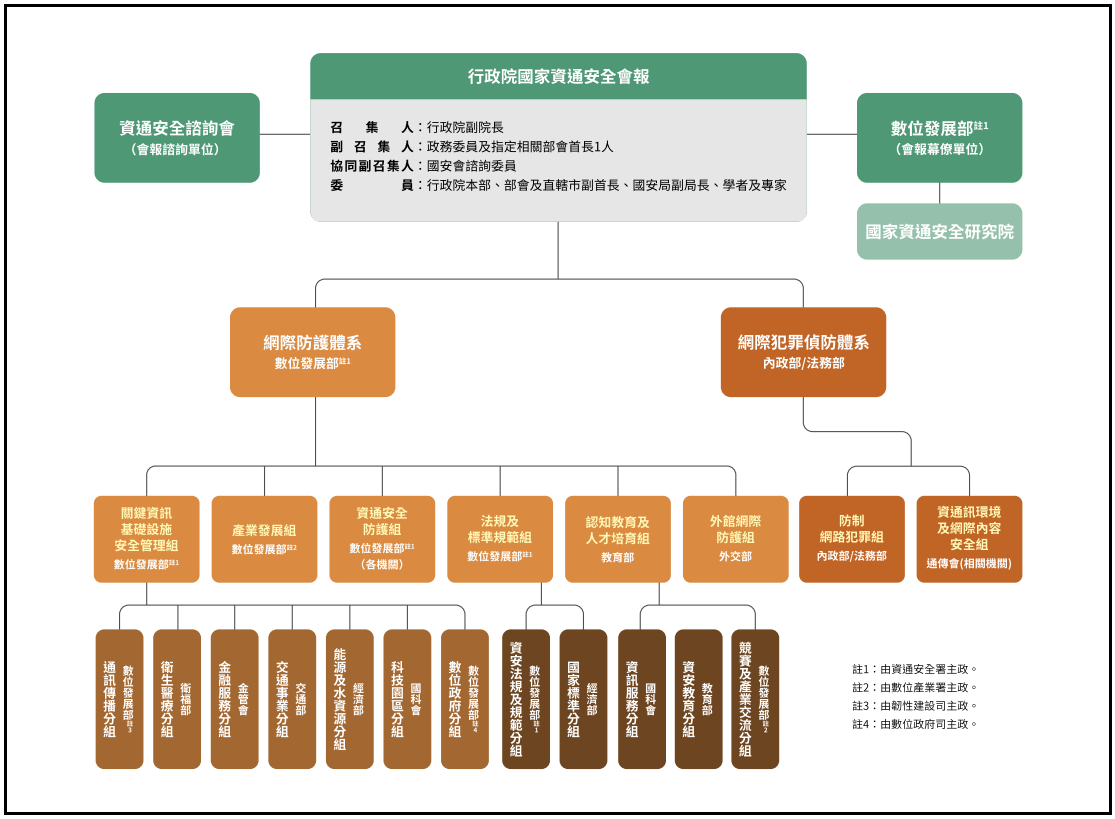

圖 1　資安會報組織架構圖

(一) 網際防護體系

由數位發展部主辦(資通安全署主政)，負責整合資通安全防護資源，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：數位發展部主辦(資通安全署主政)，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：數位發展部主辦(數位產業署主政)，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：數位發展部主辦(資通安全署主政)(各機關)，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：數位發展部主辦(資通安全署主政)，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。

6. 外館網際防護組：外交部主辦，負責統合外館各合署機關之資訊及網路管理，以提升外館資通安全防護能力，降低發生網駭及資安事件之風險。

(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. 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、數位鑑識及檢討防制網路犯罪相關法令規章等工作。

2. 資通訊環境及網際內容安全組：國家通訊傳播委員會主辦，負責促進資通訊傳播環境及網際內容安全，推動通訊傳播事業配合辦理防治網路犯罪及維護網際內容安全等措施，協助防治網路犯罪等工作。

為提升國家資通安全科技能力、推動資通安全科技研發及應用，於 112 年 1 月 1 日特設國家資通安全研究院，研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際合作交流、協助規劃及推動國家資通安全防護機制、協助政府機關(構)及關鍵基礎設施重大資通安全事件應變處置、協助規劃及支援國家關鍵基礎設施之資通安全防護、協助規劃及培育資通安全專業人才；推廣全民資通安全意識、支援具有特殊敏感性之政府機關(構)資通安全防護工作、支援產業資通安全重大發展及法規推動之需求。

另在民間資安推動的部分，數位發展部轄管之「臺灣網路資訊中心」(Taiwan Network Information Center, TWNIC) 負責維運「臺灣電腦網路危機處理暨協調中心」(Taiwan Computer Emergency Response Team/Coodination Center, TWCERT/CC)，TWCERT/CC 主導推動民間資安事件通報、資安教學資源提供及舉辦資安宣導活動等多項工作，協助民間單位建立產業內部 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，以縮短資安事件處理時效。

二、推動進程

資安會報自 90 年迄今，陸續推動 6 個階段、各為期 4 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。

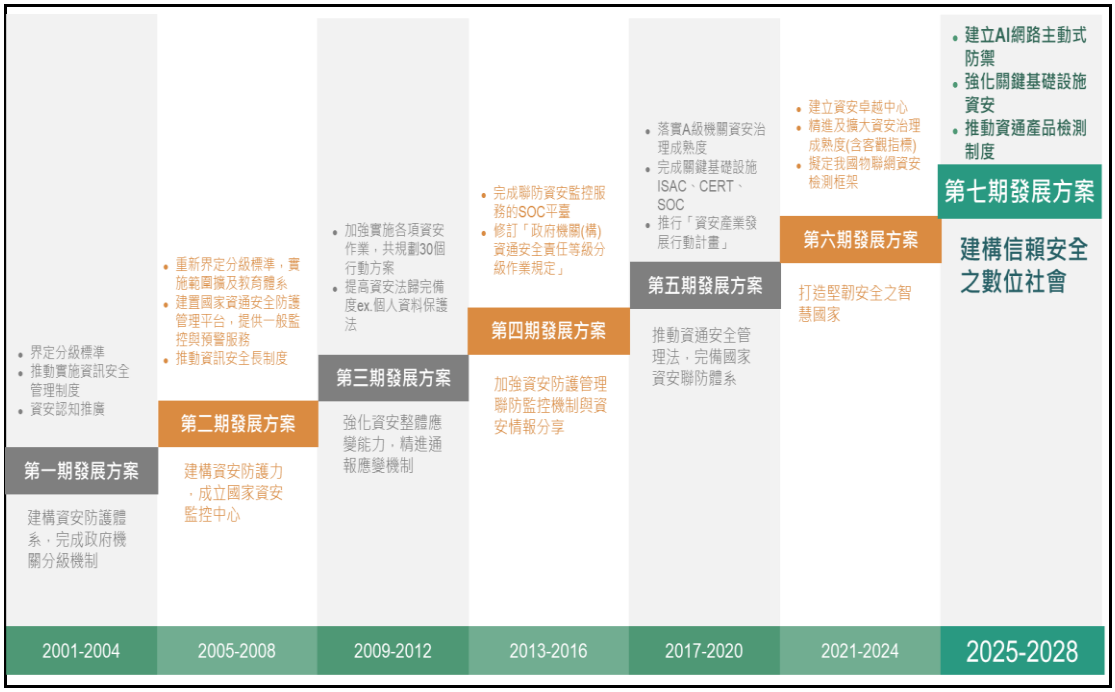

圖 2　我國資安推動進程

(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 日行政院頒布「建立我國通資訊基礎建設安全機制計畫」(第一期機制計畫)，以「確保我國擁有安全、可信賴的資訊通訊環境」為願景。本期主要成果為建構資安防護體系，成果包含：

1. 成立資安會報，同時成立技術幕僚單位資安會報技術服務中心，作為我國負責資通安全建設與政策的主責單位。
2. 針對涉及國家民生的重要政府機關推動資通安全管理制度，透過建立機關資通安全危機事件通報及預警機制、責任等級分類標準，對於不同責任等級的機關提供對應的資安支援與工作要求，並針對受指定機關進行資安外稽。
3. 針對資訊人員推廣資安教育訓練、加強通資訊安全人力培訓及觀念宣導、提升大眾資安認知等。

4. 檢討及增修訂通資訊安全相關法令、訂定通資訊安全技術標準及規範，建立產品檢驗及保證機制。
5. 針對 CI 的重要作業系統，規劃推動建置資訊安全管理制度(Information Security Management System, ISMS)，以及資安監控中心預警及通告機制與人員訓練等資安管制方案。

(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

延續第一期機制計畫，行政院於 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)」(第二期機制計畫)，持續強化我國整體資安防護基礎，重要成果包含：

1. 建置國家資通安全防護管理平台(National Security Operation Center, N-SOC)，針對重要核心政府機關提供監測、預警服務，進行 24 小時防護。
2. 建立政府機關資訊安全長(Chief Information Security Officer, CISO)機制，指定部會業管資通安全業務之副首長兼任資訊安全長，推動執行單位內資通安全相關計畫。
3. 擴大政府機關資安責任等級分級作業實施範圍，大幅增加重要政府機關納入資安防護體系的數量，並將實施範圍擴及教育體系。
4. 推動教育體系導入 ISMS，以及輔導縣(市)教育網路中心建置 ISMS。
5. 透過稽核提升作業成效，各機關導入內部稽核制度，落實資安相關推動工作，並持續針對公民營單位進行資安外稽，提供稽核建議。

6. 延伸資通安全計畫防護領域，加強訂定促進線上交易安全與保障民眾個人資料的資通安全計畫。

(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

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)」(第三期發展方案)，以「安全信賴的智慧臺灣，安心優質的數位生活」為願景，將政府推動資安經驗擴散至民間，逐步強化民間的資安防禦機制。主要成果如下：

1. 建立資安事件偵測、識別及分析回應等應變程序，提升通報時效，持續強緊急通報、應變及復原等能力。
2. 推動政府 A、B 級機關導入資安治理及績效評估，要求機關依需求配置資安專責及兼辦人力，建立資訊系統分類分級及對應的基本資安防護需求
3. 採用「規劃－執行－檢查－行動」(Plan-Do-Check-Act, PDCA)過程模型，藉以提升政府機關資訊安全管理水準，降低相關作業風險，並推動國內政府機關與民間企業通過國際資安標準驗證(如 ISO 27001)。
4. 強化電子商務信賴安全，加強線上交易安全身分認證機制，推動運用公開金鑰基礎設施(Public Key Infrastructure, PKI)憑證服務。
5. 促進事業機構運用第三方評鑑，依法規授權加強對各目的事業資安查核，促使業者強化個資保護、建立資安管理制度、辦理內稽及委託第三方進行資安外稽。
6. 強化資安研究能量，鼓勵高教體系開設資安課程，培育資安專業研究人才，研發關鍵資安技術，移轉提供產業加值應用。

7. 宣導強化資安概念，推動各級學校資安認知活動、針對企業宣導檢視自身資訊資產安全、辦理全民資安健檢及競賽等活動，提升全民資安認知程度。

(四) 第四期發展方案(102-105 年)

加強資安防護管理聯防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)」(第四期發展方案)，以「建構安全資安環境，邁向優質網路社會」為願景，強化中央政府因應資安攻擊的對抗能力為重心，推動四大目標如下：

1. 國家政策與環境建構：持續增修資安政策、規範、指引、標準及手冊，盤點我國資安相關法規，研議制定資安專法；推動各政府機關資安合理人力及預算機制，每年辦理資安服務廠商評鑑；辦理「國家資通安全科技中心」籌設及運作事宜，推動行政法人化；推動資通設備安全驗證作業，積極與國際認驗證組織交流，並定期檢討檢設項目
2. 資安防護與情資分享：推動建立政府資安治理架構，評估 A、B、C 級政府機關資安治理成熟度；成立 iWIN 網路內容防護機構，以強化網路內容安全管理機制；落實資安攻防演練，規劃資安情境演練與實兵演練；推動政府資安管理制度，提升政府機關資通安全管理作業；推展資安基礎環境安全設定，持續規劃不同系統政府組態基準(Government Configuration Baseline, GCB)設定；增進資安威脅情報蒐集能量，強化資訊分析與分享機制。
3. 產業發展與技術升級：建構資安防護技術研究能量，強化新興資安自主技術競爭力；加強與企業及學研機構的資安技術研發合作，進

行新興資安技術實務的應用；強化犯罪偵查應用、完善數位證據保全、推動數位鑑識實驗室，即時掌握資安犯罪動向；針對當期重點技術，如行動裝置、行動應用程式、無線網路、安全軟體發展生命週期(Secure Software Development Lifecycle, SSDLC)等，建置相應安全檢測機制。

4. 人才培育與國際交流：推動資安專業訓練認證機制，規劃建立資安專業人員登錄與認證機制；建立資安職能評量制度，規範各職類人員定期完成資安職能課程訓練並通過課程評量。

(五) 第五期發展方案(106-109 年)

推動資通安全管理法，完備國家資安聯防體系

行政院於 106 年核定「國家資通訊安全發展方案(106 年至 109 年)」(第五期發展方案)，以「打造安全可信賴的數位國家」為願景，推動我國資安縱深防禦及聯防體系，穩固我國數位國土的資安防線，推動重點成果如下：

1. 完備資安基礎環境：通過資通安全管理法及六項子法正式施行，奠定了資安法制基礎並要求落實各項資安作業；建構資通訊產品的安全標準及推動資通訊產品資安檢測暨認驗證制度，優先針對市場規模大且影響民生的物聯網（IoT）產品裝置制定資安標準。
2. 建構國家資安聯防體系：統籌中央主管機關與關鍵基礎設施（CI）提供者資安防護，透過國家層級橫向聯防形成「三層式資安聯防架構」，強化國家關鍵基礎設施安全；推動各層級資訊安全監控中心（SOC）、電腦緊急應變小組（CERT）及資訊分享與分析中心（ISAC）等聯合防護機制，強化情資掌握、事件通報應處及整合分享應用；以六都地方政府為核心推動區域聯防，結合鄰近縣市與學

研機構合作培育人才，完成區域 ISAC（皆為國家級 N-ISAC 會員）與 SOC 建置，推升地方資安情資自主能量。

3. 推升資安產業自主能量：公布採購原則鼓勵公部門優先採用國產資安產品，帶動產業發展並強化國家防護能量；建置資安整合服務平臺（SecPaaS）媒合資安服務供需方，協助業者導入產品試煉與實證，推動垂直整合解決方案；結合資安新創社群辦理技術交流活動，深化產學研合作與技術紮根，促進白帽駭客社群產業化及引導企業投資。
4. 孕育優質資安人才：增設公費留學資安學門，推動大學成立資安碩士班，透過「臺灣好厲駭」實務培訓及 AIS3 暑期進階課程強化學生實作能力；開辦全職養成班與不同產業領域在職人員短期培訓，強化產業即戰力與資安能量；透過 TWISC 中心聯盟向下成立特色中心，產出豐碩的研究發表、產學合作與技轉成果，全方位建構臺灣資安人才庫。

(六) 第六期發展方案(110-113 年)

打造堅韌安全之智慧國家

行政院於 110 年核定「國家資通訊安全發展方案(110 年至 113 年)」(第六期發展方案)，以「打造堅韌安全之智慧國家」為願景，並以「成為亞太資安研訓樞紐、建構主動防禦基本網路、公私協力共創網安環境」為目標，四項推動策略，分別從「吸納全球高階人才，培植自主創研能量」、「推動公司協同治理，提升關鍵設施韌性」、「善用智慧前瞻科技，主動抵禦潛在威脅」及「建構安全智慧聯網，提升民間防護能量」等四大面向著手，其執行重點推動成果說明如下：

1. 吸納全球高階人才，培植自主創研能量

(1)教育部培育並輔導可投入資安產業或成為資安新創人才，開設EC-Council Certified Ethical Hacker (CEH)駭客技術專家認證課程，共41名學員通過證照考試；優化15門資安實務示範課程教材資源內容，並鏈結新興應用場域開設課程，培育資安實務人才，110年至113年推廣至大學校院資安課程中使用，已融入計516門課程中使用，修課人次逾2萬人次。數位發展部資通安全署培養我國高階技術人才，邀請國外資安知名人士自110年至113年辦理實戰人才菁英班，計培植452名頂尖資安技術人才。數位發展部數位產業署協助企業在職資安人才培育，自110年至113年累計培育5,114人次。

(2)國家科學及研究委員會110年至113年累計開發重要資安技術/機制 153 項，並串接產學研，促成產學合作及技術移轉金額近8,815 萬元。數位發展部資通安全署成立資安卓越中心，長期目標係成為亞太高階資安人才及技術創新基地，每年均提出至少9篇資安相關前瞻研究論文或報告，並延攬6位國外高階研究人員擴充研究團隊規模，提升整體資安防護量能，並與國際技術或研究機構累計簽定4個合作協議書或MoU，且持續開發及接觸可合作之國外資安技術或研究機構。

2. 推動公私協同治理，提升關鍵設施韌性

(1)數位發展部資通安全署推動資安法修正草案，業已踐行相關法制作業程序，包含辦理修正草案說明會蒐集意見、進行草案預告、召開跨院部會、地方政府等機關協商會議、政委審查會議及提報行政院院會通過核轉立法院審議，以適時檢討以因應國際資安防護趨勢；並滾動調修納管機關資安責任等級，確保納管機關資安防護要求之妥適，截至113年底為止，已累計587個機關資訊向上集中。

(2) 交通部訂定交通領域工業控制系統資安防護基準，包含 9 大防護構面，計 90 項控制措施，供所管 32 家特定非公務機關依循。經濟部 111 年公告「經濟部能源與水資源領域工業控制系統資安防護基準」並修訂「經濟部能源及水資源領域工業控制環境資安防護建議」，110 至 113 年已完成 27 個場域防護基準輔導。衛福部 112 年發布「醫療關鍵基礎設施醫院醫療儀器相關系統資通安全防護基準」。數位發展部發布關鍵電信基礎設施資通設備資通安全檢測技術規範。各 CI 主管機關落實稽核 CI 提供者及每年均辦理資安攻防演練，110 至 113 年完成 116 家 CI 提供者資安稽核，以督促其落實資通安全管理法法遵及資安防護措施。

3. 善用智慧前瞻科技，主動抵禦潛在威脅

(1) 數位發展部數位產業署 110 至 113 年累計研發 24 式主動式智能偵防技術，執行主動式防禦技術場域實證累計達 42 家，協助企業主動抵禦潛在資安威脅，並研發「勒索軟體智能獵捕平台」，可有效透過三大模組(人工智慧、防毒軟體及沙箱)來協助使用者辨識惡意程式與軟體，自動化建立惡意檔案資料庫並應用於 AI 偵防模型，在駭客造成傷害前先一步阻斷威脅，避免企業再次受到勒索病毒入侵，榮獲 2022 年美國 R&D 100 百大科技研發獎。

(2) 數位發展部資通安全署發展主動式防禦手法相關技術與應用情境，並完成實作驗證，擴充系統功能與整合驗證已發展之攻擊情境，驗證駭客攻擊手法與流程，以剖析新興駭客攻擊手法，提醒政府機關留意攻擊威脅與強化資安防護，110 至 113 年已累計完成實作驗證 8 套攻擊情境。完成研擬完成零信任驗證機制與部署機制，111 至 113 年分別於文化部及退輔會完成零信任架構之身分鑑別、設備鑑別及信任推斷機制試行，並辦理零信任產品驗測，計有 16 項身分鑑別產品及 3 項設備鑑別產品通過功能符合性驗證。

4. 建構安全智慧聯網，提升民間防護能量

(1)數位發展部完成滾動修正資通安全維護計畫參考框架暨稽核計畫 1 份，以完備 5G 網路資安管理機制與相關資安法規，並推動建置通訊領域軟體安全實驗室，為 5G、系統廠商及物聯網相關業者提供檢測服務，以提升該等產業資安體質。數位發展部數位產業署 110 年針對 5G 通訊、智慧製造、遠距辦公等領域，打造解決領域需求及新興資安議題之解決方案，並進行場域實證；111 年聚焦於製造業，發展能解決產業共通性問題之整合型資安方案，藉由推動資安業者於指標製造業場域進行導入實證；112 年起以臺灣自主研發的零信任資安解決方案為推動主題，將新興資安技術導入電商、數位內容、資訊服務、電信、高科技製造等產業場域；113 年度由企業主領頭打造供應鏈安全的零信任資安示範場域。

(2)數位發展部資通安全署 113 年協處國內企業資安通報共 458 件，惡意檔案檢測服務達 1,800 件，審核並發布國內產品資安漏洞(CVE)計 168 個，並協調廠商修補產品漏洞，以提升我國資通訊產品信賴度；並依據國內外最新資安法令及標準修定「資通系統防護基準驗證實務」等 10 項參考指引，提供政府機關及民間資安需求使用。數位發展部數位產業署透過制定我國標準及測試規範，完成與 SESIP 標準調和，在標準面層面達成國際接軌；建立我國晶片安全檢測實驗室並取得國際認證，培養我國晶片安全檢測能量，在檢測能力上與國際對接；協助我國晶片產品業者通過 SESIP 產品驗證，實現「在地檢測，全球通行」。

三、資安發展問題評析及應對策略

(一) 全球資安風險趨勢

世界經濟論壇(World Economic Forum, WEF)在 2024 年 1 月 10 日公布了 2024 年度「全球風險報告」(Global Risks Report)，對氣候變遷、生活成本危機和戰爭帶來的威脅提出示警。認為「極端氣候和地球系統重大變化」是最令人擔憂的長期問題，但是 AI 技術快速發展產生的錯誤訊息和惡意假訊息，則是短期內最大的風險。由於錯誤訊息和惡意假訊息的擴散、社會被極端化和分裂，再加上人口的老化和不平衡等社會問題將導致信任危機、衝突暴力、貧富差距等社會風險。而在科技風險方面，人工智慧、生物技術、網路安全等前瞻技術的快速發展，將帶來新的機遇和挑戰，但也可能引發道德、法律、人權等方面的爭議和風險。

除了 WEF 公布的 2024 年全球風險報告，全球風險集團，歐亞集團也對 2024 年面臨的政經風險進行預測，包括日益複雜的國家環境風險，認為世界將進入 G-Zero 的世界，亦即一個沒有全球領導力的世界，美國的國內挑戰，使其不在扮演世界警察的角色。加上進行中的三場區域戰爭，將主宰 2024 年世界事務，引起全球地緣政治緊張局勢，也危及企業全球營運、為實體與數位安全風險帶來新挑戰。

另外，也認為數位落差與隱私的社會風險升高：由於數位不平等是自疫情開始以來惡化最嚴重的風險之一，需要政府、企業和社會共同努力，提供數位基礎設施、數位技能培訓、數位金融服務等，以實現數位包容和數位公民權。

最後，科技帶來的機會與風險交織：人工智慧、量子科技等前瞻技術的快速發展，將帶來新的機遇和挑戰，新式犯罪、資訊監控、惡意假訊息等引發道德、法律、人權等方面的爭議和風險。

(二) 臺灣資安發展評析與對策

臺灣作為全球供應鏈的關鍵據點，近年來躍升駭客威脅的重點攻防熱區。Fortinet 數據顯示，2023 年上半年亞太地區共偵測到 4,120 億次惡意威脅，其中臺灣佔比逾五成(55%)，數量高達 2,248 億次，相當於每秒就有近 1.5 萬次攻擊發生，居亞太之冠。此外，與 2022 年同期相比，2023 年上半年 Fortinet 在臺灣偵測到的威脅數量更大增超過八成(81.6%)，駭客最常使用的威脅手法則包含分散式阻斷服務(DDoS)攻擊、濫用雙倍脈衝星(Double Pulsar)漏洞等。

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，爰依據第六期發展方案成果與前述全球資安威脅與國際政策趨勢，進行 SWOT (Strength Weakness Opportunity Threat)深入分析我國內部環境之優劣勢及外部環境面臨之機會與威脅，以下表分析作為規劃本方案之重要參考。

表 1　現階段資安發展 SWOT 分析

優勢 S	劣勢 W
1. 政府已將資安提升至國家安全層級，且成立專責部門「數位發展部」及專業資安法人組織「國家資通安全研究院」積極推動 2. 在《資通安全管理法》推動下，完善法律基礎與相關制度配套 3. 臺灣在高度發展的資通訊產業基礎上，擁有完整的半導體與資通訊產業鏈 4. 在政府計畫和相關教育資源挹注下，積極培育資通安全專業人才，儲備資安研究與專業能量 5. 為提升臺灣資安產業自主能量，積極推動產業導入資安防護	1. 中小企業及國民之資安防護意識仍待提升，造成資料和隱私外洩事件，且缺乏足夠資源應對資安威脅 2. 臺灣民眾面臨詐騙事件的擔憂程度不斷升高，對於新興科技存在諸多疑慮 3. 社交工程郵件攻擊為政府機關面臨之主要資安威脅之一，且逐年上升趨勢 4. 我國資安產業受限國內市場規模，產業規模較小，面臨國際大型資安公司的競爭壓力 5. 政府機關、工控及各產業資安人力質量嚴重不足，成為各組織單位面臨之窘境，有待更完整的培訓制度

機會 O	威脅 T
1. 我國具有全球重要的資安戰略位置 2. 臺灣具有專責之科技偵查單位、專業的網路犯罪偵查人員，臺灣能攜手國際，共同打擊網路犯罪 3. 臺灣面對國家級駭客攻擊，可優先掌握攻擊來源、攻擊手法和惡意程式，透過情資傳遞分享，可讓全球機先掌握資安攻擊情資 4. 政府致力提升國家資通安全科技能力，無論是科技研發和應用，持續擴充國家資安團隊及能量，強化我國整體資安防護 5. 臺灣資安產業近年呈現穩定成長態勢，可發展核心產業所需之資安解決方案，加速資安產業應用情境，提升資安產業自主能量 6. 針對新興科技資安技術應用與開發，如：生成式 AI 與後量子密碼等前瞻資安技術	1. 臺灣政經情勢特殊，長期遭受網路駭侵，關鍵基礎設施及供應鏈資安風險日益嚴峻 2. 由於新興科技的發展，造成資安治理的困難，對於新興科技的風險控管不足 3. 新型態之網路犯罪生態系，造成勒索軟體攻擊風險激增、高科技產業遭駭破壞供應鏈安全

嗣後，採用 TOWS 矩陣針對前述 SWOT 進行策略研析，藉由優勢、劣勢、機會制定進攻策略及轉進策略，再依優勢、劣勢、威脅制定迴避策略及避險策略。進一步依據第六期發展方案 4 項推動策略：「吸納全球高階人才，培植自主創言能量」、「推動公司協同治理，提升關鍵設施韌性」、「善用智慧前瞻科技，主動抵禦潛在威脅」及「建構安全智慧聯網，提升民間防護能量」等的執行成果，可分析在菁英人才培育及國家資安聯防方面應擴增高教資安師資及投入資安科研，以及強化主動防禦能量及偵查技術等措施；而在治理基礎環境及產業防護能量方面應強化公私協同治理運作及供應鏈安全，並輔導企業強化數位轉型之資安防護能量等作為，最後將各項分析結果進行歸納彙整，研析出本方案之發展藍圖。

表 2　TOWS 分析矩陣

SO 進攻策略	WO 轉進策略
1. 建構中央及地方主動安全聯防 (S1+S2+S5+O1+O4) 2. 與國際組織合作，交流情資與技術研發趨勢(S3+S4+O2+O3+O6) 3. 建立從在學到在職的完整人才職涯發展地圖，促進資安人才就業 (S4+O2+ O5)	1. 挖掘新興資安需求，發展資安產業 (W2+W4+O5+O6) 2. 深化跨國情資分享研析，強化網路犯罪偵防量能(W2+O1+O2+O3) 3. 推動各級各類資安人才培訓計畫，包含工控、攻防、企業資安人才 (W1+W3+W5+O4)
ST 迴避策略	**WT 避險策略**
1. 強化關鍵基礎設施及供應鏈安全管理(S1+S2+S4+T1+T3) 2. 針對新興科技，加強前瞻資安技術研發 (S3+S4+T2+T3) 3. 整合資源，健全我國資安產業環境 (S1+S2+S3+T1)	1. 提升民眾資安素養與能力(W1+W2) 2. 公私合作，強化工控環境防護韌性 (W5+T1+T3) 3. 促進人才國際交流，汲取最新趨勢與經驗(W4+W5+T2+T3)

肆、發展藍圖

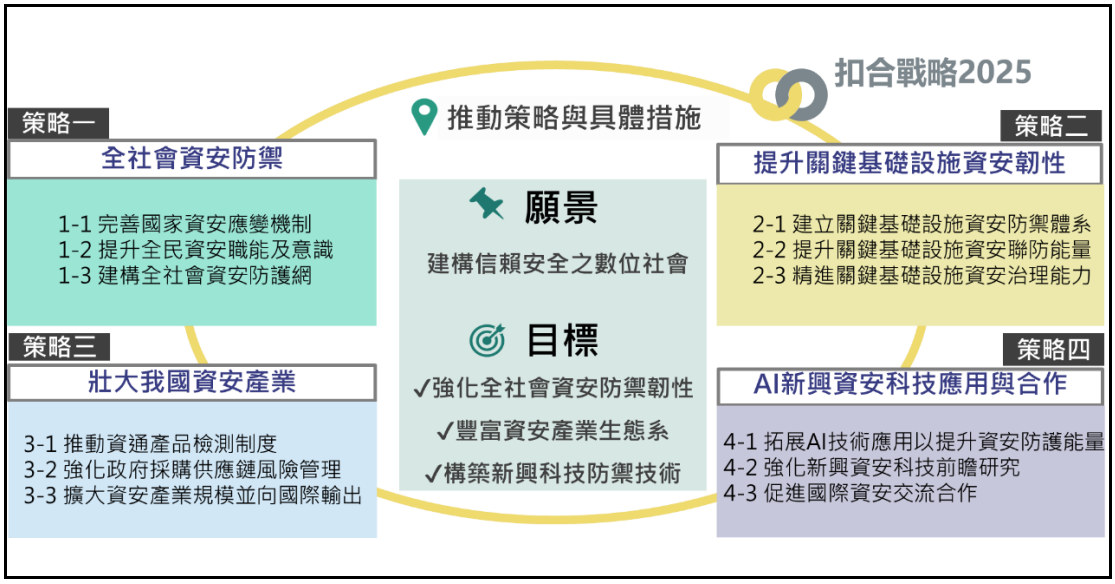

圖 3　第七期國家資通安全發展方案架構

一、願景

我國資安政策推動已歷經前六階段之系統性發展，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。

鑒於資通訊服務應用廣泛，以及我國重大科技創新政策，對於國家安全，甚至是社會經濟活動各種應用層面，資通安全皆扮演關鍵角色，為能因應國際趨勢與新型態資安攻擊與威脅，在既有的防禦基礎及面向上延續我國的資安防護能量與優勢，除持續落實第六期發展方案，行政院國家資通安全會報為逐步提升我國資通安全防護能量，並以賴總統治國理念「國家希望工程」、「五大信賴產業」、「國家資通安全戰略 2025—資安即國安」，打造韌性臺灣，維護安全與和平為應用。爰以「**建構信賴安全之數位社會**」為願景，期打造安全、信賴、開放

的數位新社會。將提出「第七期國家資通安全發展方案(114-117 年)」，作為我國推動資安防護策略與計畫之依循目標。

二、目標

隨著新興科技發展和 IoT 設備普及，以及 5G 時代來臨，資通威脅日益加劇，研擬建構信賴安全的數位社會。我國政府亦因政經情勢特殊，面臨更加嚴峻的挑戰，地緣政治區域爭端影響的實體與資安威脅，應強化關鍵基礎設施韌性，適時納入複合式攻擊情境，改變以往資安事件發生後才精進之反應式防禦，改採「化被動為主動」模式，以因應多元複雜的惡意攻擊。為延續我國資安防護能量與優勢，積極培育充沛資安人才為首要目標，爰本方案中第一項目標設定為「**強化全社會資安防禦韌性**」，涵蓋各領域資安菁英團隊建立，並且建構關鍵基礎設施防衛體系。

第二項目標為「**豐富資安產業生態系**」，持續結合產、官、學、研各界資源與能量，提升企業和民眾的資通安全意識和能力，強化個人隱私保護和數據應用。研議規範軟體安全及提供網路服務之資安責任與供應鏈安全機制，使用高品質且可靠之第三方或開源軟體，以消除數位危害和攻擊風險，強化資安治理。

第三項目標「**構築新興科技防禦技術**」，發展新興資安技術研究能量，解決新型網路犯罪、資訊監控、假訊息等等風險。確保機敏資料保護為核心的 AI 資安、雲端應用安全，開發後量子密碼技術，並發展更具隱私安全、公平公正且可互通操作之保護數位身分隱私技術，維護數位平權。

三、推動策略

為共創安全可信的數位環境，打造以資料為核心的智慧資安研究重鎮，培育我國資安人才生態系，精進國家資安防護作為，利用 AI 等智慧科技強化主動防禦機制並溯源阻斷，透由公私協同資安治理將資安意識與量能普及於民間企業，並健全國家防禦能量，本方案擬具四項推動策略，分別從「**全社會資安防禦**」、「**提升關鍵基礎設施資安韌性**」、「**壯大我國資安產業**」及「**AI 新興資安科技應用與合作**」等四個面向著手，並配合「五大信賴產業之安控產業」規劃持續推動資安產業，期以實現安全、可信賴、開放的數位社會。

1. 全社會資安防禦

持續推動與強化數位政府資安韌性，確保政府機關因應自然災害、人為或其他突發事件中得以快速復原，協助臺灣政府及關鍵基礎設施更具資訊安全與韌性，邁向韌性社會之基礎建設。此外，推動資安區域聯防，建立中央與地方聯合資安防護網，協助區域聯防組織擬定情境腳本、執行沙盤推演及事故通報演練等，透過政府間之區域聯防，提升政府對於資安預警與應變能量。

為因應國家發展之資安人力需求，於第六期發展方案期間，著手增加高教資安師資員額與教學資源，包括增加師資員額、開放學術區域網路中心與政府網路等場域供實習、實戰。本方案透過規劃及開設資安課程教學與實務培訓課程，有效訓練未來資安從業人員具備實務技能，培養高階資安人才，加強國際合作交流機會，並搭配防詐、資安等意識宣傳，提升全民資安素養。

本策略爰規劃三大面向：完善國家資安應變機制、提升全民資安職能及意識、建構全社會資安防護網。

1-1　完善國家資安應變機制

1-1-1 增強政府機關防護能量及完善應變處理機制

完善政府網路安全防禦縱深與廣度，輔導中央機關導入零信任架構，蒐整國內外零信任架構導入推動文件及經驗，研訂政府機關零信任導入相關指引，運用零信任工具建立身分鑑別機制，作為政府機關未來導入設備鑑別與信任推斷之基礎，更能因應數位轉型下之資安防護需求。

1-1-2 推動統籌並協處支援重大資安事件

為培訓公務人員實戰經驗，推動統籌支援重大資安事件入法機制，當資安事件發生時，可視機關意願及事件嚴重情形，調動相關機關資安人員至事件發生機關支援，以求更有效率解決資安事件，並提升資安人員實戰能力，進一步強化公務機關間調度支援聯防機制。

1-1-3 辦理攻防演練，提升防禦部署之有效性

鼓勵已建置 SOC 之重要政府機關引入攻擊方思維，定期藉由網路攻擊手法，如：DDoS 攻防演練、紅藍隊演練及入侵與攻擊模擬等，檢驗資安監控及防禦部署之有效性。

1-1-4 強化國家資安會報統籌督導機制及資安預算正規化

推動國家資通安全會報入法，強化總統府、五院及部會協調機制(視審議進度調修)並強化管考機制。另透由辦理資安會議與資安長探討最新威脅趨勢及資安事件處理。另盤點各公務機關資安經費需求，以利預算規劃，俾利整體國家資安業務推展。

1-1-5 資安法子法或相關指引調修，強化資料保護機制

因應新興科技發展，國際資安威脅趨勢不斷變化，我國資通安全管理法應與時俱進，持續調修資安法子法、相關指引並落實施行。

1-2　提升全民資安職能及意識

1-2-1 推動我國資安人才框架，完善就學到在職之資安職涯發展路徑

檢視我國資安人才框架，推動資安人才能力鑑測機制，並提供資安領域學術參與管道及資安課程系統化規劃建議，配合設計合適從校園到職場各階段之資安課程，並整合產學提供合適之職涯發展建議，辦理學術資安活動與新型態資安課程，推動資安人才培育工作，增強就業競爭力。

1-2-2 培育高階型資安人才，強化實戰人才知能

關鍵基礎設施資安人才養成，培訓國內工控場域實戰資安人才；並精進攻防平台之環境，建置以藍軍為主的紅藍攻防平台供競賽及訓練使用，培訓國內高階實戰人才及參加培訓。

1-2-3 精進政府資安人才職能發展地圖，推動資安專業證照

考量我國資安人才需求，完成資安人才職能基準，並將資安人才分級分類培訓，例如資安長、資安人員、CI 各領域之異質特殊性，進行各資安課程與評量開發，以精進國內資安人才的職能地圖與人才發展路徑；針對強化政府資安人才，提供發展藍圖、教材、職能轉換、學分專班等培訓，辦理「資通安全專業證照」審查、高考資安類科考試錄取人員實務訓練，完善我國政府資安人才發展路徑。

1-2-4 推動社會資安意識提升，全民共同守護資通安全

推動全民資安意識、媒體素養和教育相關課程講座；設置主題式之資安競賽或遊戲等，以不同活動強化全民資安意識，推動資安技能向下扎根，提升全民資安素質與水準。

1-2-5 推動公務機關留才機制，提升人員留任誘因

訂定公務機關資通安全業務績效評核及獎勵規範，辦理績效評核及獎勵作業；訂定資安專業人才留任獎勵金支給表，提升資安人員待遇增加留任意願。

1-3　建構全社會資安防護網

1-3-1 強化數據與隱私保護，降低個資外洩風險

強化各公務機關或中央目的事業主關機關辦理所屬非公務機關個資防護管理措施，尤其對於掌握大量個人資料之機關，應有進一步之保護措施，以降低個資外洩風險。

1-3-2 強化資料與情資分析，打擊網路犯罪

從源頭防堵詐騙訊息，確保政府資訊不被仿冒，降低民眾遭詐騙之風險，透過科技解析社交工程、駭侵事件等情資，協助提升民眾的生活保障。

1-3-3 運用數位科技偵查技術，精進資安鑑識能量

精進網路情資、虛擬通貨金流及追蹤等新型態犯罪之鑑識技術，透過智慧化分析駭侵行為攻擊態樣及防禦機制，加強犯罪偵查技能之實務訓練；並建置自主性智慧分析及追蹤平台，輔助案件偵辦，以強化整體新興犯罪之科技偵查實戰能量。

2. 提升關鍵基礎設施資安韌性

為精進關鍵基礎設施之資安防護能量，提升我國數位韌性(Resilience)，本策略將持續推動及落實各領域之資安防護基準，並輔以攻防演練及定期稽核檢視執行成效，從能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區八大關鍵基礎設施領域精進聯防。

本策略爰規劃三大面向：強化關鍵基礎設施資安防禦體系、提升關鍵基礎設施資安聯防能量、精進關鍵基礎設施資安治理能力。

2-1 建立關鍵基礎設施資安防禦體系

2-1-1 建置關鍵基礎設施之資安防衛體系

建立保護關鍵基礎設施資通安全之專業團隊，係政府維持國家與社會之安全與穩定，不可或缺之關鍵決策。團隊成員具備資通安全知識，熟悉工控系統特點，掌握工控系統最新之資通安全威脅，了解駭

客之攻擊方法，以及具備使用專業軟硬體工具，進行工控系統之檢測，協助關鍵基礎設施業者確保工控系統之穩定運作與保護資料。

2-1-2 建立國家層級威脅模型，蒐集各領域威脅特徵

建立自評估、威脅狩獵、事件處理、自動化開發及作業管理各階段一致性管理流程，降低人為錯誤風險，維持作業品質。

2-1-3 辦理檢測核心技術訓練及移轉，提升防護能量

融合國際資安重點國家專業知識與我國目前之資通安全能量，結合八大關鍵基礎設施提供者之需求，前二年採循序漸進方式執行，第三年起以公私協力模式，發展進階持續型服務，實施工作自動化與 AI 化，使檢測與威脅狩獵提升為全年持續型防護，強化 CI 防護網之韌性。

2-2 提升關鍵基礎設施資安聯防能量

2-2-1 強化關鍵基礎設施資安威脅監控

在基礎設施上部署防禦系統，透過誘捕與網路部署進行蒐集，依據蒐集到的樣本分析惡意攻擊行為，以掌握、應變關鍵基礎設施領域所面臨之資安威脅，透過整合與加強八大領域情資分享與聯防，強化各領域應變、防護及網路訊息蒐集處置，共同提升資安防護能量。

2-2-2 加強關鍵基礎設施情資分享運作，提升整體數位防護

持續精進關鍵基礎設施間之資安聯防機制(情資分享、通報應變及資安監控)，有效整合並且擴大領域資安情資資料庫，透過自動化分享機制，強化各領域之資通安全防護能量，提升跨域資安聯防成效。

2-2-3 關鍵基礎設施資安實地演練與稽核，提升資安韌性

辦理資通安全管理法納管機關之資安稽核，邀集適當攻擊手及 CI 主管機關辦理攻防演練，發掘機關系統潛在弱點，相互交流與分享成果，並作為示範案例及設計資安事件情境模擬教學訓練，用於結合工控場域培育國內高階實戰人才。

2-2-4 辦理跨國網路攻防演練(CODE)及相關國際演訓

透過舉辦關鍵基礎設施跨領域或跨國網路攻防演練，與國際單位組成攻防聯隊共同進行實戰演練，提升資安專業技術與應變能力。

2-3 精進關鍵基礎設施資安治理能力

2-3-1 落實各領域資安防護基準，強化關鍵基礎設施資安防護

各 CI 主管機關落實防護基準執行控制措施、辦理資安治理成熟度或訂定相關規範，強化資安防護基準措施，確保我國關鍵基礎設施資安韌性；並產製相關資安防護評估報告，提供我國各中央目的事業主管機關參考修訂工控資安防護基準。

2-3-2 提升工控領域資安治理成熟度

輔導檢視 A、B 級之公務機關或 CI 提供者擇選資安治理成熟度執行弱項，以促進關鍵基礎設施提供者之完善資安防護整備度。

3. 壯大我國資安產業

近年來網路攻擊者除了針對政府機關進行駭侵外，目標轉移至民間企業及相關產業供應鏈，因此，除持續強化我國政府機關資安防護能量外，積極協助產業重視物聯網產品資安外，亦將數位服務資安、供應鏈資安納為重點推動項目。

5G 網路時代，各類資通訊設備資通安全益顯重要，除協助我國電信業者聚焦 5G 資安風險議題外，亦須同時關注新興科技資安議題，制訂相關合規驗證及實證場域，加速物聯網資安解決方案落地與商用化，並參考國際標準，據以推動具備國際競爭力之資安解決方案，期以未來輸出國際市場。

本策略爰規劃三大面向：推動資通產品檢測制度、擴大資安產業規模並向國際輸出、強化政府採購供應鏈風險管理。

3-1 推動資通產品檢測制度

3-1-1 推展產品資安檢測及驗證，確保產品安全

藉由研擬國內物聯網資安相關標準及檢測框架，透過公私部門合作，發展資安檢測技術或產業標準等，提升臺灣資通訊產品之資安防護能量，建構安全可信賴之數位基礎環境。

3-1-2 推動數位服務之資安檢測，提升資安防護能量

數位服務、網際網路是民眾容易遭受資安事件的重要入口，透過協助檢測，將有效提升我國數位服務企業安全，同時守護民眾資安，促成可信賴的網路服務環境。

3-2 強化政府採購供應鏈風險管理

3-2-1 促進政府機關導入優質民間資安廠商，降低風險發生與衝擊

辦理資安服務廠商評鑑；遴選重要廠商辦理資安訪視，或以其他適當方式協助提升資安防護能量；精進採購作業資安要求相關文件之檢視或增修訂。

3-2-2 協助民間廠商漏洞審查及諮詢，加強風險監控與審查

受理及審核國內企業產品資安漏洞，並協助民間資訊安全相關諮詢或應變處置，提升企業資安能量。

3-3 擴大資安產業規模並向國際輸出

3-3-1 提升資安產業創新能量與解決方案，提升零信任環境

輔導物聯網場域業者偕同供應鏈廠商建立零信任資安強化示範應用案例，引導資安產業發展零信任物聯網資安技術，推動符合不同領域的零信任資安防護產品。

3-3-2 整合相關資源，打造具國際信賴之資安產業

透過資安產業整合平臺，整合技術、資金、市場渠道等相關資源，協助資安新創獲得資金和創業資源，促成資安新創投入技術開發，提升臺灣資安新創中長期之競爭力，並藉由多元發展資安新技術、新應

用及創新商業模式，幫助資安產業進軍國際，健全整體資安產業環境發展。

3-3-3 升級資安科技園區，帶動南部產業鏈發展

將臺南沙崙資安服務基地打造成為以資安為主軸之產業聚落，吸引國際大廠進駐，將臺灣建設成為亞太地區重要的資安發展基地。

4. AI 新興資安科技應用與合作

隨著科技進展，無人機、智慧醫療、雲端服務等應用出現不同資安挑戰，需要與國際之間交流新興趨勢，共同應對全球性的資安挑戰，並分享最佳實踐和經驗。為能因應國際趨勢與新型態資安攻擊與威脅，亟須拓展新興資安科技前瞻研究，以提升資安防護的效能。藉由研發資安尖端技術，追趕國際資安技術前緣，所研發之技術未來可藉由技轉、新創等方式回到業界，活絡本國資安產業，提升國際競爭力。

本策略爰規劃三大面向：拓展 AI 技術應用以提升資安防護能量、強化新興資安科技前瞻研究、促進國際資安交流合作。

4-1 拓展 AI 技術應用以提升資安防護能量

4-1-1 推動 AI 網路主動式防禦關鍵技術研究，提升處理威脅情資之效能

專注 AI 推論能力應用威脅偵測演算法與自適應防禦機制研發，運用深度學習技術開發異常行為識別、攻擊模式預測與自動化應變系統，建立高效能 AI 資安模型，提升系統對未知威脅的預警與防禦能力，並透過 AI 推論能力結合自動化收集與分析多來源威脅情報，為資安團隊提供即時精確的威脅評估與預警，提升組織對新興威脅的感知與應變能力

4-1-2 應用 AI 強化資安治理，掌握國家威脅態勢並強化治理透明度

蒐整我國資安治理與威脅之資料來源、樣態，並進行分析，以機器學習發展專屬 AI 模型，規劃及建置「國家資安治理情資平臺」系統，發展結合資安治理與威脅態勢之高可視性戰情牆。

4-1-3 運用 AI 技術於資安稽核資料分析，擴展資安防護層面

為精進資安稽核作業，深入剖析機關整體資安防護情形，並透過系統化作業，簡化稽核作業之流程，爰規劃建置稽核資料分析平臺，綜整資安法納管機關稽核資料與資安會報資安稽核結果資料，期以系統及自動化方式進行關聯分析，提升對於各機關整體資安防護檢視之深廣度，以發掘潛在之資安風險，強化我國資安整體防護韌性。

4-1-4 推動我國 AI 評測制度與可信任 AI 環境發展

檢測 AI 模型的資安風險與隱私洩露風險，包括提示注入攻擊模擬與隱私保護能力評估，協助公部門及鼓勵企業進行第三方評測，評測 AI 模型之表現，以及提供回饋建議，提升企業產品競爭力，健全模型符合資訊安全與隱私保護。

4-2 強化新興資安科技前瞻研究

4-2-1 輔導無人機安全及醫療應用等新型資安技術能量

研發我國自主無人載具關鍵技術，補足國內無人機技術缺口，培養我國無人機人才並落實產業應用；另結合領域標準之研析，強化醫療機構新科技，訂定應用新科技資安及個資保護參考規範，以供相關單位運用。

4-2-2 精進雲端服務資安，保護資料安全與隱私

建置臺灣可信賴資料雲端分析平臺，以具高資安與隱私防護、特別權限管理、隔離封閉之儲存區，以及可提供資料不落地分析等特色服務，推動於科研、生醫研究、國土治理與國防科技應用，並發展雲端服務的政府組態基準，持續檢視並視需要調修雲端服務應用資安參考指引。

4-2-3 研析後量子密碼資安架構及國際趨勢

研析各國後量子密碼相關推行政策、發展情形，提出我國後量子密碼發展建議，並推動業者發展後量子密碼相關解決方案。

4-3 促進國際資安交流合作

4-3-1 建立技術交流及情資分享等合作管道，促進國際聯防

新興科技快速變遷所帶來的威脅與挑戰，需與國內外單位進行技術和情報交流，促進並強化全球網路犯罪防禦之合作，藉由持續參與國際資安組織之工作小組與定期會議，並深化與美、歐及亞太區等國資安研究機構之交流，建立長期合作與情資分享機制，強化跨國協防體系，提升我國整體資安防禦能力。

4-3-2 舉辦及參與國際研討會或競賽，鏈結國際夥伴信任關係

透過辦理及參與跨國研討會、討論議題及蒐集專家意見，協助我國與各國經驗交流，瞭解新型科技應用，深化臺灣資安業者與國際資安組織社群鏈結，促進臺灣資安視野國際化，強化臺灣數位外交；並於賽事部分，辦理選手增能活動，增加我國資安選手實力，爭取國際曝光機會。

四、機關(單位)分工

表 3　機關(單位)分工表

措施	主(協)辦機關
策略一：全社會資安防禦	
1-1 完善國家資安應變機制	
1-1-1 增強政府機關防護能量及完善應變處理機制	數發部、國科會、法務部、內政部
1-1-2 推動統籌並協處支援重大資安事件	數發部
1-1-3 辦理攻防演練，提升防禦部署之有效性	數發部
1-1-4 強化國家資安會報統籌督導機制及資安預算正規化	數發部、主計總處
1-1-5 資安法子法或相關指引調修，強化資料保護機制	數發部
1-2 提升全民資安職能及意識	
1-2-1 推動我國資安人才框架，完善就學到在職之資安職涯發展路徑	數發部、教育部、國科會
1-2-2 培育高階型資安人才，強化實戰人才知能	數發部、交通部、經濟部、衛福部、金管會
1-2-3 精進政府資安人才職能發展地圖，推動資安專業證照	數發部、內政部
1-2-4 推動社會資安意識提升，全民共同守護資通安全	數發部、內政部、原民會
1-2-5 推動公務機關留才機制，提升人員留任誘因	數發部
1-3 建構全社會資安防護網	
1-3-1 強化數據與隱私保護，降低個資外洩風險	各機關
1-3-2 強化資料與情資分析，打擊網路犯罪	內政部、法務部
1-3-3 運用數位科技偵查技術，精進資安鑑識能量	法務部
策略二：提升關鍵基礎設施資安韌性	
2-1 建立關鍵基礎設施資安防禦體系	
2-1-1 建置關鍵基礎設施之資安防衛體系	數發部
2-1-2 建立國家層級威脅模型，蒐集各領域威脅特徵	數發部

措施	主(協)辦機關
2-1-3 辦理檢測核心技術訓練及移轉，提升防護能量	數發部
2-2 提升關鍵基礎設施資安聯防能量	
2-2-1 強化關鍵基礎設施資安威脅監控	各 CI 主管機關
2-2-2 加強關鍵基礎設施情資分享運作，提升整體數位防護	各 CI 主管機關
2-2-3 關鍵基礎設施資安實地演練與稽核，提升資安韌性	各 CI 主管機關
2-2-4 辦理跨國網路攻防演練(CODE)及相關國際演訓	數發部
2-3 精進關鍵基礎設施資安治理能力	
2-3-1 落實各領域資安防護基準，強化關鍵基礎設施資安防護	各 CI 主管機關
2-3-2 提升工控領域資安治理成熟度	數發部
策略三：壯大我國資安產業	
3-1 推動資通產品檢測制度	
3-1-1 推展產品資安檢測及驗證，確保產品安全	數發部
3-1-2 推動數位服務之資安檢測，提升資安防護能量	數發部
3-2 強化政府採購供應鏈風險管理	
3-2-1 促進政府機關導入優質民間資安廠商，降低風險發生與衝擊	數發部、工程會
3-2-2 協助民間廠商漏洞審查及諮詢，加強風險監控與審查	數發部
3-3 擴大資安產業規模並向國際輸出	
3-3-1 提升資安產業創新能量與解決方案，提升零信任環境	數發部
3-3-2 整合相關資源，打造具國際信賴之資安產業	數發部
3-3-3 升級資安科技園區，帶動南部產業鏈發展	數發部、國科會
策略四：AI 新興資安科技應用與合作	
4-1 拓展 AI 技術應用以提升資安防護能量	
4-1-1 推動 AI 網路主動式防禦關鍵技術研究，提升處理威脅情資之效能	數發部
4-1-2 應用 AI 強化資安治理，掌握國家威脅態勢並強化治理透明度	數發部

措施	主(協)辦機關
4-1-3 運用 AI 技術於資安稽核資料分析，擴展資安防護層面	數發部
4-1-4 推動我國 AI 評測制度與可信任 AI 環境發展	數發部
4-2 強化新興資安科技前瞻研究	
4-2-1 輔導無人機安全及醫療應用等新型資安技術能量	國科會、衛福部
4-2-2 精進雲端服務資安，保護資料安全與隱私	國科會、數發部
4-2-3 研析後量子密碼資安架構及國際趨勢	數發部
4-3 促進國際資安交流合作	
4-3-1 建立技術交流及情資分享等合作管道，促進國際聯防	數發部
4-3-2 舉辦及參與國際研討會或競賽，鏈結國際夥伴信任關係	數發部、內政部

註：CI 主管機關係指經濟部、數位發展部、金管會、衛福部、交通部、農業部及國家科學及技術委員會。

伍、預期效益

一、 我國於第六期發展方案，已著力於培育資安人才及建立主動防禦等策略，在人才培育上，數量上已採取國家考試取才、職能轉換訓練等方式持續擴展資安人員，質量上也透過資安增能培訓、資安職能評量等機制確保其知能提升；而在主動防禦，已於部分機關完成零信任驗證部署，並於主要網路閘口部署 APT 流量阻斷、黑名單自動化、內網威脅誘捕及惡意郵件偵測等機制，加強政府大內網之縱深防禦能量，主動防禦潛在威脅。本方案透過前期推行的成果上，提出「全社會資安防禦」之策略，確保我國於面對資安事件時能迅速應變並恢復正常運作，並從法制面及政策面同步推動。在法制面上，積極推動《資通安全管理法》及相關子法之修正作業，明確規範機關資安業務權責、擴大資安稽核與管理監督，以完備的法治基礎提升國家資安應變機制；在政策面上，制訂政府機關多元儲備資安人才方式，厚植資安訓練能量，藉以提升全民資安職能及意識，建構全社會資安防禦機制。

二、 為保護關鍵基礎設施系統，避免因網路攻擊而導致重大社會事件與經濟劇變，已於第六期發展方案訂定交通、能源與水資源等領域工業控制系統資安防護基準，醫療儀器相關系統資通安全防護基準，及關鍵電信基礎設施資通設備資通安全檢測技術規範；現本方案立基於前述成果上，藉由「提升關鍵基礎設施資安韌性」於民生關鍵基礎設施，強化關鍵基礎設施資安縱深防禦，拓展資安檢測涵蓋至少 6 個領域，協助關鍵基礎設施完善資安基礎環境與資安治理成熟度，並發展進階持續型服務與

自動化工作流程，強化關鍵基礎設施防禦韌性，使關鍵基礎設施資安防護安全可信，全面提升資安防護治理之效。

三、 從數位服務至數位產品，從軟體至硬體供應鏈安全意識逐漸抬頭，提升產業資安聯防能力，多元方式培育跨域產業資安專業人才並輔導資安業者打造資安整合服務平臺及工控資安聯防生態，數位服務資安、供應鏈資安已為當前重點項目，因此本方案以「壯大我國資安產業」為策略，推動資通產品及服務之檢測驗證制度、驗證標準接軌國際，強化政府採購供應鏈風險管理，推展新興科技應用資安防護技術與指引，使整體產品資安環境可信，進一步透過良善的資安產業環境建置，有效提升我國數位服務企業安全，同時守護民眾資安，促成可信賴的網路服務環境，並使我國資安品牌逐漸向國際輸出成長，促進我國資安產業產值達新臺幣(以下同) 1,200 億，成為全球可信賴安控與資安大國。

四、 因應新興科技發展，數位應用資安生態系持續擴張，及近年來崛起的生成式 AI 所帶來的威脅與挑戰，對於新興科技資安防護技術發展的需求也同步升高，需要投入大量資源進行新型資安技術研發，包括如何正確使用 AI、AI 應用政策與治理及研發，以及深化與國際經驗交流，包含鏈結國際資安組織社群與全球網路犯罪防禦之合作，掌握新型科技應用及科技偵查技術，研擬科技犯罪對策因應未來犯罪發展趨勢，強化臺灣數位外交；是以本方案「AI 新興資安科技應用與合作」為策略，充實資安前瞻研究能量，研發新穎資安技術，透由 AI 自動化資安防護分析各式情資，偵測未知威脅及預測可能攻擊，建立政府骨幹網

路 AI 主動防禦機制，進一步守護我國資通安全。

表 4　重要績效指標

	114 年	115 年	116 年	117 年
培訓政府機關專職人力	培訓政府機關專職人力達 2,000 人次	培訓政府機關專職人力累計達 4,000 人次	培訓政府機關專職人力累計達 6,000 人次	培訓政府機關專職人力累計達 8,000 人次
強化關鍵基礎設施資通安全	試行檢測建置標準作業流程	各領域規劃執行專案檢測至少 10 處	各領域規劃執行專案檢測至少 25 處	各領域規劃執行專案檢測至少 50 處
資安產業規模化，促進資安產業產值提升，推動資安產業發展	促進資安產業產值逾 895 億	促進資安產業產值逾 1,000 億	促進資安產業產值逾 1,097 億	促進資安產業產值逾 1,200 億
建立政府骨幹網路 AI 主動防禦機制	1. 開發威脅態勢預警技術 2. 開發攻擊酬載來源鑑技術	1. 開發未知漏洞風險識別技術 2. 開發蜜罐攻擊誘捕分析技術	1. 惡意郵件誘捕分析技術 2. 資安自評報告分析產製技術	1. 資安風險與解方推論技術 2. 跨維度數據語意關聯技術

陸、推動組織、資源需求及計畫管理

一、推動組織

為強化我國整體資通安全防護能量，建構全方位、跨領域之防護體系，數位發展部資通安全署依據「行政院國家資通安全會報設置要點」，擔任我國資通安全政策之統籌規劃與推動單位，整合跨部會資源與協作機制，推動本行動方案之各項策略與具體工作項目，期能建立韌性、可信任之數位環境。

本方案依據當前國內外資安情勢與科技發展趨勢，以建構信賴安全之數位社會為願景，規劃四大策略主軸，涵蓋全社會資安防禦、提升關鍵基礎設施資安韌性、壯大我國資安產業與 AI 新興資安科技應用與合作，希冀達到強化全社會資安防禦韌性、豐富資安產業生態系、構築新興科技防禦技術之目標，並細分為 12 項推動目標及 38 項具體措施。

各策略措施內容藉由行政院國家資通安全會報明確責成各分組分工並務實推動，由「資通安全防護組」辦理全社會資安防禦相關工作事項，「關鍵資訊基礎設施安全管理組」辦理提升關鍵基礎設施資安韌性作業，及「產業發展組」協助壯大我國資安產業與豐富資安產業生態系，並協調各分組量能強化新興資安科技前瞻研究，例如：AI 技術應用、後量子密碼資安架構及雲端服務資安等，並攜手國際促進資安交流合作以提升資安防護能量。

二、執行規劃

數位發展部自 112 年起辦理國際情勢研析、各國資安政策蒐整、前瞻科技議題掌握、國內資安政策推動情形調研及相應部會意見徵集，113 年辦理專家訪談、部會座談等相關研商會議，同步針對整體未來方案政策議題、相應計畫辦理之工作研商。

本方案工作項目之主(協)辦機關(單位)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(單位)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(協)辦機關(單位)應依據本方案訂定計畫以籌措經費預算，並以各措施工作項目內容務實推動。年度計畫之執行應每年進行檢討，並配合預算審議與績效綜合評估結果等做必要之修正。

四、相關行動方案之管考

為確保本行動方案之推動成效，落實工作項目之執行與績效指標之達成，特訂定明確之管考機制，並由行政院國家資通安全會報負責統籌督導。本管考機制係結合現行既有之督導程序，透過計畫推動期程中各階段之資料調查、進度追蹤、績效評估與改善建議等方式，確保各主辦及協辦機關依循本方案進行分年規劃與執行，並達成所設定之目標與效益。

(一) 管考目的

本方案之執行涉及多項工作項目及多個機關協作，為促進整體推動效率與目標落實，管考機制將達成下列目的：

1. **掌握推動進度**：透過定期之進程調查與回報，隨時掌握各項工作執行現況與進度，作為整體推動進程參考。
2. **評估績效成果**：依據各機關所設定之績效指標，進行具體成果評估，判斷目標達成程度。
3. **辨識問題與協助解決**：發掘執行過程中所遇瓶頸或資源缺口，協助機關提出調整建議或資源調配方案。

4. 提供政策滾動修正依據：透過年度成效分析，做為後續政策調整與資源投入之依據，促進方案持續優化。

(二) 管考架構

本管考機制主要分為三層架構：

1. 中央統籌層：由行政院國家資通安全會報負責統籌全案執行狀況之督導、追蹤與協調，並彙整年度工作成果與績效報告，供主管機關參酌。

2. 主辦機關層：各主辦機關負責本方案中其所轄之工作項目規劃、執行與成效監控，並定期回報推動情形。

3. 協辦機關層：依據工作需求配合主辦機關執行相關協力事項，並參與管考調查及資料提供作業。

(三) 管考時程與執行程序

本管考機制之推動，將採年度循環機制進行，依據以下年度時程進行各項資料蒐集與成效檢核：

1. 114 年度起始作業

為確保 114 年度方案之執行準備作業完整，預計於 114 年 6 月，由數位發展部資通安全署正式函文各主(協)辦機關，調查 114、115 年之**分年推動進程**（即分別年度內各項工作預定之完成里程碑），以掌握年度預計推動情形。

主(協)辦機關(單位)應依據兩年內之分年推動進程，預先準備人力與經費等資源。

2. 115 及後續年度執行與追蹤

依循前一年調查結果，115 年及後續年度將依下列時程進行相關追蹤與成效分析：

(1) 115 年 6 月辦理 116 年度分年進程之調查。調查內容將包含：各機關對 116 年度預計啟動或延續執行之工作項目、

各項目預期達成目標與具體績效指標、所需配合事項或潛在資源需求。

(2) 115 年 12 月底至 116 年 1 月初請各主(協)辦機關填復 115 年度實際執行情形，內容包括：原定工作項目完成度、各項績效指標達成狀況、遇到之困難與改進建議、異常狀況處理情形。

該年度成效資料彙整後，數位發展部資通安全署將進行分析與彙編，並形成年度推動成果報告，同時做為政策滾動調整與次年度管考基礎；另 116 至 118 年度執行與追蹤方式比照上述事項辦理。

(四) 績效指標設計原則

各主(協)辦機關於回報分年進程與執行情形時，須依據本方案所設定之總體目標，擬定具體可衡量之績效指標。績效指標原則如下：

1. **具體明確**：指標須能對應特定工作項目，具可衡量性與量化標準。
2. **可追蹤性**：須能於年度內透過紀錄或調查方式獲得具體數據。
3. **可行性**：指標所需數據應為執行單位可合理取得或掌握者。
4. **結果導向**：優先考量結果層級指標，如「完成件數」、「完成場次」、「完成率」、「使用率」等。

(五) 持續改善與協調機制

考量本方案推動期程橫跨多年，過程中難免因外部環境變化或機關本身業務調整而需進行調整，因此本管考機制亦強調以下要素：

1. **滾動式修正**：每年度調查及成效檢核，皆將提供彈性調整空間，容許機關依據實際推動狀況修正項目時程或執行方式。

2. **跨機關協調**：針對多機關共同執行項目，行政院國家資通安全會報將扮演溝通與協調角色，必要時召開協調會議，調整工作與配合事項。

3. **案例分享與經驗交流**：鼓勵各機關彙整執行過程中之成功案例與挑戰經驗，視情形安排至「行政院國家資通安全會報」委員會議進行議題交流，以提升整體方案推動品質。

五、方案核定與修訂

本方案經核定後實施，未來如有修正，亦應循年度循環機制(PDCA)辦理，以確保政策推動之合法性與一致性：

1. **規劃(PLAN)**：由行政院國家資通安全會報統籌方案進程，各機關依本方案訂定計畫以編列預算。

2. **執行(DO)**：數位發展部資通安全署確認方案執行工項之分年進程，各機關依執行工項推動並適時回饋與溝通。

3. **管考(CHECK)**：各機關定期填報年度執行成效，數位發展部資通安全署檢視執行成效並評估績效成果。

4. **回饋(ACT)**：數位發展部資通安全署依實際執行情形進行方案滾動調整，各機關適時說明績效結果或經驗分享。

整體方案施行期程為期四年，期滿前將進行全面性整體檢討，依施行成果、國內外資安情勢變化及技術發展趨勢，研擬未來四年發展方向及修正內容，作為新一期方案之依據。為維持方案推動之靈活性與即時性，本方案亦設有滾動式檢討機制，得依實際執行情形與情勢需要，每年進行階段性修正，包含策略方向、推動項目、經費配置等，確保方案內容持續貼近實務需求、政策目標與國家資通安全整體發展方向。此一制度設計，有助於強化政策調整彈性，提升整體資安治理韌性與前瞻性。

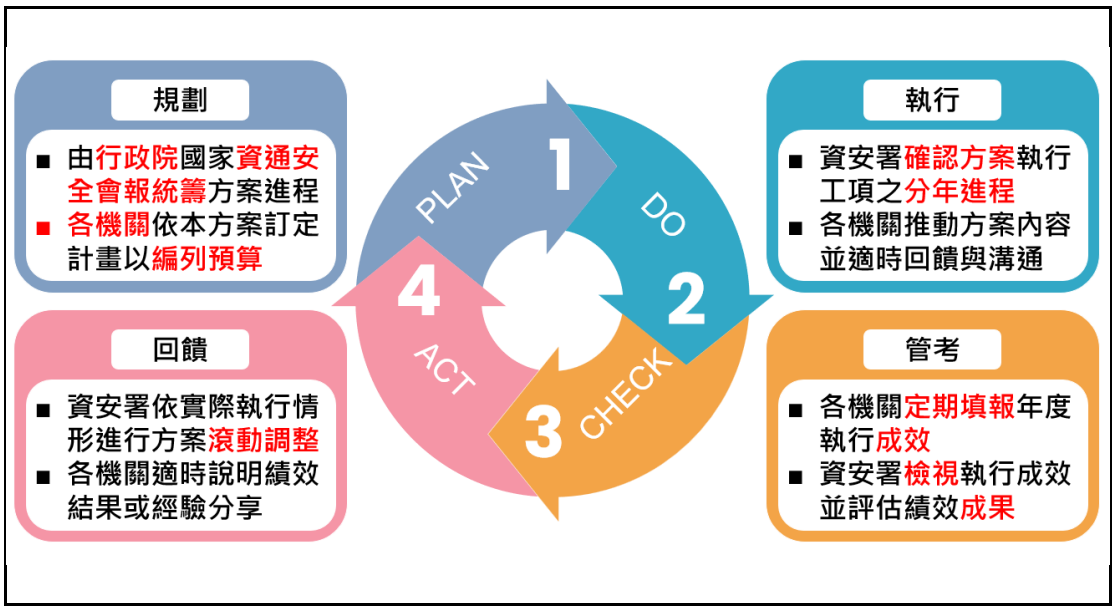

圖 4　第七期國家資通安全發展方案推動循環機制（PDCA）

柒、附件

附件 1、各措施之工作項目

措施	主(協)辦機關	工作項目
策略一：全社會資安防禦		
1-1 完善國家資安應變機制		
1-1-1 增強政府機關防護能量及完善應變處理機制	數發部、國科會、法務部、內政部	數發部： (1) 持續推動 A 級公務機關及 A 級 CI 提供者導入黑名單自動化部署服務。 (2) 透過駭侵樣本萃取威脅情資，製作並部署偵測規則；導入 AI 技術之惡意 URL 偵測。 (3) 推動全國共通資通安全業務推動相關系統建置與持續發展。 (4) 蒐整國內外零信任架構導入推動文件及經驗，研訂政府機關零信任導入相關指引。 (5) 精進 GSN 內網，及建置 EASM。 國科會：持續優化及推動本會智慧辦公環境，導入新趨勢安全架構之資通訊系統與創新資訊服務，並落實各項資通訊安全管理法法遵規範與提升資安防護量能。 法務部：完成重要系統導入零信任網路之身分鑑別機制。 內政部：打造國境安全智慧應用數位韌性，導入智慧化資安管理系統。
1-1-2 推動統籌並協處支援重大資安事件	數發部	推動統籌支援重大資安事件入法機制，強化公務機關間調度支援聯防機制(視審議進度調修)。
1-1-3 辦理攻防演練，提升防禦部署之有效性	數發部	執行網路攻防演練作業，蒐整機關為民服務資通系統弱點樣態，提供各界參考。

措施	主(協)辦機關	工作項目
1-1-4 強化國家資安會報統籌督導機制及資安預算正規化	數發部、主計總處	(1) 推動資安會報入法機制，強化總統府、四院及部會協調機制(視審議進度調修)。 (2) 辦理資安會議與資安長探討最新威脅趨勢及資安事件處理。 (3) 盤點各公務機關資安經費需求，以利預算規劃。
1-1-5 資安法子法或相關指引調修，強化資料保護機制	數發部	辦理資安法及其子法修訂及施行(視審議進度調修) 。
1-2 提升全民資安職能及意識		
1-2-1 推動我國資安人才框架，完善就學到在職之資安職涯發展路徑	數發部、教育部、國科會	數發部：檢視我國資安人才框架，推動資安人才能力鑑測機制。 教育部：提出資安課程系統化規劃建議，辦理新型態資安課程。 國科會：提供資安領域學術參與管道，推動資安人才培育工作，辦理學術資安活動。
1-2-2 培育高階型資安人才，強化實戰人才知能	數發部、交通部、經濟部、衛福部、金管會	數發部： (1) 結合工控場域建置，開發相關實戰訓練教材。 (2) 培養高階資安實戰人才，建立我國資安實戰人力。 交通部：交通領域工業控制系統資安職能課程。 經濟部：辦理工控領域教育訓練 2 場。 衛福部：修訂醫療領域資安人才培育藍圖。 金管會：依據金融資安人才職能地圖，開設金融資安人才養成專。

措施	主(協)辦機關	工作項目
1-2-3 精進政府資安人才職能發展地圖，推動資安專業證照	數發部、內政部	數發部： (1) 檢視政府資安職能訓練發展藍圖合宜性，並編修政府機關資安職能訓練科目教材內容。 (2) 每年辦理資通安全專業證照審查作業。 (3) 辦理高考資通安全類科考試錄取人員集中實務訓練。 (4) 培訓資安長與資訊（安）主管，精進資安治理知能。 (5) 辦理公務人員職能轉換訓練，包含學分專班培訓、資安職能訓練培訓。 (6) 培訓資通安全管理法納管機關資安人員，強化實務專業能力。 內政部：建構以民需為本的數位服務，採取以「雲端申辦授權、服務隨手可得」形式，系統管理人員資訊安全認知、教育訓練。
1-2-4 推動社會資安意識提升，全民共同守護資通安全	數發部、內政部、原民會	數發部： (1) 辦理資安技能金盾獎、資安搶旗攻防賽(CTF)相關活動，鼓勵學子投入資安領域工作，引發民眾對資安興趣。 (2) 每年辦理資通安全防護巡迴研討會，宣導資安相關議題。 (3) 舉辦推廣活動，透過多元管道與推動手法，擴大資安意識教育與社會影響範圍與深度。 (4) 提供我國企業與民眾資安新興攻擊手法或資安新知，每年研析資安相關新聞或文章。 內政部：提供新住民及其子女免費資訊課程，推廣資安意識及媒體素養相關課程。 原民會：辦理原住民族網路詐騙防治相關資訊安全課程講座。

措施	主(協)辦機關	工作項目
1-2-5 推動公務機關留才機制，提升人員留任誘因	數發部	(1) 訂定公務機關資通安全業務績效評核及獎勵規範，辦理績效評核及獎勵作業。 (2) 訂定資安專業人才留任獎勵金支給表，提升資安人員待遇增加留任意願。
1-3 建構全社會資安防護網		
1-3-1 強化數據與隱私保護，降低個資外洩風險	各機關	各領域訂定個人資料檔案安全維護管理辦法等相關規定。
1-3-2 強化資料與情資分析，打擊網路犯罪	內政部、法務部	內政部：建立駭侵情資蒐整與分析機制，提升資安事件、駭侵案件等之溯源追查能力。 法務部：建置文字模型子系統及專案數位跡證分類庫，自動產出通訊內容摘要，並開發和訓練 AI 生成文字內容識別模型。
1-3-3 運用數位科技偵查技術，精進資安鑑識能量	法務部	(1) 犯罪金流分析：包括交易情資蒐集與金流分析功能，建立自主性情資蒐集及偵調分析工具。 (2) 建置區塊鏈會員協作節點，使訴訟活動實際運用於數位證據之驗真。
策略二：提升關鍵基礎設施資安韌性		
2-1 建立關鍵基礎設施資安防禦體系		
2-1-1 建置關鍵基礎設施之資安防衛體系	數發部	(1) 建立 CI 專業保護團隊，提供評估、威脅狩獵及事件處理三類服務。 (2) 115-117 每年擇定 CI 提供者提供深度檢測服務。
2-1-2 建立國家層級威脅模型，蒐集各領域威脅特徵	數發部	建立自評估、威脅偵測、事件處理、自動化開發及作業管理各階段一致性管理流程，降低人為錯誤風險，維持作業品質。

措施	主(協)辦機關	工作項目
2-1-3 辦理檢測核心技術訓練及移轉，提升防護能量	數發部	融合國際專業知識與我國目前之資通安全能量，結合 CI 提供者之需求，發展進階持續型服務。
2-2 提升關鍵基礎設施資安聯防能量		
2-2-1 強化關鍵基礎設施資安威脅監控	各 CI 主管機關	各 CI 領域辦理資通安全威脅監控與防護。
2-2-2 加強關鍵基礎設施情資分享運作，提升整體數位防護	各 CI 主管機關	精進各 CI 資安聯防機制(情資分享、通報應變、資安監控)，強化橫向分享交流。
2-2-3 關鍵基礎設施資安實地演練與稽核，提升資安韌性	各 CI 主管機關	各 CI 辦理攻防演練及資安稽核，檢測資安監控及防禦部署之有效性。
2-2-4 辦理跨國網路攻防演練(CODE)及相關國際演訓	數發部	(1) 配合工控訓練場域及演練領域，分年度增建演練場域。協調中央目的事業主管機關及 CIP，規劃 CODE 賽制及演練場域設計。 (2) 辦理 CODE 2025 及 CODE 2027
2-3 精進關鍵基礎設施資安治理能力		

措施	主(協)辦機關	工作項目
2-3-1 落實各領域資安防護基準，強化關鍵基礎設施資安防護	各 CI 主管機關	(1) 產製 CI 領域工業控制系統資安防護評估報告，提供我國各中央目的事業主管機關參考修訂工控資安防護基準。 (2) 研擬或滾動修訂通傳領域 CI 特定類型資通系統之防護基準草案，並辦理配合公告事宜。 (3) 輔導所管機關落實「交通領域工業控制系統資安防護基準」，整合通訊多元服務與強化資安防禦。 (4) 持續依資通安全責任等級分級辦法附表十規定之資通系統防護基準執行控制措施。 (5) 挑選場域進行 ISO27001 與 IEC 62443 之差異化分析。 (6) 辦理防護基準輔導、資安稽核，並辦理 OT 資安治理成熟度輔導作業。 (7) 醫療機構落實 OT(連網醫療儀器)資安防護基準，提升整體醫療領域資安意識。 (8) 選擇高風險 CI 提供者場域試行金融零信任架構。
2-3-2 提升工控領域資安治理成熟度	數發部	每年自 A、B 級之公務機關或 CI 提供者擇選輔導檢視資安治理成熟度待精進處，以協助完善 CI 資安防護整備度。
策略三：壯大我國資安產業		
3-1 推動資通產品檢測制度		
3-1-1 推展產品資安檢測及驗證，確保產品安全	數發部	(1) 推動衛星通訊產業資安標準/指引或規範。 (2) 提升電信網路設備及遙控無人機之資安防護。 (3) 研析國際產業資安標準，提供諮詢並輔導國內廠商合規。 (4) 推動 IOT 檢測實驗室，發展資安產品驗證標章。

措施	主(協)辦機關	工作項目
3-1-2 推動數位服務之資安檢測，提升資安防護能量	數發部	協助電商及企業完成資安檢測。
3-2 強化政府採購供應鏈風險管理		
3-2-1 促進政府機關導入優質民間資安廠商，降低風險發生與衝擊	數發部、工程會	數發部： (1) 每年對資安服務廠商辦理評鑑。 (2) 每年遴選軟體共契重要廠商辦理資安訪視。 數發部、工程會：每年精進採購作業資安要求相關文件之檢視或增修訂。
3-2-2 協助民間廠商漏洞審查及諮詢，加強風險監控與審查	數發部	(1) 每年受理及審核國內企業產品資安漏洞。 (2) 每年協助民間資訊安全相關諮詢或應變處置。 (3) 每年辦理企業資安演練。
3-3 擴大資安產業規模並向國際輸出		
3-3-1 提升資安產業創新能量與解決方案，提升零信任環境	數發部	(1) 引導資安產業發展零信任物聯網資安技術，推動符合不同領域的零信任資安防護產品。 (2) 輔導物聯網場域業者，偕同供應鏈廠商建立零信任資安強化示範應用案例。
3-3-2 整合相關資源，打造具國際信賴之資安產業	數發部	(1) 推動資安廠商完成募資輔導。 (2) 輔導資安廠商於海外落地成立分公司或據點。 (3) 推動國際資安廠商合作解決方案。
3-3-3 升級資安科技園區，帶動南部產業鏈發展	數發部、國科會	數發部：持續推動沙崙資安服務基地場域參訪及觀摩，協助產業導入資安防護及提升競爭力。 國科會：強化沙崙科學城 C 區資安暨智慧科技研發專區大樓之優質智慧設施環境。

措施	主(協)辦機關	工作項目
策略四：AI 新興資安科技應用與合作		
4-1 拓展 AI 技術應用以提升資安防護能量		
4-1-1 推動 AI 網路主動式防禦關鍵技術研究，提升處理威脅情資之效能	數發部	(1) 推動資安網路防禦技術 AI 化：專注 AI 推論能力應用威脅偵測演算法與自適應防禦機制研發，運用深度學習技術開發異常行為識別、攻擊模式預測與自動化應變系統，建立高效能 AI 資安模型，提升系統對未知威脅的預警與防禦能力。 (2) 應用 AI 技術強化主動資安情資蒐整能力：目標透過 AI 推論能力結合自動化收集與分析多來源威脅情報，為資安團隊提供即時精確的威脅評估與預警，提升組織對新興威脅的感知與應變能力。 (3) 前瞻資安技術發展：專注於研發下一代資安技術，透過監測全球趨勢與分析新興威脅，結合人工智慧技術設計創新防護機制，為組織建立更具韌性的資安防線，有效應對未來網路攻擊挑戰。
4-1-2 應用 AI 強化資安治理，掌握國家威脅態勢並強化治理透明度	數發部	規劃建置「國家資安治理情資平臺」，發展結合資安治理與威脅態勢之高可視性戰情牆。
4-1-3 運用 AI 技術於資安稽核資料分析，擴展資安防護層面	數發部	規劃建置稽核資料分析平臺，綜整資安法納管機關稽核資料與資安會報資安稽核結果資料。
4-1-4 推動我國 AI 評測制度與可信任 AI 環境發展	數發部	(1) 修訂 AI 產品評測指引。 (2) 協助公部門及鼓勵企業進行第三方評測，評測 AI 模型之表現，以及提供回饋建議，提升企業產品競爭力，健全模型符合資訊安全與隱私保護。
4-2 強化新興資安科技前瞻研究		

措施	主(協)辦機關	工作項目
4-2-1 輔導無人機安全及醫療應用等新型資安技術能量	國科會、衛福部	國科會：研發我國自主無人載具關鍵技術，補足國內無人機技術缺口。如飛行控制、感測技術、航電資通訊、軟體開發、AI 導控及無人機資安能力等創新技術為目標；培養我國無人機人才並落實產業應用。 衛福部：強化醫療機構新科技，訂定應用新科技資安及個資保護參考規範，並於 CI 醫院試行。組成專家小組訂定應用新科技(如人工智慧、大型語言模型、穿戴式裝置、雲端服務)資安及個資保護參考規範，並於 CI 醫院試行。
4-2-2 精進雲端服務資安，保護資料安全與隱私	國科會、數發部	國科會：建置臺灣可信賴資料雲端分析平臺，以具高資安與隱私防護、特別權限管理、隔離封閉之儲存區，以及可提供資料不落地分析等特色服務，推動於科研、生醫研究、國土治理與國防科技應用等。 數發部：發展雲端服務的政府組態基準，持續檢視並視需要調修雲端服務應用資安參考指引。
4-2-3 研析後量子密碼資安架構及國際趨勢	數發部	(1) 研析各國後量子密碼相關推行政策、發展情形，提出我國後量子密碼發展建議。 (2) 推動業者發展後量子密碼相關解決方案。
4-3 促進國際資安交流合作		
4-3-1 建立技術交流及情資分享等合作管道，促進國際聯防	數發部	促成與國外技術或研究機構交流機制。
4-3-2 舉辦及參與國際研討會或競賽，鏈結國際夥伴信任關係	數發部、內政部	數發部：辦理跨國研討會、討論議題及蒐集專家意見，協助我國與各國經驗交流，強化與友好國家資安聯防交流，深化我國於國際資安領域之發展。 內政部：培育科技偵查專業人才，加強犯罪偵查技能之實務訓練及認證，強化新型網路犯罪偵查能量，並參加國際研討會，瞭解新型科技應用。

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
中華民國 108 年 2 月 14 日行政院院臺護字第 1080163928 號函修正發布，並自 108 年 2 月 14 日生效
中華民國 109 年 12 月 25 日行政院院臺護字第 1090202543 號函修正發布，並自 109 年 12 月 25 日生效
中華民國 112 年 2 月 22 日行政院院授數資安字第 1121000065 號函修正發布，並自 112 年 2 月 22 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(以下簡稱本會報)。

二、本會報任務如下：

(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、本會報置召集人一人，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。

為協調及推動國家資通安全政策，本院置資通安全長一人，由本

會報召集人兼任。

四、本會報之幕僚作業，由數位發展部辦理。

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：由數位發展部主辦，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：數位發展部主辦，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：數位發展部主辦，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：數位發展部主辦，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：數位發展部主辦，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。
6. 外館網際防護組：外交部主辦，負責統合外館各合署機關之資訊及網路管理，以提升外館資通安全防護能力，降低發生網駭及資安事件之風險。

(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. 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、數位鑑識及檢討防制網路犯罪相關法令規章等工作。
2. 資通訊環境及網際內容安全組：國家通訊傳播委員會主辦，負責促進資通訊傳播環境及網際內容安全，推動通訊傳播事業配合辦理防治網路犯罪及維護網際內容安全等措施，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，本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，由本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、本會報原則上每半年召開會議一次，由本會報召集人主持；資通安全諮詢會原則上每年召開會議一次，由本會報召集人指定之副召集人主持；各項會議，必要時得召開臨時會議。

八、本會報及資通安全諮詢會委員、各組召集人，均為無給職。