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

中華民國 112 年 5 月修正

目　錄

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)受駭等。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，可見提升國家資安防護能量，強化基礎通訊網路韌性及安全，的確有其必要性。

另外，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」，透過建立臺灣品牌、靈活多元的金融支援、安全的產業發展環境、匯聚及培養數位/雙語人才，讓我國成為全球經濟的關鍵力量。然各項產業在創新經濟的轉型過程中，均應納入資安防護思維，以形成政府機關與民間企業協力聯防之基礎，讓資安意識可深植人心，形塑資安文化，提升國家資安軟硬實力，建立讓社會大眾可安心信賴的智慧國家。

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，除持續落實第五期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(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(110 年至 113 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)「全球風險報告」顯示，在 109 年全球可能風險排名中，網路攻擊不論是在影響風險(Global Risks in Terms of Impact)或是在可能風險(Global Risks in Terms of Likelihood)皆位於前 10 名之列，顯見網路攻擊儼然已成另一種虛擬戰爭，影響範圍小至個人生活，大至國家安全層級。

網路攻擊已為資通安全顯學，經綜整 108 年全球重大網路攻擊事件，以資安事件發生之種類與多寡，進一步分析全球相關資安事件，歸納出 6 大面向資安威脅趨勢，包含「個人資料與憑證外洩攻擊白熱化」、「勒索軟體攻擊風險激增」、「IoT 與行動式設備資安弱點威脅升高」、「APT 鎖定式攻擊竊取機敏資料」、「資安(訊)供應商持續遭駭破壞供應鏈安全」及「關鍵資訊基礎設施資安風險倍增」，茲說明如下。

(一)個人資料與憑證外洩攻擊白熱化

身分情報公司 4iQ 於 108 年第 1 季發布「2019 4iQ Identity Breach Report」，報告中指出 107 年在網路上流傳的身分資料約有 149 億筆，遠高於 106 年的 87 億筆。分析外洩事件發生的產業別，以網路論壇占 27.5%位居第一，政府機關占 12.2%居次，遊戲產業占 11.8%，電子商務網站占 11.7%，教育及學術界則占 9.2%。根據數據分析顯示，渠等於網路上流竄之個人身分資料僅有 37%係遭駭客攻擊而外洩，其餘 63%係因意外曝光。4iQ 推測此乃許多公司將系統移轉到雲端，未

注意安全存取權限設定，意外洩露資料庫或伺服器所造成。

108 年第 4 季國內某科技大廠發生員工竊取客服資料庫事件，足以顯見企業面臨更加險峻的內部威脅(Insider Threat)，該公司同年 11 月 5 日於官方部落格坦承，發現員工竊取客服資料庫內容，並販賣給不知名犯罪組織牟利，影響近 12 萬名用戶。因此個人資料與憑證外洩來源不僅可能來自於外部駭客惡意攻擊，更可能源自於內部意外或惡意洩露。

(二)勒索軟體攻擊風險激增

108 年 10 月資安業者 Emsisoft 於官方部落格公布美國 108 年前 3 季勒索軟體調查結果，此一調查係針對遭到勒索軟體攻擊的美國政府機構、學校及醫療服務供應商進行相關統計，調查結果顯示 9 個月以來，至少有 621 個組織遭到勒索軟體攻擊。當美國各州、城市或郡遭到勒索軟體攻擊時，很容易就會躍上新聞版面，但在遭到攻擊的 621 個組織中，僅有 68 個為政府機關，代表有更多組織遭受勒索軟體攻擊，卻密而不宣。

根據 Emsisoft 觀察，越來越多駭客鎖定託管服務供應商或第三方服務供應商，因為一次成功攻擊就能同時入侵眾多個使用同樣資通服務的組織。此外，駭客所要求的贖金也越來越高，假設受害者願意支付第一次贖金，那麼駭客下一次可能就會提高贖金金額。另一個值得觀察的趨勢是資安險之興起，當越多組織投保資安險，將使該組織更願意支付贖金，並成為駭客持續攻擊之動機與目標。

分析目前勒索軟體的攻擊手法，相較於直接攻擊鎖定目

標，駭客採取迂迴手法先試圖攻擊防護等級較弱之第三方服務供應商，進而攻擊真正目標對象，同時隨著受害者因保險的風險轉嫁而選擇支付贖金，更助長利用勒索軟體入侵之盛行。

(三)IoT 與行動式設備資安弱點威脅升高

前於 105 年間，駭客利用 Mirai 殭屍網路病毒挾持 50 萬台網路攝影機，發動 DDoS 攻陷代管業者。嗣後，Palo Alto Networks 的研究單位 Unit 42 於 108 年初發現 11 隻新的 Mirai 變種病毒，與先前版本不同之處，這些變種病毒係針對企業級 IoT 設備，如無線投影系統、智慧電視等，顯示駭客似乎已將目標轉向企業網路，藉以取得更大頻寬建立殭屍網路，便於日後發動 DDoS 攻擊。

行動式設備風險隨著運用範圍廣泛與擁有行動式設備普及而日益增加，108 年 11 月在東京舉辦的全球知名白帽駭客大賽「PWN2OWN」，參賽的駭客便破解多項連網裝置並揭露其漏洞，例如手機、路由器及家用智慧裝置等產品，可見其嚴重性。

(四)APT 鎖定式攻擊竊取機敏資料

駭客採用 APT 攻擊手法通常鎖定具有機敏性資料或大量個人資料之目標對象，如金融業者、國防單位或社群媒體等，特別是現在政府機關或企業高度仰賴之雲端服務，皆是被鎖定之攻擊目標。駭客鎖定目標後，處心積慮蒐集各種可以使用的弱點與漏洞，包含社交工程手法、偵測所使用之資通系統漏洞及供應鏈等各種可能入侵手法，以達到成功入侵組織

內部之目的。

108 年德國法蘭克福遭受 Emotet 惡意程式鎖定攻擊，致數個城市與學術網路關閉。Emotet 具備自我傳播的進階模組化木馬程式，最初被駭客運用於銀行木馬惡意程式，近來則被廣泛用於作為其他惡意軟體或惡意攻擊的傳播程式。Emotet 使用多種方法與規避技術來維護其持續性，更透過夾帶惡意附件或連結的網路釣魚垃圾郵件進行傳播。在受到 Emotet 惡意程式感染後，法蘭克福於 108 年 12 月關閉網路，然於此之前，德國已有 2 家大學與另一個位於法蘭克福以北城市因遭受 Emotet 攻擊，同樣先行關閉網路，可見 APT 攻擊帶來之影響衝擊須審慎應對。

(五)資安(訊)供應商持續遭駭破壞供應鏈安全

資安業者 Proofpoint 於 108 年 9 月在官網發布訊息，某國家級駭客集團持續鎖定美國公用事業服務(Utilities Sector)供應商，展開魚叉式網路釣魚(Spear Phishing)攻擊，在受害者系統上植入 LookBack 惡意程式，經統計，至少已有 17 個供應商遭到攻擊。Proofpoint 進一步指出，同一駭客集團於同年 8 月再度發動新一波攻勢，目標同樣是美國公用事業服務供應商，但這次在網路釣魚郵件中偽裝成全球能源認證機構(Global Energy Certification, GEC)，邀請受害者參加認證考試，同樣附上含有惡意巨集的 Word 檔案。Proofpoint 表示，駭客集團未因之前攻擊曝光而銷聲匿跡，反而不斷地改善網路釣魚攻擊策略、技巧及程序，明確暴露該集團對美國公用事業服務供應商的惡意企圖。

供應商可能因為資安防護機制缺陷或是專注於業務成長輕忽資安重要性，因此相對於駭客的真正目標較易入侵。爰此，駭客可利用資通訊設備供應商做為跳板，進一步針對真正目標進行攻擊。

(六)關鍵資訊基礎設施資安風險倍增

關鍵基礎設施(Critical Infrastructure, CI)範圍相當廣泛，且與民眾生活密不可分，包含能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等領域，而支持 CI 所需之資通系統為關鍵資訊基礎設施(Critical Information Infrastructure, CII)，亦是重要防護範圍，一旦遭駭，將影響民眾生活，甚至社會秩序與國家安全。近年來，因 CII 資訊架構漸趨開放式與網路串連，相關資安風險也隨之而來。

美國國家能源技術實驗室公布 108 年第 1 季 OE-417 電力緊急情況與干擾報告說明網路攻擊造成的電力系統運行中斷事件，報告顯示該事件受害者為一家位於猶他州的再生能源(Renewable Energy)電力生產商。該攻擊利用防火牆已知漏洞，觸發阻斷服務攻擊(Denial of Service, DoS)指令，造成系統重新啟動，導致該公司控制中心與其他各個站點設備之間通訊中斷。

另一項讓各國政府及社會持續高度關注的議題為影響社會秩序及安全甚鉅的暗網(Darknet)，根據資安業者 Digital Shadows Photon Research 發現，在暗網上流傳的被盜用戶帳號與密碼數量是全世界人口數量的近 2 倍。在暗網賣家所

販售與分享的憑證，總計有 150 億組的外洩憑證，其中三分之一為不重複的憑證。這些藉由資安事件外洩的帳戶資訊主要來自於線上服務，如網路銀行、社群網站及音樂串流服務等，而利用暗網的黑市交易與分享，造成憑證外洩事件擴大，亦讓資安事件層出不窮。

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、加拿大、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

美國資安主管機關為國土安全部(Department of Homeland Security, DHS)。在 2018 年後，美國通過網路安全暨基礎設施安全局(Cybersecurity and Infrastructure Security Agency, CISA)法，由該局負責資通安全相關業務。另有美國國家標準技術研究所(National Institute of Standard and Technology, NIST)制定國家測量標準，NIST 於 2014 年 2 月發布資通安全架構(Cybersecurity Framework, CSF)1.0 版，並於 2018 年 4 月發布修正後之 1.1 版，以利聯邦政府各機關或相關單位遵守。茲摘述重點如表 1。

表 1：美國 NIST CSF 架構(2018 年 4 月 1.1 版)

識別	保護	偵測	應變	復原
1.資產管理 2.營運環境 3.治理 4.風險評估 5.風險管理策略 6.供應鏈風險管理	1.身分管理與存取控制 2.認知與訓練 3.資料安全 4.資訊保護流程與程序 5.維運 6.防護技術	1.異常與事件 2.持續性安全監控 3.偵測流程	1.應變計畫 2.溝通 3.分析 4.減輕 5.改善	1.復原計畫 2.改善 3.溝通

資料來源：NIST Cybersecurity Framework

美國 NIST 之 CSF 架構係以識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、復原(Recover)五大功能進行區分(架構如圖 1)。聯邦政府各機關及關鍵基礎設施等，搭配 NIST 之 CSF 架構與資通安全相關文件，如 Special Publication (SP) 800 系列，據以規劃與建立資通安全管理制度。且因該架構亦能適用於一般企業，爰已逐漸成為其他國家或地區之企業或組織，就資通安全之風險管理的主要參考工具之一。

為進一步提升主動防禦與相關能量，保護國家資產及民眾隱私，並提高惡意者攻擊代價，美國於 2018 年 9 月公布國家網路戰略(National Cyber Strategy)，共計分 4 大構面及 10 項目標。該戰略將提供安全的網路、資訊及關鍵基礎設施，並將積極打擊網路犯罪，強化事件通報與應變等作為目標。

據此，預計加強管理資通安全、強化風險管理及供應鏈安全之相關作為。

圖 1：美國 NIST 之 CSF 架構圖

(二)加拿大

加拿大資安主管機關為公共安全部(Public Safety Canada, PS)。為強化資通安全相關能量，加拿大於 2018 年依據「國家資通安全戰略(National Cyber Security Strategy, NCSS)」，將有關資通安全之業務單位進行整合，設立資通安全中心(Canadian Centre for Cyber Security, CCCS)。

資通安全中心成立後，主要負責資通安全事件之應變，並為該國電腦緊急應變團隊(Computer Emergency Response Team, CERT)及政府電腦事件應變團隊(Computer Incident Response Team, CIRT)，與其他政府部門、關鍵基礎設施、企業及國際夥伴等密切合作。該中心亦透過監控識別威脅、風險與漏洞等，協助聯邦政府部門強化資安防禦能量，並與研究人員、關鍵基礎設施及學術機構積極合作，解決相關資通安全問題。

而加拿大於 2019 年 5 月公告國家資通安全行動計畫(National Cyber Security Action Plan)2019-2024，計有3大目標：(1)強化關鍵基礎設施防護並增強網路犯罪調查能力，(2)支持前瞻研究並協助創新企業，(3)國內與各省及民間合作、國外結合盟友共同塑造環境。

為了加強公私協力，以共同打擊網路犯罪，加拿大將擴大資通安全合作計畫(Cyber Security Cooperation Program, CSCP)，強化與內外部利害關係人，如民眾、社區等對象之連結，並提供必要資源。

(三)歐盟

歐盟資安與資訊主管機關為歐盟網路與資訊安全局(European Union Agency for Cybersecurity, ENISA)。歐盟於2019年6月施行資通安全法(Cybersecurity Act)，擴大ENISA之權利與義務，不僅可協助ENISA強化治理權限、提高人力、財務資源分配，並建立「歐盟資通安全驗證架構(European Cybersecurity Certification Scheme)」機制，評估資通訊產品、服務及製程是否符合安全。茲就其驗證方式、內容及影響對象等摘述如下：

1、方式：訂定產品或服務之類別、資通安全規範(如參考標準或技術規範)、評估類型(如屬自我評估或第三方評估)、預期的保證等級(如基本、稍多、高)。證明書上使用3個級別：基本(basic)、稍多(substantial)及高(high)以顯示其資通安全風險，認證為高等級的產品代表已經通過最高等級的安全性測試，使企業進行跨境交易，讓使用者更

容易理解產品或服務的安全性，亦使歐盟市場的供應商間能進行有益的競爭，從而產生更好的產品及性價比。

2、對中小企業及新企業的價值：有助於減少中小企業和新企業進入市場的阻礙，因為公司只需經過一次產品認證，其證書在整個歐盟範圍內均有效，同時隨著安全需求增加的趨勢，產品獲得認證的中小企業將在全球享有一定的競爭優勢。

3、資通安全驗證或認證機制：供應商藉由該機制使其產品取得證書，以確保資通訊科技(Information Communication Technology, ICT)產品、服務和流程的資通安全能維持足夠水準，並改善內部市場的運作。

4、設計安全性：鼓勵產品、服務或流程設計的開發製造商或提供商在設計和開發的最初階段就實施該機制，能以更高的程度保護這些產品、服務或過程的安全性，並使受到網路攻擊的損害最小化。

5、受惠者：如公民及營運商。例如個人、商業買家、政府，在購買某產品或服務時，可以查詢 ENISA 資通安全認證網站，使產品或服務的資通安全資訊更透明。或是產品服務的供應商和提供者(包括中小型企業和新創企業)藉由該機制獲得相關證書，提升其競爭力。

（四）英國

英國政府之資通安全主管機關為家資通安全中心(National Cyber Security Centre, NCSC)，且於 2016 年 11 月公告國家資通安全戰略(National Cyber Security

Strategy)2016-2021，主要包含防禦(Defend)、嚇阻(Deter)及發展(Develop)3 大戰略目標，希冀達成防護政府網路及關鍵基礎設施、扼制網路犯罪、發展資通安全相關科學研究。該國內政部於 2019 年 5 月公開該戰略之執行情形，其成效包含提升對資通安全威脅的了解，降低來自網路攻擊的威脅，並為建議與支持提供整合資源。另透過積極網路防衛計畫(Active Cyber Programme)成功阻擋每個月 450 萬件惡意電子郵件，以及抵禦超過 14 萬個惡意網路釣魚網站等。

英國雖於 2020 年 1 月底正式脫離歐盟，但在資通安全或資料保護等法制，仍期與歐盟法規一致。如英國已在 2018 年修正資料保護法(Data Protection Act 2018)，對於個人資料定義類同「一般資料保護規範(General Data Protection Regulation, GDPR)」，並參採如當事人同意、資料近用權(right of access)、被遺忘權、資料可攜權、設置資料保護專員等規範。此外，英國也在 2017 年 3 月公布「數位策略政策(Digital Strategy)」，包含：打造世界級的數位基礎設施、讓英國成為全世界最適合數位企業創業與發展的國家、幫助每家英國企業成為數位企業、成為全世界網路最安全的國家、持續作為提供公民最佳線上服務的世界級領先國家、發揮資料經濟實力、並改善民眾使用資料的信心等 7 項內容，相關措施可看出英國希冀不因脫歐而失去在資料經濟時代的影響力。

(五)日本

日本資安主管機關為資通安全戰略本部(Cybersecurity

Strategic Headquarters)與國家資通安全資安事件應變處理與戰略中心(National center of Incident readiness and Strategy for Cybersecurity, NISC)。日本政府於2014年通過資通安全基本法(Cybersecurity Basic Act)，目的為加強日本政府與民間在資安領域的協調，後於2018年12月進行修正，主要有兩項，一是新增設立「資通安全委員會」，主要成員為國家行政機關首長、地方自治團體、關鍵基礎設施營運者等民間專業人士，負責推動資通安全相關政策的協議；二是擴增資通安全戰略本部掌理的業務，當資安事件發生時，對國內外利害關係人進行聯繫。

2018年7月公告最新之資通安全戰略(3年期)，具有「提升經濟社會活力及永續發展」、「實現人民安全、安心生活的社會」及「確保國際社會的和平、安全，並確保日本安全」等3大目標，並包含4項策略：(1)實現資通安全供應鏈及架構安全IoT系統，(2)建構大學教研環境，(3)制定網路犯罪對策，以及(4)強化政府網路防禦、抑制網路攻擊能力與應變大規模攻擊之能力。

另外，日本因考量中小企業、地區的資源及人才都有限，無法完全倖免網路攻擊，爰透過事先支援中小企業，派遣資訊安全專家(Registered Information Security Specialist, RISS)協助企業進行資安管理及處理相關事項，於資安事件發生後則設有資通安全救援隊提供中小企業相關協助；至於在社區方面，透過與高階專業機構等產業、學界與政府的合作推動地方人才培訓，並展開合作平台，與地方確保資訊安全

專家及產業資通安全中心研習生合作。

(六)韓國

韓國主要資安推動機關為國家安全辦公室(Office of National Security)，並分別由國家情報院(National Intelligence Service, NIS)負責總管國家與公共機關之資訊安全業務，科學技術情報通信部(Ministry of Science and ICT)負責總管民間資通訊基礎設施保護以及主要資通訊基礎設施之業務。

韓國整體資通安全政策係依據「國家情報院法」、「資訊通信基礎保護法」、「電子政府法」、「國家資訊化基本法」等相關法令設置，負責整體國家資訊安全業務等計畫、調整案及安全政策之建立、施行，並總管對於國家、公共機關之資訊安全業務。搭配相關法規結合各部會能量，推動資安業務，例如：韓國資訊安全產業振興法於 2018 年 2 月進行修正，並於同年 5 月施行，該產業振興法設立目的是為了奠定資訊安全產業的基礎以及加強競爭力，因此針對資訊安全產業振興之所需事項訂立政策目標，讓資訊通訊使用環境更安全，並且提升國民經濟。在該法第 3 條更進一步要求國家及地方政府，為振興資訊安全產業，必須施行所需政策，並建立財政確保方案；另依該法第 14 條，科學技術資訊通訊部(Ministry of Science and ICT)部長可促進相關事業之資訊安全技術的開發與投資。

於 2019 年 4 月公告最新之國家資通安全戰略，具有 6 個目標，包含：加強國家核心基礎設施安全、提高網路攻擊應變

能力、建立具信任和管理的網路治理、奠定資通安全產業基礎環境、培養資通安全文化，以及領導國際資通安全合作。

以前述目標 2 為例，為增強韓國對於網路攻擊之應變能力，將就確保網路攻擊之防範、增強對大規模網路攻擊之準備能力、制定針對網路攻擊全面且有效的對策、增強網路犯罪之應變能力，據以制訂相關措施，如集中國家(各部會)能量對應影響國家安全與利益之網路攻擊，廣泛蒐研威脅或弱點相關資訊，並進行分析，以增強應變能力等。

(七)新加坡

新加坡資安主管機關為新加坡資通安全局(Cyber Security Agency, CSA)。在整體資通安全政策部分，新加坡於 2016 年公布「資通安全策略」(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以面對網路威脅、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)發展包含技術勞動力、具備先進技術的企業以及強大研究能量之資通安全生態系統(Cyber Security Ecosystem)，以支持新加坡的資通安全需求。(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。

目前最新的 5 年期資通安全精進計畫為「2018 年國家資通訊安全精進計畫」(Infocomm Security Masterplan, ISMP)。在前兩期精進計畫的基礎上，藉由政府、關鍵資通訊基礎設施(Critical Infocomm Infrastructure)、企業與個人的努力來強化新加坡的資通安全，包含 3 項重點：(1)強化關鍵資

通訊基礎設施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)。

另為發展數位經濟，新加坡特別加強電信領域之資安防護工作，以因應國內外之資安威脅。自 2018 年開始，由資通訊媒體發展管理局(Infocom media development authority, IMDA)籌備成立電信資通安全戰略委員會(Telecom Cybersecurity Strategic Committee, TCSC)，以提高國家面對資安威脅時之因應能力，並提升新加坡處理關鍵資通訊基礎設施問題的能力。電信資通安全戰略委員會成立後，主要將與電信行業間(包含全球網路安全專家和主要電信運營商)建立合作夥伴關係，以強化電信基礎設施之防護，並建立新加坡電信運營商的網路安全能力。

(八)澳洲

澳洲資安主管機關為隸屬國防部之通信局(Australian Signals Directorate, ASD)。在資通安全領域內，澳洲較著重資訊分享與犯罪防制之關聯，並透過軍事組織協助相關業務。該局主要透過 3 大項目協助維護澳洲之資通安全：(1)通知(Informing)，透過相關機制獲得未公開之國際資訊，並進行通知或資訊分享。(2)保護(Protecting)，透過對可能威脅之掌握，主動提供建議或協助，以改善政府、企業或社區面對網路威脅之風險管理。(3)破壞(Disrupting)，透過科技應用或主動防禦技術等，破壞可能攻擊，打擊恐怖主義、網路間諜活動，以及屬嚴重罪刑之網路犯罪等。

澳洲司法部自 2010 年起提供保護性安全政策架構(Protective Security Policy Framework, PSPF)，包含5項原則、4 項安全面向(Outcomes)與 16 項核心要求(Core Requirements)；其中，安全面向主要為治理(Governance)、資訊(Information)、人員(Personnel)及物理環境(Physical)之建議，並搭配對應之核心要求，採標準化方式以利執行。

目前澳洲資通安全政策最新的4年期規劃為2020年資通安全戰略,其於2020年8月公告,預計將於10年內投資16.7億澳幣，投入：(1)由政府採取行動，加強對澳洲人民、企業及關鍵基礎設施的保護，使其免受多元的威脅。(2)由企業採取行動，以保護其產品和服務，並保護其客戶免受已知網路漏洞的侵害。(3)由社區採取行動，提升民眾對於網路交易行為之安全意識，以確保消費安心購物。透過政府、民間與社區共同努力，促進資通安全。

(九)以色列

以色列政府的資安主管機關，2018年7月1日以後正式由國家網路指導委員會(National Cyber Directorate, INCD)負責，該國主要透過軍、官、民三者通力合作，建構資通安全防護機制。平時透過INCD協助公、私部門落實資安防護；當資安事件發生時，則由該委員會下設之國家資安事件準備小組(CERT-IL)協處，並執行情資分享與漏洞修補等；而當有國家層級的事件發生時，由主管機關與情報單位執行入侵源頭追查及事件應變，並與國內外情報機關合作，如嘗試找出攻擊者，以因應可能影響或威脅。

以色列對於資安或資通安全，係由部會分工，列入所屬機關之年度施政工作內。除 INCD 外，以色列公安部(Ministry of Public Security)亦權責網路犯罪，該部於 2016 年將打擊網路犯罪及防杜社交媒體霸凌，列入當年度目標，且對資料竊取、病毒、未成年色情新興犯罪模式加強查緝。該部 2019 年度報告(Ministry Overview – 2019)中，持續關切網路犯罪、資安威脅或恐怖攻擊，以及與 INCD 等機關合作，保護 CI 或其他資通系統，避免遭受外來的攻擊或威脅。

在 2018 年以色列曾研擬「資通安全法」草案，規範包含：擴大 INCD 權能，除直接對總理負責、協助評估國家網路風險、國家整備與復原能力的規劃等外，為辨識、預防、減緩敵意行為等考量，該法案授權該委員會可以直接或在法院的授權下，存取私部門的文件與電腦資料，及獲取設備進行檢查。但由於部分項目爭議過大，目前暫未完成相關程序。

此外，值得特別說明的是，以色列政府非常鼓勵資安產業發展，例如以色列創新局(Israel Innovation Authority, IIA)建立孵化器或平臺，讓該國境內企業得以全球作為市場，或鼓勵境內廠商參與國際論壇，協助尋求合作夥伴或促進媒合，並補助具發展潛力的企業投資計畫等。

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，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，除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 2 月 22 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 2。

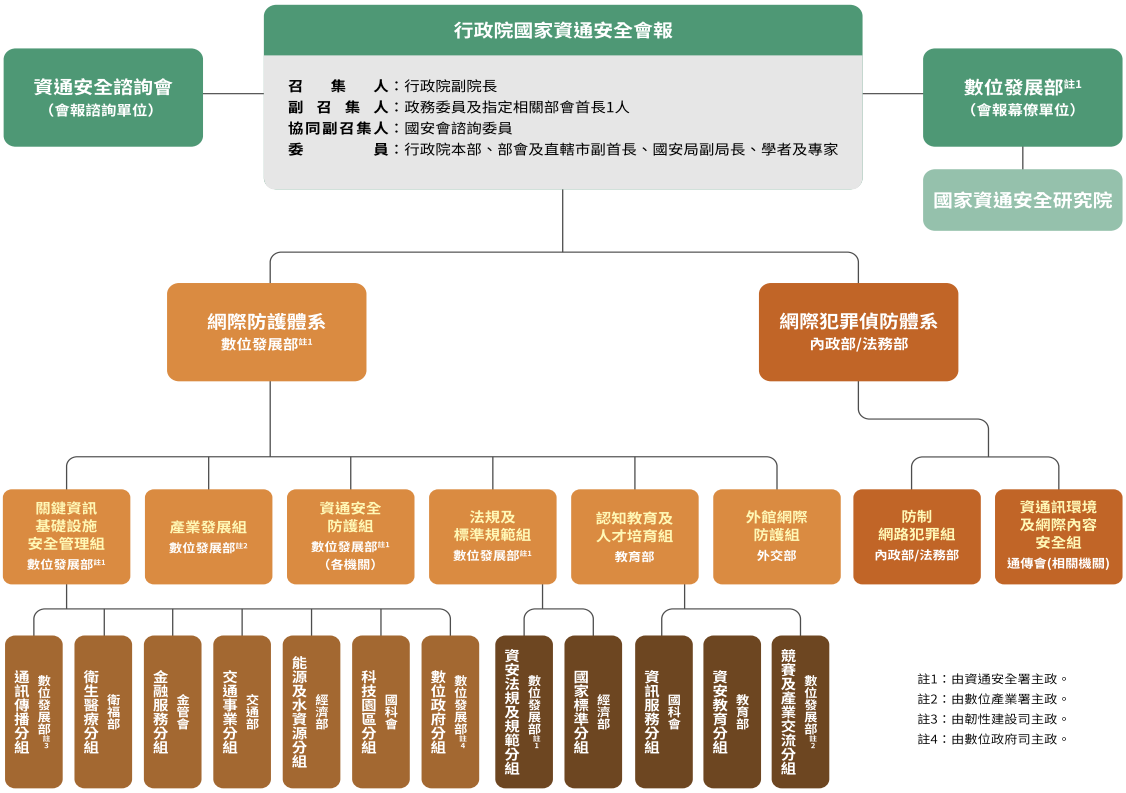

圖 2：資安會報組織架構圖

(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「台灣網路資訊中心」(Taiwan Network Information Center, TWNIC)負責維運「台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5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3。

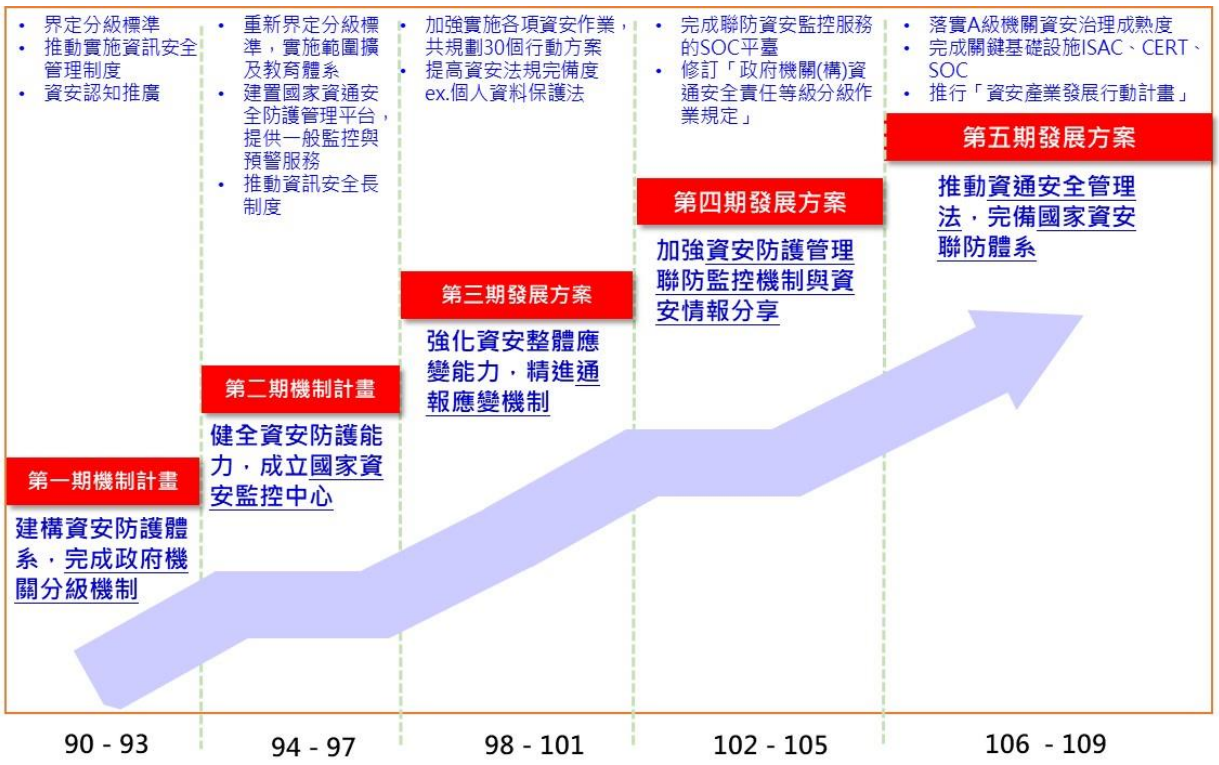

圖 3：我國資安推動進程

（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)，為因應政府推動數位國家與創新經濟發展所面對的資通安全威脅和挑戰，在我國「資安即國安」的政策方向下，將資安提升至國安防護層級，持續推動政府精進與落實各類資安防護措施，以因應複雜多變的資

安威脅。

第五期以「打造安全可信賴的數位國家」為願景，搭配「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」3 大政策目標，並從「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 4 大推動策略著手，訂定 11 項具體措施，逐步推動我國資安縱深防禦及聯防體系，以穩固我國數位國土的資安防線，其目前執行重點及推動成果說明如下：

1、 完備資安基礎環境

(1) 107 年 5 月 11 日經立法院三讀通過資通安全管理法，6 月 6 日總統令公布，12 月 5 日函頒施行令，建立我國資安法制化之基礎，於 108 年 1 月 1 日正式施行，資通安全管理法制定之六項子法亦同步施行，明定落實各項資安作業。

(2) 為建構我國資通訊產品資安防護標準，經濟部及國家通訊傳播委員會共同推動資通訊產品資安檢測暨認驗證制度，包括產品資安檢測基準制定、測試實驗室認證、資安檢測服務提供、產品資安驗證及合格標章核發及公告等，並以具市場規模及影響民生較大之產品為優先推動標的，目前已制定影像監控(IP CAM、NVR、DVR)、智慧巴士(車載機與智慧站牌)及智慧路燈(燈控器與照明閘道器)等 IoT 資安標準，其中 IP CAM 資安產業標準現已成為國家標準(CNS 16120)。

2、建構國家資安聯防體系

(1)我國資安聯防體系以八大 CI 領域為核心，由行政院統籌，結合中央目的事業主管機關串連 CI 提供者進行領域資安防護，並銜接國家層級進行橫向跨域聯防，形成「三層式資安聯防架構」，以減緩 CI 受資安攻擊致營運中斷的影響，進而強化整體國家安全，目前已推動建置國內層級及各 CI 領域層級之資訊安全監控中心(Security Operations Center, SOC)、電腦緊急應變小組(Computer Emergency Response Team, CERT)及資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)等聯合防護機制，以系統化及制度化方式，進行資安情資掌握及傳遞、事件通報及應處、情資整合分享與應用等，建構完整的防禦陣線。

(2)有關地方政府部分，藉由強化地方政府及所屬基層公所之資安防護，協助其建構安全資通作業環境，建立可信賴的資通安全環境，且以六都為核心，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。目前已建置 6 個區域 ISAC 且成為「國家資安資訊分享與分析中心」(National Information Sharing and Analysis Center, N-ISAC)會員，使情資可迅速地分享予地方政府，亦完成 6 個區域 SOC，彙整所屬鄰近縣市之資安情資，進行

綜合分析以掌握可疑惡意行為。

3、推升資安產業自主能量

(1)為推動我國資安產業之自主發展，提高國內自主率等事宜，行政院於108年11月28日公布「資通安全自主產品採購原則」，鼓勵中央與地方機關(構)、公立學校、公營事業及行政法人依政府採購法採用資通安全自主產品，進而帶動資通安全產業發展及強化國家資通安全防護能量。另，經濟部為協助我國資安業者提升中長期競爭力，建置資安整合服務平台(SecPaaS)，推動國產資安產品與服務媒合服務，供給方為可提供資安服務的廠商，如安全軟體開發工具商、滲透測試服務供應商、新興資安產品供應商，其產品與服務經審核通過後即可上架。需求方為場域代表或產品整合商，如系統整合服務商、解決方案提供商。透過平台協助媒合需求方場域導入資安產品試煉與實證，以期建推動垂直整合領域資安解決方案。

(2)為加速我國資安產業發展，政府投入資源為我國資安業者創造有利條件及發展環境，使業者於發展初期快速蓄積多方面能量並獲得成長空間。並結合資安新創社群，辦理技術聚會、工作坊，建立產學研界資安趨勢與技術交流環境，串接國內資安研發能量，讓資安技術向下紮根，同時扶植新創公司累計達25家，如白帽駭客社群產業化或帶動大企業進行投資。

4、孕育優質資安人才

(1) 107 年教育部於原有公費留學考試中增設電資學群，設立「資通安全學門」，提供錄取生出國研習，並推動4所大專院校自108年起成立5個資安碩士(學程)班，逐步建置系統性資安人才培育體系。另辦理多元實務培育模式，自 105 年推動「台灣好厲駭」培訓課程，以培育具資安技術實務能力的人才為目標，結合學界與業界教師，推動業師(Mentor)制度，以師徒制方式教授資安實務技術及資安競賽經驗，另針對資安技能表現優異的學生給予更專精深造的機會，於 106 年啟動新型態資安暑期課程(Advanced Information Security Summer School, AIS3)，以培養高素質資安人才為目標，並舉辦 Final CTF 或資安實務應用專題競賽。透過多元實務培育模式，近年來我國資安學員出國參加全球駭客搶旗攻防大賽(DEF CON CTF)等國際資安競賽均名列前茅。

(2) 針對資安產業的人才培育，經濟部自 106 年起開辦資安產業人才養成班，補助每位學員 400 小時全職資安培訓，結訓後由培訓單位提供就業媒合服務；106 年結訓後 3 個月內達 100%媒合，107 年亦達 80%，且成功媒合中有 20%直接投入資安產業。而產業資安人才的推展，採結合市面各資安培訓能量，針對不同產業領域開設資安在職班進行短期培訓，由企業選派學員後由工業局提供補助，即時強化產業內的資安能量。109 年短期資安人才累計開訓 11 班 220 人次、CI 資

安人才累計開訓 6 班 133 人次、長期資安人才訓練課程累計開訓 3 班 69 人次。針對高階資安人才養成，TWISC 中心聯盟向下成立 7 個 TWISC 資安特色中心，累計培育資安碩博士生 792 名，至 109 年第 3 季已發表 289 篇期刊及研討會論文，執行 96 件產學合作，並移轉 15 項資安技術。

三、資安發展問題評析及應對策略

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，爰依據第五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，詳如下圖4，以作為規劃本方案之重要參考。

優勢	劣勢
1、資安為我國重點政策且積極推動 2、施行資通安全管理法與子法、制定產業標準與檢測規範，完備法律基礎與相關制度配套 3、我國 ICT 產業供應鏈與工控電腦產品出口優勢 4、我國資訊相關人才素質佳，高階駭客人才藏富於民	1、資安法規尚難全面擴及，企業及國民資安意識仍待提升 2、國家整體資安聯防機制仍待深廣化 3、國內資安產業規模較小、產值較低 4、欠缺前瞻研究、實戰及關鍵基礎設施等資安人才
機會	**威脅**
1、我國具有全球重要的資安戰略位置 2、網路犯罪偵查及資安防禦機制等已具一定能量，提升國際合作意願 3、政府資通訊環境逐步集中，有助強化防護 4、5G、IoT、AI 及產業創新等資安防護需求日益提升	1、政經情勢特殊，面臨國家級組織駭客威脅 2、新型態資安威脅不斷推陳出新，主動防禦機制仍有不足 3、關鍵基礎設施及供應鏈資安風險日益增加，缺乏公私協同合作機制 4、我國資安業者面臨國際大廠強大競爭壓力

圖 4：現階段資安發展 SWOT 分析

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，詳如下圖 5。進一步依據第五期發展方案 4 項推動策略：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、孕育優質資安菁英人才，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。

SO 進攻策略	WO 轉進策略
1. 建構安全智慧聯網(S1+S2+S3+04) 2. 提升科技偵查能量防制新型網路犯罪(S1+S4+02) 3. 制敵機先阻絕攻擊於邊境(S1+02+03)	1. 賡續推動政府資訊(安)集中共享(W2+03) 2. 擴大國際參與及深化跨國情資分享(W2+02) 3. 擴增高教資安師資員額與教學資源(W4+01+04) 4. 挹注資源投入高等資安科研(W4+01+02+04)
ST 迴避策略	**WT 避險策略**
1. 強化供應鏈安全管理(S2+S3+S4+T3) 2. 建立各領域公私協同治理運作機制(S2+S4+T3) 3. 公私合作深化平時情資交流與應變演練(S2+S4+T2+T3)	1. 輔導企業強化數位轉型之資安防護能量(W1+W2+T1) 2. 培育頂尖資安實戰及跨域人才(W4+T1+T2) 3. 增強人員資安意識與能力建構(W1+T2+T3)

圖 5：TOWS 分析矩陣

肆、發展藍圖

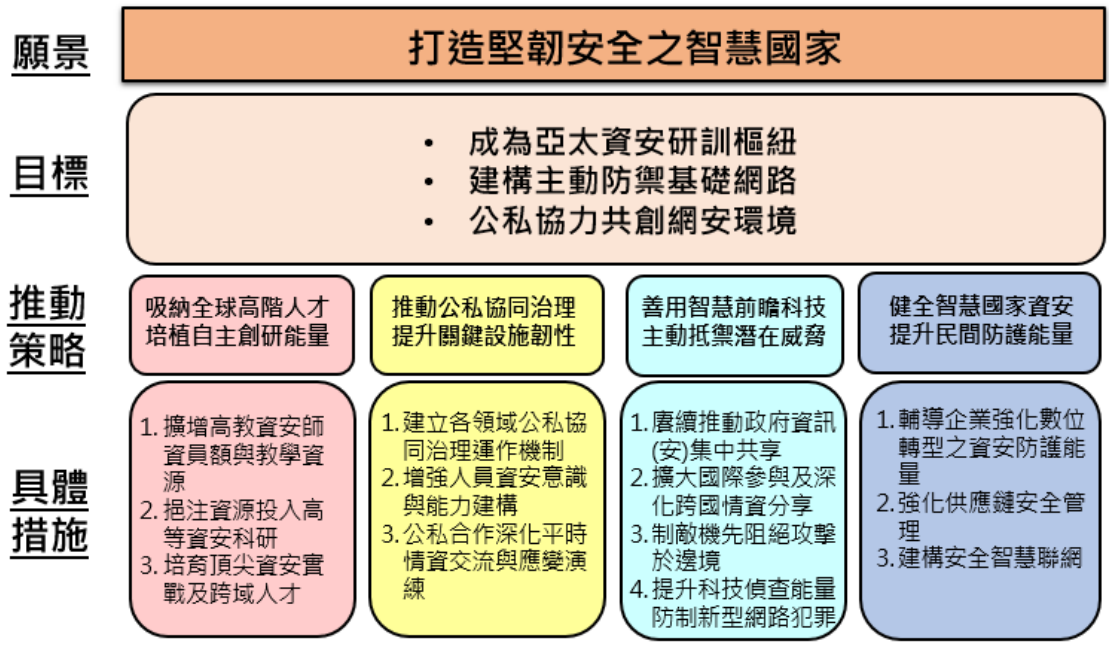

圖 6：第六期資安發展方案架構

一、願景

我國資安政策推動已歷經前五階段之系統性發展，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。

為加速臺灣產業轉型升級，政府打造以「創新、產值、就業」為核心價值，追求永續發展的經濟新模式，並透過「連結未來、連結全球、連結在地」三大策略，激發產業創新風氣與能量。為達成上述標的，於 105 年推動「5+2 產業創新計畫」，作為驅動台灣下世代產業成長的核心，並自 106 年起推動「數位國家・創新經濟發展方案(2017-2025 年)」(DIGI+方案)，以「發展活躍網路社會、推進高值創新經濟、開拓富裕數位國

土」為發展願景作為引領數位發展、帶動創新的施政藍圖，期加速我國產業及生活融入人工智慧、IoT、大數據等智慧科技。

為發展活躍網路社會、推進高值創新經濟、建構豐饒數位國家，本方案將做為前述 2 項現階段主要數位經濟計畫之穩固基石，並搭配六大核心戰略產業之資安卓越產業發展方案所定之推動策略，在穩健資通安全之環境下，大幅茁壯各項數位經濟之脈動，爰以「**打造堅韌安全之智慧國家**」為願景，期打造安心社會與智慧生活。

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。我國政府亦因政經情勢特殊，面臨更加嚴峻的挑戰，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，爰本方案第一項目標設定為「成為亞太資安研訓樞紐」，將籌備資安卓越中心，從資安前瞻研究、頂尖實戰人才養成、實習場域建置、國際合作及技術移轉創新育成等 5 個面向著手，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量。

「建構主動防禦基礎網路」為本方案第二項目標，改變以往僅能於資安事件發生後採取被動防禦，化被動為主動之防守，調整防護機制並精進應變措施，將溯源、偵查、預警及反制等作為導入防護策略，用以因應多元複雜的惡意攻擊。近年國際各國已陸續採取此方式，本方案亦將透過國家任務導向型研究相關應用技術，同時完善政府網際服務網

(Government Service Network, GSN)資安防護，分析情資並轉換為有效情報，進而提升科技偵查能量以防制新型網路犯罪。

最後一項目標為「公私協力共創網安環境」，則是持續結合產、官、學、研各界資源與能量，將資安防護能量擴及至民間單位；另因近年發現多起資安事件肇因於惡意攻擊者駭侵資訊服務供應商後，進一步透過遠端連線等方式入侵政府機關，使得承包政府標案之供應鏈廠商成為資安破口，可見落實政府資訊作業委外安全管理愈趨重要。另，5G 網路及 IoT 設備等與國人生活息息相關，本方案除推動晶片安全以提升設備核心安全外，亦藉由健全新世代行動通訊技術網路安全及推動 IoT 合規驗證及場域實證，讓國人體驗新科技帶來之便利，同時享有安全保障，共同維護智慧聯網安全環境。

三、推動策略

為培育我國卓越資安人才，精進CI 防護作為，利用前瞻科技主動防制威脅並溯源阻斷，透由公私協同合作將資安意識與量能普及於民間企業，並健全智慧國家資安，本方案擬具四項推動策略，分別從「吸納全球高階人才、培植自主創研能量」、「推動公私協同治理、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「健全智慧國家資安、提升民間防護能量」等四個面向著手，並配合六大核心戰略產業之「資安卓越產業」規劃持續推動資安產業，期以打造安全堅韌之智慧國家。

（一）吸納全球高階人才、培植自主創研能量

為因應國家發展之資安人力需求，於第五期發展方案期間，各權責機關(單位)推動相關計畫挹注資源布建資安培育環境，強調以實務與產學鏈結為導向之創新培育模式，結合國內大學校院資安教學能量，建立以需求為導向之資安人才培訓體系為目標，孕育優質資安人才，提供我國各產業所用，已建立培訓能量。

現我國正值推動 DIGI+方案及 5+2 產業創新計畫，並以其為基磐打造六大核心戰略產業，帶動產業數位升級，資安儼然已為最重要之基底，亟須培育充沛資安人才及前瞻研究，本策略爰規劃成立資安卓越中心，從技術面及人才面為我國未來資安需求扎根，目標成為亞洲地區代表性高階人才及技術創新基地。

1. 擴增高教資安師資員額與教學資源

1.1 專案增加師資員額

邀請國內外一流資安競賽團隊、業師、學界和社群知名人士，並提供優渥薪資待遇，以延攬頂尖高階研究人員擔任資安師資，鼓勵大專校院與國內外產業及學研機構競逐優秀資安人才，以利學校培育資安專業人才並維持教學品質。

1.2 開放學術區域網路中心、政府網路等場域供實習、實戰用

(1) 透過大學區網中心與大學資安實驗室，提供「教學實驗主題」與「實習場域(實體/虛擬)模式」

及「結合大學資安系所教研課程」三面向，將區網或實驗室網路擬真情境,融入教學實習並進行研析或攻防演練，養成資安實務人才。

(2) 規劃政府 GSN 骨幹網路作為開放資料場域,拓展資安教學實習場域，完善資安教學設備環境。

2. 挹注資源投入高等資安科研

2.1 發展國家任務導向型及關鍵(核心)資安型前瞻研究

因應資安新興威脅及趨勢發展，由資安卓越中心延聘國際優秀人才，負責政府機關短中長期所需之應用技術以培育並厚植我國資安前瞻研究自主能量。其中國家任務導向型研究，以提供政府機關短中期所需之應用技術研究為主，包括技術面及政策面議題;而關鍵核心研究屬長期性基礎型研究,以發展國防、國安之關鍵技術及研究為主。

2.2 深耕學術型資安研究

精進研發軟、硬體相關資安技術,以切合國家與民間產業之資安技術需求,提升產官學研發能量,活絡資安研究生態系統。

2.3 跨國人才交流與研究合作

(1) 參與國際資安合作交流，確保開發技術與國際接軌、辦理大型國際學術會議發表研究成果等，藉由國際合作，提升我國國際能見度。

(2) 培育具有國際視野與研發技術之高階人才為目標，並積極推動科技外交，經營跨國人才培育的合作夥伴關係。

3. 培育頂尖資安實戰及跨域人才

3.1 培育在學、在職及政府資安人才

(1) 在學：建構以需求為導向的設計課程內容與模組，優化資安實務教學資源，培養跨域資安人才與強化資安認知教育，養成資安實務人才。

(2) 在職：針對主軸產業推動產業資安教學及實作課程，發展資安專業訓練及實務應用之人才，加速產業提升資安人才能量。

(3) 政府：推動資安職能訓練藍圖，分策略、管理及技術 3 個面向，規劃 6 個資安職能訓練構面，提升機關資安管理與技術能力，培訓政府機關專職人力。

3.2 培育實戰型之頂尖資安人才

初期培訓對象聚焦我國具資安潛力菁英，擇優挑選產學政軍之人才進行培訓，施予訓練計畫。並針對不同類型資安人才，規劃不同評核機制(如取得相關證照或通過考試等)，完訓之頂尖人才獲得較優渥之就業機會，並可協助政府及關鍵資訊基礎設施(CII)資安防護，做為國家緊急需調用人力之後盾，長期招收對象將擴及亞太地區，並以成為亞太資安頂尖人才培育基地為目標。

（二）推動公私協同治理、提升關鍵設施韌性

第五期發展方案已建立8大CI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(SOC)，有助政府管理與傳遞全國跨領域資安情資，協助國內在應對資安事件時的緊急處理能力，並全時掌握資安聯防監控情形。

為精進CI之資安防護能量及應對能力，以提升其防護韌性(Resilience)，本策略將持續推動及落實各領域之資安防護基準，並輔以攻防演練及稽核檢視其執行成效，同時建構各該領域資安職能學習藍圖以提升CI一線人員之資安素質。

1. 建立各領域公私協同治理運作機制

1.1 賡續推動落實資通安全管理法，並適時檢討以因應國際資安防護趨勢

因應實務執行及推動需求，進行相關法規調適，並持續精進及擴大推動資安治理成熟度評估，以加速建構我國資通安全環境。

1.2 推動落實關鍵基礎設施資安防護基準

訂定並滾動修正CI領域資安防護基準並導入資安責任等級B級以上之CI提供者。且透過資安稽核以瞭解CI提供者資安法遵事項(如維護計畫、應辦事項及資安防護基準)落實情形，強化資安防護工作之完整性及有效性。

1.3 建構工控領域資安治理成熟度

工業控制系統係針對各類工業過程提供管理及控制，

廣泛應用於石油、水資源、天然氣、電網等 CI 領域。為能有效衡量工控系統之資通安全防護程度，將建立工控領域之資安治理評估模式，以掌握 CI 提供者資安執行情形，提升其資安防護整備度。

1.4 推動國家層級資安風險評估

識別各 CI 領域核心資通系統及其資安威脅，有效掌控我國整體資安風險威脅。

2. 增強人員資安意識與能力建構

2.1 設置資安長並強化人員資安專業能力

(1) 推動 CI 提供者設置高階資安長統籌資安政策推動協調與資源調度，帶動 CI 重視資安的組織文化。

(2) 建置 CI 各領域資安專家資料庫(如退休人員或廠商)，辦理 CI 提供者外部資安稽核或演練之用。

(3) 發展 CI 各領域資安職能學習地圖，逐年開發相關課程，並培訓一定數量之人員。

2.2 建立模擬場域，作為實證應處能力及納入資安情境進行教學訓練

建置國家型 CI 模擬場域，提供國內 CI 領域所需資安防護解決方案之實證場域，並支援教育訓練、大型攻防演練及國際資安攻防競賽。

3. 公私合作深化平時情資交流與應變演練

3.1 精進關鍵基礎設施資安聯防機制(情資分享、通報

應變、資安監控）

(1) 持續提升政府領域資安監控之完整性及有效性。

(2) 訂定符合國際最新標準之通報單交換格式，將資安事件資訊快速轉化應用分享，縮短通報應變處理與情資整合時效。

(3) 各 CI 領域主管機關持續精進資安聯防運作，並提升其質化及量化效益。

3.2 定期於場域進行公私聯合攻防演練

各 CI 領域主管機關定期實施攻防演練，以提高人員對於資安攻擊事件熟悉度及警覺性，加速事件的應變處理時間並減少損失。

3.3 辦理關鍵基礎設施跨領域(或跨國)攻防演練

定期辦理跨 CI 領域或跨國之攻防演練，以驗證資安防護之有效性，並強化 CI 資安防護韌性。

（三）善用智慧前瞻科技、主動抵禦潛在威脅

鑒於攻擊手法日益精進，傳統防禦已不敷使用，透過情資轉換為有效情報，預測攻擊方式備妥準備，甚至追溯攻擊來源並阻斷等積極防禦手段，以作為我國未來推動重點。本策略以網路攻擊狙殺鏈(Cyber Kill Chain)提出之 7 個攻擊階段：偵查、武裝、遞送、攻擊、安裝、命令與控制、採取行動，制定各個階段之防禦作為。

於偵查階段，透過事先建立資通系統弱點之主動發掘、通報及修補機制，並推動政府大內網及資安防護向上集中，以降低資安風險；於武裝階段，提升威脅情蒐與主動偵測能

量，並與國際合作增加情蒐深廣度，預測攻擊模式以超前部署；於遞送、攻擊、安裝、發令與控制等階段，藉由發展主動式防禦技術，建立零信任架構資安防護驗證環境，完善網路防禦縱深；最後於採取行動階段，則透過強化網路犯罪偵防能量、提升溯源追蹤能力，並加強跨境網路犯罪偵查以達嚇阻作用。

1. 賡續推動政府資訊(安)集中共享

1.1 連結國家防衛自主需求，發展國內資安產業生態系

(1) 提供具備內對內、內對外及跨機關網路導流作業，以強化 GSN 內部資通安全性。

(2) 配合資訊資源向上集中，推動政府機關網路出口集中至上級機關。

(3) 強化政府大內網之主動防禦能量，及時阻擋惡意攻擊。

1.2 建立資通系統弱點之主動發掘、通報及修補機制

透過自動化之通報機制，縮短機關資安漏洞發布及修補間的空窗期，降低系統被駭侵之風險。

2. 擴大國際參與及深化跨國情資分享

2.1 發展主動式防禦前瞻研究及技術應用

研發自動化智慧協作與應變資安模組，並結合 AI 技術，提高快速檢測和響應網路攻擊的能力，建構資安研發生態圈。

2.2 整合國內外情資來源，並深化國際合作

發展 N-ISAC 成為國內主要情資彙整平臺，整合國內

外情資來源，提升威脅情蒐與主動偵測能量，並推動標準情資交換格式，以介接國際。

3. 制敵機先阻絕攻擊於邊境

3.1 應用新興技術淬鍊有效情報，發展主動式防禦技術

以主動式防禦思維，透過情蒐研析、縱深防禦、主動防制及溯源阻斷等重點工作面向，強化相關技術研發與應用，以提升政府機關資安防護能力。

3.2 完善政府網際服務網防禦深廣度

(1) 評估並導入零信任網路(Zero Trust Network)，並逐步試行以驗證其可行性。

(2) 提升 GSN 資安威脅分析能量，掌握主動防禦情資與整體威脅攻擊概況。

(3) 強化外網惡意入侵偵測及區域聯防，並提升網域名稱系統(Domain Name System, DNS)抵禦攻擊之抗性，以確保 DNS 資料之「機密性」與「完整性」，及 DNS 持續「可用性」。

4. 提升科技偵查能量防制新型網路犯罪

4.1 強化新型網路犯罪偵查能量

分析 IoT 及中繼站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，並建置資安事件調查模擬平臺，以強化整體偵查實戰能量。

4.2 提升資安事件溯源追蹤能力

持續拓展資安鑑識能量，自主研發現場取證工具，並強化情資分享及技術交流，分析比對策動攻擊之來

源與駭客組織，以達溯源目的。

4.3 加強跨境網路犯罪偵查機制

(1) 積極參與各項司法機關及國際資安研討會，建立與國外企業調閱相關犯罪資料窗口，增進跨境網路犯罪偵查管道及技術，並促進國際情資交換。

(2) 善用資訊科技研發自主應用系統，機先發掘境內潛藏之惡意威脅端點。

（四）建全智慧國家資安、提升民間防護能量

近期發現惡意攻擊者改採迂迴攻擊模式，先入侵政府機關之委外資訊服務供應商，再間接駭侵政府機關，因此除持續強化我國政府機關資安防護能量外，委外資訊服務供應商亦為重要環節，爰將強化委外供應鏈風險管理納為推動重點工作。

面對 5G 網路時代，各類資通訊相關設備安全性益顯重要，除協助我國電信業者聚焦 5G 資安風險議題，提出對應解決方案，同時亦須關注隨著新世代網路發展之各項 IoT 設備及服務，制訂相關合規驗證及場域實證，加速 IoT 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，期以輸出國際市場。

1. 輔導企業強化數位轉型之資安防護能量

1.1 結合民間資源，建立公私協同合作機制，協助企業提升資安防護能量

(1) 優化 TWCERT/CC 資安情資系統及服務，深化我國企業資安事件諮詢及協處服務，擴大資訊安全宣

導，提升民間資安防護能量及意識。

(2) 提升網路零售業者之資安素養及資安防護能量，並降低個資外洩之風險。

1.2 提升民眾資安意識

政府應與民間共同提升全民資通安全意識，將資安意識融入國人生活，內化為服務使用的基本需求，以利先進資通安全技術、軟硬體、專業人才等之發展。

2. 強化供應鏈安全管理

2.1 強化委外供應鏈風險管理

協助及輔導各機關辦理委外作業時，包含資通系統之建置、維運或資通服務，加強對委外廠商之資安管理。

2.2 聚焦資通訊晶片產品安全性

(1) 研發晶片資安檢測工具，解決晶片潛藏資安風險問題。

(2) 成立國際認可晶片資安檢測實驗室，補強國內晶片檢測技術缺口與檢測環境生態系，減少國內產品外銷的資安合規障礙。

3. 建構安全智慧聯網

3.1 健全新世代行動通訊技術網路安全

(1) 持續完備 5G 資安監理法規及作為，並藉由建置 5G 資安檢測實驗室，驗證法規可行性及協助業者完備 5G 網路資安防護。

(2) 成立國家級通訊資通安全實驗室，並研擬資通安

全防護參考框架與指引文件，以提升我國 5G 網路之安全。

(3) 建構 5G 垂直應用發展環境、推動整合協調促成各方合作、調適法規促進 5G 垂直應用之發展。

3.2 推動物聯網合規驗證及場域實證

(1) 制定我國物聯網資安檢測驗證框架，並擬訂物聯網資安檢測優先策略及清單項目。

(2) 建置產品淬煉場域，推動供需媒合機制，強化資安服務鏈價值整合。

(3) 協助國內法人及資通訊廠商參與資安相關國際標準制定，並與國際標準相關機構辦理資訊交流，促進我國資安技術與國際接軌。

(4) 推廣 IoT 設備資安檢測，提升製造商及使用者資通安全防護意識，促進數位創新應用發展。

四、機關(單位)分工

表 2：機關(單位)分工表

工作項目	主(協)辦機關(單位)
策略一：吸納全球高階人才，培植自主創研能量	
1、擴增高教資安師資員額與教學資源	
1-1 專案增加師資員額	教育部
1-2 開放學術區域網路中心、政府網路等場域供實習、實戰用	教育部、數位發展部資通安全署、(數位發展部)
2、挹注資源投入高等資安科研	
2-1 發展國家任務導向型及關鍵(核心)資安型前瞻研究	數位發展部資通安全署、數位發展部
2-2 深耕學術型資安研究	國家科學及技術委員會

工作項目	主(協)辦機關(單位)
2-3 跨國人才交流與研究合作	數位發展部資通安全署、國家科學及技術委員會
3、培育頂尖資安實戰及跨域人才	
3-1 培育在學、在職及政府資安人才	教育部、數位發展部數位產業署、數位發展部資通安全署
3-2 培育實戰型之頂尖資安人才	數位發展部資通安全署、數位發展部
策略二：推動公私協同治理，提升關鍵設施韌性	
1、建立各領域公私協同治理運作機制	
1-1 賡續推動落實資通安全管理法，並適時檢討以因應國際資安防護趨勢	數位發展部資通安全署、(各機關)
1-2 推動落實關鍵基礎設施資安防護基準	各 CI 主管機關
1-3 建構工控領域資安治理成熟度	數位發展部資通安全署、(各 CI 主管機關)
1-4 推動國家層級資安風險評估	數位發展部資通安全署、(各 CI 主管機關)
2、增強人員資安意識與能力建構	
2-1 設置資安長並強化人員資安專業能力	各 CI 主管機關
2-2 建立模擬場域，作為實證應處能力及納入資安情境進行教學訓練	數位發展部資通安全署、數位發展部、(各 CI 主管機關)
3、公私合作深化平時情資交流與應變演練	
3-1 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)	數位發展部資通安全署、各 CI 主管機關
3-2 定期於場域進行公私聯合攻防演練	各 CI 主管機關
3-3 辦理關鍵基礎設施跨領域(或跨國)攻防演練	數位發展部資通安全署、(各 CI 主管機關)
策略三：善用智慧前瞻科技，主動抵禦潛在威脅	
1、賡續推動政府資訊(安)集中共享	
1-1 推動政府大內網及資安防護向上集中	數位發展部、數位發展部資通安全署、(各機關)
1-2 建立資通系統弱點之主動發掘、通報及修補機制	數位發展部資通安全署、(各機關)
2、擴大國際參與及深化跨國情資分享	
2-1 發展主動式防禦前瞻研究及技術應用	數位發展部數位產業署
2-2 整合國內外情資來源，並深化國際合作	數位發展部資通安全署、(各 CI 主管機關)

工作項目	主(協)辦機關(單位)
3、制敵機先阻絕攻擊於邊境	
3-1 應用新興技術淬鍊有效情報，發展主動式防禦技術	數位發展部資通安全署
3-2 完善政府網際服務網防禦深廣度	數位發展部資通安全署、數位發展部
4、提升科技偵查能量防制新型網路犯罪	
4-1 強化新型網路犯罪偵查能量	內政部、法務部
4-2 提升資安事件溯源追蹤能力	內政部、法務部、(數位發展部資通安全署)
4-3 加強跨境網路犯罪偵查機制	內政部、法務部
策略四：健全智慧國家資安，提升民間防護能量	
1、輔導企業強化數位轉型之資安防護能量	
1-1 結合民間資源，建立公私協同合作機制，協助企業提升資安防護能量	數位發展部、(數位發展部數位產業署)
1-2 提升民眾資安意識	數位發展部
2、強化供應鏈安全管理	
2-1 強化委外供應鏈風險管理	數位發展部資通安全署
2-2 聚焦資通訊晶片產品安全性	數位發展部數位產業署
3、建構安全智慧聯網	
3-1 健全新世代行動通訊技術網路安全	數位發展部
3-2 推動物聯網合規驗證及場域實證	數位發展部數位產業署、經濟部、(數位發展部)

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

五、重要績效指標

本方案依據願景、目標及推動策略，訂定 3 項重要績效指標，分述如下：

(一)培育 350 名資安實戰人才

為因應國家發展之資安人力需求，數位發展部資通安全署近年與教育部、國家科學及技術委員會、數位發展部數位產業署等機關(單位)共同推動辦理資安專業人才厚植作業，

挹注資源以布建資安培育環境，結合國內大學校院資安教學能量，建立以需求為導向之資安人才培訓體系。目前，校園方面已推動資安碩士(學程)班；產業方面，推動產業資安教學及實作課程，發展資安專業訓練及實務應用之人才；國家方面，我國學研機構針對資安前瞻研究部分已完成諸多學術研究，逐步建置系統性資安人才培育及前瞻研究制度。

本方案將持續提升國內高階資安人才人數，並建立國家級前瞻研究中心，從技術面及人才面為台灣未來之資安需求扎根，目標成為亞洲地區代表性高階人才及技術創新基地，邀請國外資安學界、業界和社群知名人士培訓國內及國際實戰人才至少 350 人次，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量。

(二)推動政府機關資安治理成熟度(含客觀指標)達第 3 級

為衡量我國政府機關之防禦能力及治理成效，於第五期發展方案積極推動政府機關資安治理成熟度，並於資通安全管理法子法「資通安全責任等級分級辦法」之管理面應辦事項，明定資通安全責任等級 A 級與 B 級之公務機關，每年應辦理 1 次資安治理成熟度評估作業。

現有資安治理成熟度評估方式係於資安治理之「策略面」、「管理面」及「技術面」三大面向設計對應之檢核項目，包含政策與組織管理有效性、績效與成果監督落實性、資安事件管理與緊急應變有效性等指標問項，將評估後之能力度等級由低至高分為 6 級，分別為「Level 0 未執行流程(Incomplete Process)」、「Level 1 已執行流程 (Performed Process)」、

「Level 2 已管理流程（Managed Process)」、「Level 3 標準化流程（Established Process)」、「Level 4 可預測流程（PredictableProcess）」及「Level 5 最佳化流程(Optimizing Process)」，統計至 109 年底，A 級機關成熟度等級平均值為 2.56。

為精進既有資訊科技領域(Information Technology)之資安治理成熟度，後續將加入客觀指標，例如蒐集監控數據、攻防演練成效等資訊，分析其防護等級真實性；另，同步訂定 OT 資安治理成熟度評估機制相關標準文件，並試行導入至 CI 提供者。藉由上述資安治理成熟度衡量機制，於 113 年時，所有 A 級政府機關達資安治理成熟度(含客觀指標)第 3 級以上，期望我國資安防禦作為能達超前部署、制敵機先及溯源追蹤。

(三)制定 12 項資安檢測技術指引或產業標準

隨著 4G 及 5G 通訊蓬勃發展，IoT 設備應用亦趨廣泛，為提升我國資通訊產品資安防護能量，經濟部與通傳會相互合作制訂 IoT 設備資安測試標準，自 106 年起，已陸續制定影像監控(IP CAM、NVR、DVR)、智慧巴士(車載機與智慧站牌)及智慧路燈(燈控器與照明閘道器)、無線接取點(Access Point, AP)、無線路由器、MOD(Multimedia on Demand)機上盒、有線電視機上盒、智慧音箱等資安標準、技術指引或草案，另亦建立各類型產品資安檢測實驗室，在各界共同努力下已陸續見證成果，特別是影像監控資安產業標準已於 108 年成為我國國家標準(CNS 16120)。

鑒於 IoT 設備多元發展，現階段採取逐步制定單一品項之資安檢測標準方式恐跟不上產品推陳出新的速度，因此需有整體策略及推動規劃；爰此，本方案將參考美國 NIST 及歐盟 ENISA 所提出之產品認證架構，據以制定我國 IoT 資安檢測框架，預期 4 年累計制定 IoT 資安檢測技術指引或產業標準達 12 項，期使 IoT 設備資安檢測生態鏈可永續維持，提供國人安全可信賴的數位基礎環境。

表 3：分年里程碑

重要績效指標	110 年	111 年	112 年	113 年
培育 350 名資安實戰人才	培育 50 名資安實戰人才	培育 50 名資安實戰人才	培育 125 名資安實戰人才	培育 125 名資安實戰人才
推動政府機關資安治理成熟度(含客觀指標)達第 3 級	建立政府機關資安治理成熟度客觀指標	推動 3 個 A 級政府機關落實資安治理成熟度(含客觀指標)達第 2 級以上	推動 30 個 A 級政府機關落實資安治理成熟度(含客觀指標)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(含客觀指標)達第 3 級以上
制定12項資安檢測技術指引或產業標準	完成 3 項資安檢測技術指引或產業標準	完成 3 項資安檢測技術指引或產業標準	完成 3 項資安檢測技術指引或產業標準	完成 3 項資安檢測技術指引或產業標準

伍、 預期效益

一、為發展數位應用資安生態系，完備 DIGI+及 5+2 產業創新方案資安能量,將以「成為亞太高階資安人才及技術創新基地」為願景，從技術面及人才面為台灣未來資安需求扎根，挹注充足教學及研究資源，以厚植我國頂尖實戰人才培訓及資安前瞻研究能量。

二、面對日益嚴峻的資安威脅環境，將建構主動式防禦機制，於攻擊前透過強化資訊資產弱點管理，並藉由網路及資安防護向上集中，以降低資安風險，達超前部署之效；於攻擊發生時,藉由發展主動式防禦技術,以及深化國內情資綜整平臺，期阻絕攻擊於邊境，達制敵機先之效；最後於攻擊後，持續提升司法單位科技偵查能量，以防制新型網路犯罪，達溯源追蹤之效。再利用資安治理成熟度衡量機制(含客觀指標)，將政府機關之主動防禦能量採量化指標呈現，後續可依衡量結果作為擬訂改善策略之參考,協助機關完善資安基礎環境。

三、近年國內外均積極推動智慧城市/智慧國家，而搭建起智慧生活之基礎設施則是由多元 IoT 設備與敏捷網路交織而成，因此安全的 IoT 設備極為關鍵，未來擬訂之 IoT 資安檢測技術指引或產業標準，不僅依循國際標準與國際同步，亦可使民間企業製造之設備取得競爭力，最終消費者更可取得安全產品成為最大受益者，永續發展 IoT 生態鏈。

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」，數位發展部資通安全署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

各主辦機關(單位)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，由數位發展部資通安全署運用既有督導機制，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	主(協)辦部會	分年重要進程(量化目標)
策略一：吸納全球高階人才，培植自主創研能量		
1、擴增高教資安師資員額與教學資源		
1-1 專案增加師資員額	教育部	110 至 113 年每年聘任 20 名資安師資，其中由教育部核撥 15 名，另由學校自行提撥 5 名，4 年累計聘任 80 名資安教師
1-2 開放學術區域網路中心、政府網路等場域供實習、實戰用	教育部、數位發展部資通安全署、(數位發展部)	1、110 年建置 2 所區網中心為資安教學實習場域，使用學員達 30 人次；規劃政府 GSN 骨幹網路作為開放研訓場域 2、111 年使用資安教學實習場域與教材達 300 人次；建立政府開放場域營運制度 3、112 年建置政府開放場域威脅情資分析索引系統 4、113 年建置政府開放場域可模擬機關網路環境與應用系統之實驗場域
2、挹注資源投入高等資安科研		
2-1 發展國家任務導向型及關鍵(核心)資安型前瞻研究	數位發展部資通安全署、數位發展	1、110 年規劃並設立資安卓越中心，並延攬國外高階研究人才，建立頂尖研究團隊 2、111 至 113 年持續延攬國外高階研究人才，擴大頂尖研究團隊規模
2-2 深耕學術型資安研究	國家科學及技術委員會	每年開發 10 項資安技術/機制

工作項目	主(協)辦部會	分年重要進程(量化目標)
2-3 跨國人才交流與研究合作	數位發展部資通安全署、國家科學及技術委員會	1、 每年對接 1 家國外技術或研究機構 2、 每年跨國人才交流達 15 人次，科技外交或研究交流達 2 次 3、 112 年起每年參與國際組織進行資安合作交流 4、 112 年辦理 1 場大型國際學術會議
3、培育頂尖資安實戰及跨域人才		
3-1 培育在學、在職及政府資安人才	教育部、數位發展部數位產業署、數位發展部資通安全署	1、連結產業實務場域，每年至少發展 1 門跨域資安實務課程，養成資安實務人才達 1,000 人次 2、發展產業資安教學及實作環境，每年針對 2 項主軸產業培養具備相關資安專業訓練及應用之人才，加速產業提升資安人才能量 3、110 年至 112 每年完成 2 個資安職能訓練構面課程開發，並擴大推動調訓機制，110 至 113 年累計培訓政府機關專職人力 200 人次以上
3-2 培育實戰型之頂尖資安人才	數位發展部資通安全署、數位發展部	1、110 年建立國外頂尖資安實戰課程引進機制，並邀請國內資安國際競賽得獎團隊培訓國內實戰人才至少 50 人次 2、111 年引進國外頂尖資安實戰課程，並邀請國外資安學界、業界和社群知名人士培訓國內實戰人才至少 50 人次 3、112 年建立自主頂尖資安實戰課程，並邀請國外資安學界、業界和社群知名人士培訓國內實戰人才至少 125 人次 4、113 年完成自主頂尖資安實戰課程國際化，開始對國際招生，並邀請國外資安學界、業界和社群知名人士培訓國內及國際實戰人才至少 125 人次
策略二：推動公私協同治理，提升關鍵設施韌性		
1、建立各領域公私協同治理運作機制		
1-1 賡續推動落實資通安全管理法，並適時檢討以因應	數位發展部資通安全署、(各機關)	1、滾動檢討修正資通安全管理法及子法，並分別於 110 年及 113 年完成修法作業 2、資通安全管理法納管機關之資通安全維護計畫實施情形提報及稽核 3、精進政府機關資安治理成熟度客觀指標，113 年成熟度達成下列目標： (1) 政府機關：所有 A 級達第 3 級以上，80%之 B 級達第 3 級以上

工作項目	主(協)辦部會	分年重要進程(量化目標)
國際資安防護趨勢		(2) CI 提供者：所有 A 級達第 3 級以上，50%之 B 級達第 3 級以上(部分 CI 領域可視實際情況調整推動數量)
1-2 推動落實關鍵基礎設施資安防護基準	各 CI 主管機關	1、訂定並推動 CI 提供者導入 CI 領域資安防護基準 2、所有 CI 主管機關稽核 CI 提供者之總數，每年累計至少 20 個
1-3 建構工控領域資安治理成熟度	數位發展部資通安全署、(各 CI 主管機關)	1、 110 年訂定工控領域資安治理成熟度評估機制相關標準文件，並擇 2 個 A 級 CI 提供者完成自評作業 2、 111 年推動 5 個 A 級 CI 提供者工控資安治理成熟度達第 2 級以上 3、 112 年推動所有 A 級 CI 提供者工控資安治理成熟度達第 2 級以上(部分 CI 領域可視實際情況調整推動數量) 4、 113 年推動所有 A 級 CI 提供者工控資安治理成熟度達第 3 級以上(部分 CI 領域可視實際情況調整推動數量)
1-4 推動國家層級資安風險評估	數位發展部資通安全署、(各 CI 主管機關)	1、 110 年訂定國家層級資安風險評估機制相關標準文件，推動各 CI 領域導入國家層級資安風險評估機制 2、 111 年推動各 CI 領域擇 3 個 A 或 B 級以上 CI 提供者，導入國家層級資安風險評估機制 3、 112 年推動各 CI 領域擇 6 個 A 或 B 級以上 CI 提供者，導入國家層級資安風險評估機制 4、 113 年彙整各 CI 領域評估結果，完成我國資安風險地圖
2、增強人員資安意識與能力建構		
2-1 設置資安長並強化人員資安專業能力	各 CI 主管機關	1、 110 年各 CI 提供者設置資安長，建置領域資安專家資料庫，並完成規劃各領域資安職能培育藍圖 2、 逐年開發相關課程，並培訓一定數量之人員
2-2 建立模擬場域，作為實證應處能力及	數位發展部資通安全署、數位發	1、 110 年建置 1 個 CI 場域，培訓學員達 20 人次 2、 111 年持續建置 CI 場域累計達 2 個，並設置攻防實戰教室，培訓學員達 20 人次 3、 112 年持續建置 CI 場域累計達 3 個，並設置攻防技術研發實驗室，培訓學員達 20 人次

工作項目	主(協)辦部會	分年重要進程(量化目標)
納入資安情境進行教學訓練	展部、(各 CI 主管機關)	4、 113 年持續建置 CI 場域累計達 4 個，並設置攻防技術檢測實驗室，培訓學員達 20 人次
3、公私合作深化平時情資交流與應變演練		
3-1 精進關鍵基礎設施資安聯防機制(情資分享、通報應變、資安監控)	數位發展部資通安全署、各 CI 主管機關	1、110 年推動政府領域資安監控有效性評估，並納入資安服務廠商評鑑，提升政府領域監控成效；另依國際最新情資交換格式，完成國內資安事件通報單交換格式 2、111 年起推動各 CI 領域自動化通報系統導入新通報單交換格式 3、各 CI 主管機關持續提升領域層級 ISAC、 CERT、 SOC 之會員數量及精進情資分享/事件聯防/事件關聯之機制，提升其質化及量化效益，並強化橫向分享交流
3-2 定期於場域進行公私聯合攻防演練	各 CI 主管機關	各 CI 主管機關每年至少遴選 1 個 CI 提供者辦理攻防演練
3-3 辦理關鍵基礎設施跨領域(或跨國)攻防演練	數位發展部資通安全署、(各 CI 主管機關)	每 2 年辦理 1 次跨領域(或跨國)CI 攻防演練
策略三：善用智慧前瞻科技，主動抵禦潛在威脅		
1、賡續推動政府資訊(安)集中共享		
1-1 推動政府大內網及資安防護向上集中	數位發展部、數位發展部資通安全署、(各機關)	1、110 年提供至少 6 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，完成 80%網路集中出口；完成惡意郵件與網路威脅誘捕向上集中偵蒐機制規劃，並選定 2 個機關試行導入 2、111 年提供至少 10 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，完成 90%網路集中出口；推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制 3、112 年提供至少 15 個 GSN 網路節點具備 SDN 網路架構，以得設置資料中心之機關為單位，維持 90%網路集中出口；持續推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制

工作項目	主(協)辦部會	分年重要進程(量化目標)
		4、113 年依既有網路集中出口機關比例，並提供全 GSN 機房具備 SDN 網路架構；持續推動 2 個機關導入惡意郵件與網路威脅誘捕向上集中偵蒐機制
1-2 建立資通系統弱點之主動發掘、通報及修補機制	數位發展部資通安全署、(各機關)	1、 110 年 A 級公務機關完成導入資安弱點通報機制 2、 111 年 B 級公務機關及 A、B 級 CI 提供者完成導入資安弱點通報機制 3、 112 年 C 級公務機關及 CI 提供者完成導入資安弱點通報機制
2、擴大國際參與及深化跨國情資分享		
2-1 發展主動式防禦前瞻研究及技術應用	數位發展部數位產業署	1、110 年完成自動開源情資蒐集分析技術，建置異質來源威脅特徵情資之知識圖譜 1 式；整合情資分析技術，建立可行動型情資萃取雛形系統 1 式 2、111 年發展威脅特徵情資之知識圖譜生成技術 1 式；完成可支援 2 種以上國際資安領域標準合規檢測模組 1 式 3、112 年推動知識圖譜生成技術導入至少 1 個場域建立示範應用；發展異質場域智慧聯防技術，並支援至少 2 家重點領域廠商，建立主動式防禦資安解決方案 4、113 年研發技術扶植自主研發產品，帶動國內資安/系統整合廠商，支援至少 3 個重點領域(政府、醫療、金融等)，實現資安協作自動化應變技術解決方案(Security Orchestration, Automation and Response, SOAR)；建立 1 套 AI Security 協作產業標準
2-2 整合國內外情資來源，並深化國際合作	數位發展部資通安全署、(各 CI 主管機關)	1、110 年完成國際情資交換格式 STIX2.1 與 MITRE ATT&CK 框架導入規劃；擴展 2 項國內共通性資安情資 2、111 年推動國際情資交換格式 STIX2.1 與 MITRE ATT&CK 框架，並協助國內各領域 ISAC 完成系統與資料轉換；持續擴展並深化情資內容，收容亞太區共通性資安情資 3、112 年規劃開放情資分享，提供學研單位或國際資安組織參考；強化國際情蒐合作，增加全球共通性資安情資 4、113 年比對分析國內外資安情資與威脅，並提供 2 種以上開放情資；分享威脅偵測與分析情資，產製事前重點防護指標，強化 N-ISAC 主動防禦與聯防機制

工作項目	主(協)辦部會	分年重要進程(量化目標)
3、制敵機先阻絕攻擊於邊境		
3-1 應用新興技術淬鍊有效情報，發展主動式防禦技術	數位發展部資通安全署	1、110 年完成主動式防禦機制規劃，並實作驗證 2 套主動防禦情境；建立偵測規則部署與回傳機制，並選定 2 個機關試行導入 2、111 年完成主動式防禦應用平台建置，並持續實作驗證 2 套主動防禦情境；推動 2 個機關導入偵測機制 3、112 年完成主動式防禦應用平台自動化效率精進，並持續實作驗證 2 套主動防禦情境；持續推動 2 個機關導入偵測機制 4、113 年完成主動式防禦應用平台擴增，並持續實作驗證 2 套主動防禦情境；持續推動 2 個機關導入偵測機制
3-2 完善政府網際服務網防禦深廣度	數位發展部資通安全署、數位發展部	1、110 年完成零信任網路與概念性驗證機制研究與部署機制；提升 GSN 骨幹流量收容達 40G，攻擊指標與受害指標行為回溯 1 年，並強化快取 DNS 之防禦能量 2、111 年推動 2 個機關導入零信任網路之身分鑑別機制；提升 GSN 骨幹網路社交工程手法偵測能量達 40G，GSN 連外台北主節點建置 1 套高性能惡意 IP 阻斷設施 3、112 年推動 2 個機關導入零信任網路之設備鑑別機制；完成 GSN 骨幹網路威脅情資分析索引系統建置，並佈署 1 套高性能及容量之 DNS 過濾器 4、113 年推動 2 個機關導入零信任網路之信任推斷機制；精進威脅偵測與分析能力，產製我國自主資安威脅情資，並提供 DNS 權威主機代管或備援服務，提升機關 DNS 可靠度，並推動 DNSSec 安全
4、提升科技偵查能量防制新型網路犯罪		
4-1 強化新型網路犯罪偵查能量	內政部、法務部	1、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 2、建置並推廣資安事件調查模擬平臺 3、持續協助駭侵案件查處，研提新型態網路犯罪偵查報告

工作項目	主(協)辦部會	分年重要進程(量化目標)
4-2 提升資安事件溯源追蹤能力	內政部、法務部、(數位發展部資通安全署)	1、持續提升數位鑑識能量、強化情資分享及技術交流 2、分年推動建置南區延伸鑑識實驗室，加速中南部單位取得數位鑑定報告時效，拓展資安鑑識能量 3、自主研發現場取證工具，並扶植國內廠商共同開發，提升國內鑑識工具研發能量 4、透過蒐集各單位所得國內情資，比對境外提供情資，找出策動攻擊之來源與駭客組織，以達溯源目的
4-3 加強跨境網路犯罪偵查機制	內政部、法務部	1、每年建立與國外企業調閱相關犯罪資料窗口 1 件 2、參加資安研討會、常態性出席實體或線上國際會議，並積極與國際組織駐臺代表交流，每年至少 7 次 3、開發主動式威脅端點獵蒐系統，機先發掘境內潛藏之惡意威脅端點
策略四：健全智慧國家資安，提升民間防護能量		
1、輔導企業強化數位轉型之資安防護能量		
1-1 結合民間資源，建立公私協同合作機制，協助企業提升資安防護能量	數位發展部、(數位發展部數位產業署)	1、優化 TWCERT/CC 資安情資系統及服務，深化我國企業資安事件諮詢及協處服務，每年受理並審核國內企業產品資安漏洞通報至少 30 個 2、逐年擴大與國內企業分享資安威脅情資 3、每年輔導至少 10 家高風險網路零售業者導入資安防護措施，舉辦 2 場網路零售資安推廣活動
1-2 提升民眾資安意識	數位發展部	1、每年提供 12 期資安情資電子報，訂閱讀者每年成長 10% 2、每年對民眾進行 4 則資安相關宣導，以降低民眾受害風險 3、每年發布 4 篇資安小知識專欄文章及 4 則宣導影片，以提升民眾資安意識
2、強化供應鏈安全管理		

工作項目	主(協)辦部會	分年重要進程(量化目標)
2-1 強化委外供應鏈風險管理	數位發展部資通安全署	1、因應新興科技及國際資安威脅情勢，每年完成 2 份委外管理相關參考文件之檢視或增修訂 2、每年遴選 10 個機關進行實地輔導，落實委外作業安全管理 3、每年遴選至少 20 個以上機關辦理資安稽核，加強檢視委外管理制度
2-2 聚焦資通訊晶片產品安全性	數位發展部數位產業署	1、110 年研發晶片惡意邏輯威脅檢測工具 1 套；制定晶片安全檢測規範 1 份及晶片安全相關指引 10 份；完成國際認可檢測實驗室前置作業報告 1 份 2、111 年研發晶片旁通道攻擊檢測自動化工具 1 套；成立國內晶片安全檢測實驗室；協助至少 2 家國內晶片業者之晶片產品通過晶片安全測試相關標準，發行晶片安全測試報告 3、112 年研發矽前旁通道弱點模糊測試工具 1 套；晶片安全檢測實驗室取得國際認可；協助至少 2 家晶片業者之晶片產品進行場域安全實證 4、113 年發展晶片安全合規檢測系統 1 式；建立晶片安全開發垂直運用場域 1 案；提供國際 IoT 平台安全標準(PSA 或 SESIP)等測試服務，達成產品國內檢測結果受國際承認至少 1 案
3、建構安全智慧聯網		
3-1 健全新世代行動通訊技術網路安全	數位發展部	1、法規標準：修訂「5G 資通安全維護計畫」稽核計畫及標準作業程序文件，每年針對各類型 5G 網路架構納入資安防護範圍 2、技術研發：建立 5G「軟體整合開發暨運作程序」及「軟體系統」資通安全分析及檢測平台，提供業者相關評估、測試及驗證服務，另協助業者建立資安能量與能力 3、場域實證：110 年至 111 年，每年推動 5G 垂直場域實證 1 件；112 年至 113 年，每年研析國內外 5G 垂直應用場域相關政策、案例與數位轉型議題 1 件

工作項目	主(協)辦部會	分年重要進程(量化目標)
3-2 推動物聯網合規驗證及場域實證	數位發展部數位產業署、經濟部、(數位發展部)	1、110 年制定我國物聯網資安檢測驗證框架，並於 111 年擬訂物聯網資安標準優先制定策略及清單項目 2、每年建立 1 項應用示範展示場域，涵蓋至少 2 項次資安技術或產品應用；111 年起每年促成 1 案次創新資安技術或產品試煉應用實證 3、與美國國家標準暨技術研究院(NIST)進行資安標準及檢測技術交流 4、每年舉辦 1 場技術交流活動，將國際間相關技術發展資訊分享各界 5、每年制(修)訂 1 項以上 IoT 設備或通傳事業使用之資通設備資安檢測產業標準或技術規範

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

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。