國家資通安全研究院

發展目標及計畫

中華民國112年5月

112年1月17日第一屆第二次董監事聯席會議通過

數位發展部112年2月20日數位策略字第1127000268號函核定

112年4月11日第一屆第三次董監事聯席會議決議修正

數位發展部112年5月23日數位策略字第1127000969號函核定

目次

壹、總目標及說明

一、緣起

我國政經情勢特殊，除面對全球複雜多元之資通訊變革，尚需面對較其他國家更為險峻之資安威脅，為確保民眾數位生活福祉、新興資安產業發展及數位國土國家安全，持續落實並精進各項資通安全防護工作實屬必要。在「資安即國安」政策下，政府已將資通安全提升至國家安全層級，亦確立邁向數位國家之具體方向。

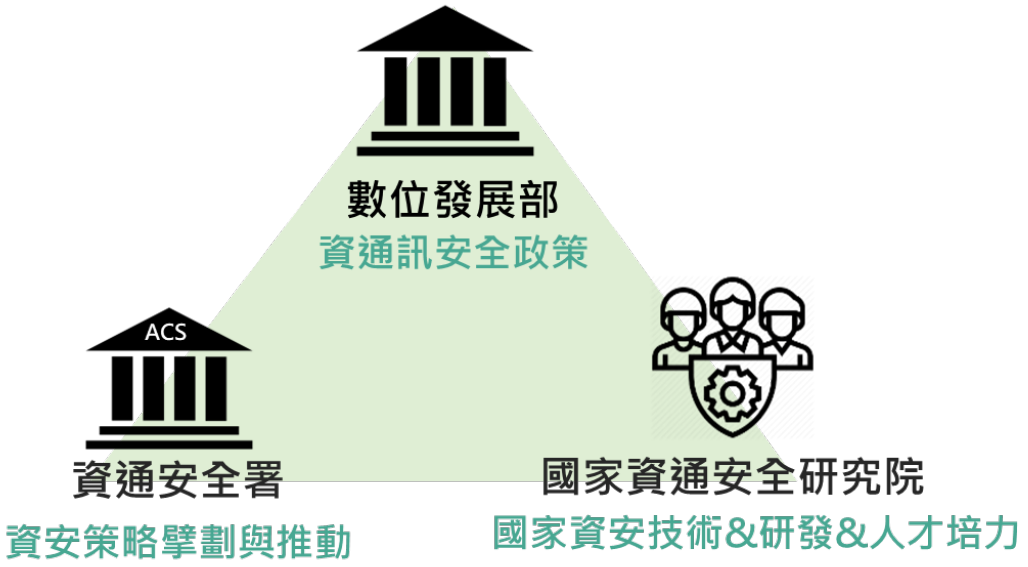
總統蔡英文於 109 年 520 就職演說中提到，我國邁向國家數位轉型，並推動 6 大核心關鍵產業，成立專責部門負責資訊、資安、電信、傳播及網路等 5 大領域業務，以統一事權、整體規劃數位發展推動相關資源，並統籌產業、政府、社會與國民生活數位轉型之基礎建設及環境整備，以及資通安全、資料治理、創新沙盒、人才培育、數位包容及法制規範等業務，協助各機關落實數位治理，因此數位發展部(以下簡稱數位部)於 111 年 8 月 27 日掛牌成立。

綜觀各國資安推動組織，大多設立資安專責機關，並設技術幕僚，於危急時扮演聯合指揮與共同作業之功能。資通安全業務涉及國家安全，具高度技術性及專業性，執行上應有可信賴且具人才延攬彈性之「專業資安法人組織」，長期投入各項資通安全技術研發及防護工作。

無論以專責單位或技術幕僚組織等形式，其組織需具備相當程度規模，並具有「專責」、「專人」及「常設性組織」等特性，專注國家整體資安防護目標，擔負國家資安技術幕僚角色，並擔任國家資安防護守門員。此外，配合「資通安全管理法」推動，在完善法制基礎下，有效協助政府加速建構完善資安環境，落實公私部門資安管理，帶動整體資安產業向上發展。

數位部下設有 6 個業務單位與 2 個三級機關、監督 1 個行政法人及主管 3 個財團法人，其中資通安全署(以下簡稱資安署)負責國家資通安

全政策規劃、計畫核議及督導考核，執行國家資通安全防護、演練與稽核業務及通訊傳播基礎設施防護，而行政法人國家資通安全研究院(以下簡稱本院)以公法人角色執行國家任務，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。因此數位部、資安署及本院構成堅實之資安推動鐵三角(詳見圖 1)，透過擴充國家資安團隊及能量、強化跨機關資安聯防機制、提升早期偵測預警能量、公私協力建立資安聯防體系、掌握自主資安科技及加速扶植資安產業等推動策略，達到國民安心使用數位服務、確保政府服務持續運作及保護政府與民間數位資產之目標。



資料來源：本院整理

圖1　資安推動鐵三角

二、依據

111 年 1 月 19 日總統令制定公布「國家資通安全研究院設置條例」，行政院定自 112 年 1 月 1 日施行。

依據「國家資通安全研究院設置條例」，本院業務範圍包含：

(一) 研發資通安全科技，推動資通安全技術應用、移轉、產學服務及國際交流合作。

(二) 協助規劃及推動國家資通安全防護機制。

(三) 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。

(四) 協助規劃及支援國家關鍵基礎設施之資通安全防護。

(五) 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。

(六) 支援具有特殊敏感性之政府機關(構)資通安全防護工作。

(七) 支援產業資通安全重大發展及法規推動之需求。

(八) 其他與資通安全科技相關之業務。

三、全球資安威脅趨勢

根據世界經濟論壇(World Economic Forum, WEF)「2022 年全球風險報告」統計，因新冠肺炎疫情對全球經濟、生活及技術應用等不同面向造成影響，有關經濟、環境、地緣政治、社會及科技等 5 大類風險中，其中科技類型風險以「資安措施失效(Failure of Cybersecurity Measures)」為最高，並包含惡意技術利用、技術治理失效、數位權利集中及 IT 基礎架構失效等。報告指出，因相關惡意工具被使用，大幅降低網路威脅攻擊之門檻，同時帶來更激進之攻擊方法，再加上缺乏網路安全專業人員與未臻完善之治理機制，更加劇維護網路安全之困難程度。全球風險認知調查還包含國際風險緩解工作，以及與科技有關之風險，如人工智慧、跨境網路攻擊及錯誤訊息等，大多數受訪者認為現階段之風險緩解工作仍處於力有未逮時期，相關回應工作尚未開始或落在早期開發階段。

面對新冠肺炎疫情同時，亦因病毒不斷變種，各項因應措施處於且戰且走之窘境，因疫情而漸趨普遍之居家辦公(Work From Home, WFH)工作

模式，帶來資訊設備、身分驗證及居家實體環境等不同挑戰，亦持續挑戰資通安全管理之因應模式。

如同疫情無法藉由邊界封鎖完全控制，網路攻擊事件、跨境攻擊更無法倖免。觀測 110 年全球重大網路攻擊事件，個人憑證或帳號通行碼之外洩事件甚囂塵上，且因社群媒體發達與民眾資安防護意識尚未完善，造成個資外洩事件無法緩解。此外，隨著物聯網(Internet of Things, IoT)設備普及，惟系統漏洞未即時被偵測與修補，科技技術之進步反造成不利之衝擊。駭客透過勒索軟體與進階持續性威脅(Advanced Persistent Threat, APT)攻擊等手法，致使各國企業與政府機關受到波及，尤以民生相關之水資源、油電等關鍵基礎設施者相關攻擊所造成之影響，實不容輕忽。

經綜整研析歐盟網路暨資訊安全局(European Union Agency for Cybersecurity, ENISA)、澳洲網路安全中心(Australian Cyber Security Centre, ACSC)及各資安業者調查等報告資料，可歸納為 6 大面向之資安威脅情勢，包含「疫情造成資安風險提高」、「勒索軟體攻擊風險激增」、「物聯網與行動式設備資安弱點威脅升高」、「資安(訊)供應商遭駭破壞供應鏈安全」、「進階持續威脅鎖定式攻擊竊取機密資料」及「社交工程詐騙盛行」。

因疫情持續蔓延，導致工作環境調整，發展出不同工作模式，如雲端運作、電子商務及遠距會議等，同時相關之詐騙郵件與新式網路攻擊亦大幅提升，可預見新型態之網路犯罪生態體系，其網路犯罪分工將更加精細，鎖定目標對象後展開之勒索軟體攻擊亦將成長，再加上有利可圖，防不勝防。

遠距工作之連網環境造成越來越多資通安全議題，使用個人擁有之 IoT 設備與行動式設備造成相關資通安全威脅，如 IoT 設備之預設帳號通行碼、未更新之系統漏洞等，皆為必須優先解決之議題。面對許多供應商所產生之資通安全事件，除主張以契約規定要求外，亦應積極在尋商時先

進行安全等級評估，並於合作期間訂定一致性之安全等級要求，檢視所有供應商符合要求之程度。組織應針對業務定期進行風險評估，瞭解業務重要性與可能成為目標式攻擊之風險程度，以因應並提升防護等級。伴隨社交工程詐騙手法不斷翻新，唯有加強教育訓練並持續測試其有效性，以建立防範社交工程詐騙之第一道防線。

四、環境與問題評估

(一) 政府資安防護現況

政府資通安全情蒐研析，主要透過威脅誘捕情蒐研析、聯防監控威脅情蒐、社交工程情蒐研析及通報事件分析，掌握面臨之整體網路安全威脅情資，強化資通安全防護部署。

威脅誘捕情蒐研析，收容國內外蜜罐系統誘捕之威脅情資進行分析，透過自行建置之攻擊歷史事件聚合模組，進行攻擊類型分類，並針對各攻擊類別產製攻擊指標及相關情資，以掌握網路攻擊概況。聯防監控威脅情蒐，收容 SOC 業者回傳之政府機關資安監控情資進行關聯分析，並透過資安聯防監控月報提供威脅情資進行聯防，以及掌握政府領域整體資安監控概況。

近年來，社交工程郵件為政府機關面臨之主要資安威脅之一，且有逐年上升之趨勢。駭客以社交工程、釣魚郵件及垃圾郵件，夾帶含惡意程式之檔案或連結，致目標電腦被感染控制，進而導致機敏公務資料外洩風險。藉由社交工程情蒐研析，分析所使用之手法，加強惡意郵件之攔截，並教育使用者瞭解風險所在。同時，分析國內外資安情資與資安通報事件資訊，統整網際網路攻擊來源、政府骨幹網路異常連線資訊及資安事件發生原因等，再經由關聯分析政府機關事件通報資訊之攻擊來源與樣本特徵，掌控駭客控制中繼站與端點攻擊目標、手法及整體威脅趨勢。

(二) 政府資通安全防護策略

依據「國家資通安全發展方案(110 年至 113 年)」，以強化政府機關縱深防禦、提升國家資安防護能量為主軸，形成資安核心技術能量。同時，配合政府資訊(安)集中共享策略，推動政府大內網資安防護向上集中機制，於向上集中機關出入閘道口部署 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，以即時阻擋惡意攻擊，主動防禦潛在威脅。

發展零信任網路資安防護環境，以完善政府網際服務網之防禦深廣度，進行零信任網路概念性驗證與部署規劃，並逐步推動零信任網路之身分鑑別、設備鑑別及信任推斷機制。

規劃內網威脅誘捕機制，蒐集向上集中機關與所屬機關之內網攻擊威脅，彙整產製攻擊威脅情資提供機關進行防護。部署 APT 攻擊偵測規則於向上集中機關之 IPS 系統，於偵測到駭客活動第一時間，可立即進行阻斷。同時，藉由自動化部署黑名單於向上集中機關之防火牆或其他阻擋機制，即時阻擋駭客攻擊。另外，針對資訊資源向上集中機關部署惡意郵件威脅偵測機制，偵測跨所屬機關之惡意電郵，強化主動式防禦能量。

(三) 物聯網與行動式設備資安風險劇增

資安業者 Check Point 110 年網路安全報告調查數據顯示，109 年 46%企業至少有 1 名員工曾於手機下載惡意軟體，且於全球關閉邊境或封城期間，手機使用量增加亦導致銀行木馬與竊取資料之手機木馬程式數量不斷增加。在其 111 年網路安全報告則指出，惡意攻擊者持續一整年對行動式設備展開使用者端與目標式之企業攻擊。調查研究顯示，因工作場所實施 BYOD 政策，約有 49%受調查組織表明，無法偵測到因員工自帶設備所遭受之攻擊或事件。

物聯網裝置普及且運用廣泛，惟若疏於管理可能造成莫大影響。檢視資安事件案例發現，殭屍網路惡意程式利用已知老舊漏洞，攻擊

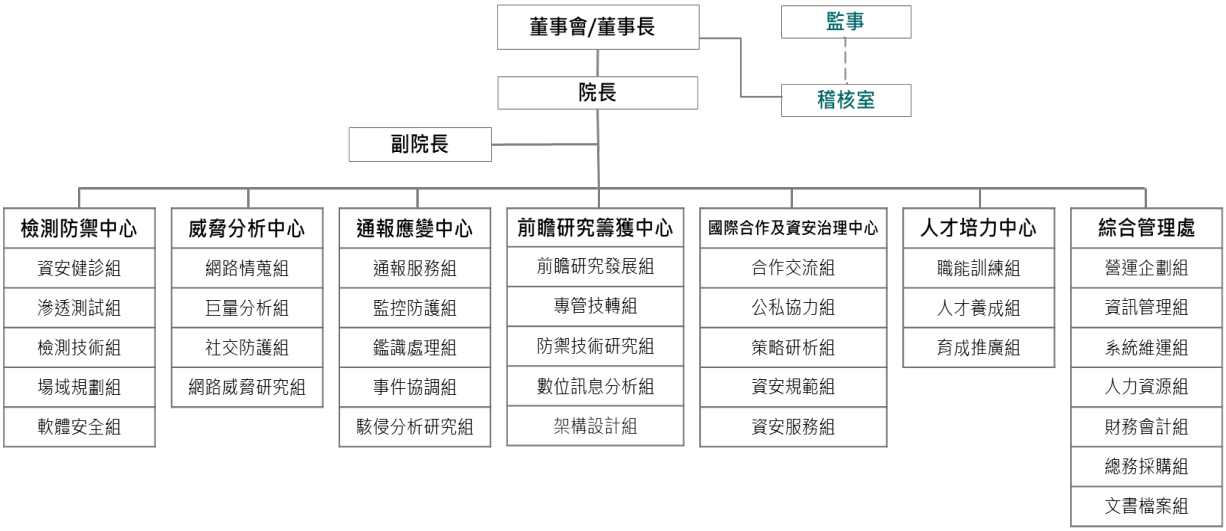
物聯網設備事件時有所聞。為大型電信業者 AT&T 資安實驗室 Alien Labs 揭露，新殭屍網路惡意程式 BotenaGo 利用 33 個已知之老舊資安漏洞，鎖定數百萬台 IoT 設備發起攻擊行動，相關設備包含網路路由器、數據機及網路儲存裝置等，其中有部分受駭裝置由台灣廠商生產製造。BotenaGo 使用程式語言 Go 撰寫，成功入侵設備後將執行遠端 Shell 指令，並依受感染設備類型，下載不同惡意封包資料(Payload)，且因駭客刪除伺服器上所有惡意封包資料，致資安研究人員無法得知駭客最終企圖。

IoT 裝置之威脅防護因應措施包含裝置設計開發階段之安全設計(security by design)，以及設計完成後之資安測試認證；裝置於現場配置時須建立合法辨識，避免非法不明裝置入侵；裝置在韌體維護更新時須有資安驗證程序，並於發現裝置漏洞時及時更新補強，以及裝置遭入侵後必須加以隔離，以避免危害範圍擴大。

貳、組織概況

本院組織架構以強化國家資通安全防護、資安人才培力及資安關鍵技術發展等功能角色，在技術面包含檢測防禦、威脅分析及通報應變等 3 個中心，管理面包含前瞻研究籌獲、國際合作及資安治理，以及人才培力等 3 個中心，據以銜接本院 5 大核心價值，並由綜合管理處擔任行政支援角色，本院組織圖詳見圖 2。

本院監督機關為數位發展部，設有董事會，並置監事 3~5 人，分別行使監督與查核等職權。本院設有院長 1 人，由董事長提請董事會通過後聘任之，負責本院營運及管理業務之執行，並設副院長 2~3 人，輔佐院長襄理本院業務，另下設稽核室，規劃推動內部稽核業務。



資料來源：國家資通安全研究院官網

圖2　國家資通安全研究院組織圖

本院檢測防禦中心、威脅分析中心、通報應變中心、前瞻籌獲中心、國際合作及資安治理中心、人才培力中心及綜合管理處之職掌，詳見表1。

表1　國家資通安全研究院各單位職掌

單位	職掌
檢測防禦中心	▪政府組態基準規劃及執行 ▪資安弱點通報機制規劃及執行 ▪資通系統滲透測試 ▪資通安全管理法相關技術檢測服務 ▪主動防制機制規劃及技術研發 ▪工業控制系統資安檢測技術研發 ▪資安模擬場域規劃及建置 ▪共用資通安全系統開發及維運 ▪其他有關資安檢測防禦事項
威脅分析中心	▪網路威脅情蒐與攻擊趨勢分析及預警 ▪社交工程攻擊情蒐機制規劃及執行

單位	職掌
	▪政府骨幹網路情資蒐集及分析 ▪政府聯防情資蒐集、分析與聯防 ▪資安情資整合及分享 ▪各項情資威脅技術研究及應用 ▪其他有關資安威脅分析事項
通報應變中心	▪資安監控及警戒服務 ▪資安事件通報諮詢 ▪資安事件鑑識分析 ▪政府機關與關鍵基礎設施重大資安事件應變協處 ▪組織型駭侵研究 ▪端點偵測及回應機制規劃及執行 ▪其他有關資安通報應變事項
前瞻研究籌獲中心	▪新興資通訊資安防護需求研析及規劃 ▪產學研合作研究規劃及推動 ▪新興資安應用技術發展研析 ▪新興資安技術規範與基準研訂 ▪資安應用科技研究及技術開發 ▪資安防護應用技術研究及移轉 ▪數位訊息防護應用技術研究及移轉 ▪資安韌性巡檢服務 ▪其他有關前瞻資安技術研究籌獲事項
國際合作及資安治理中心	▪國家資通安全策略研析 ▪資安研究國際合作及情資分享 ▪國際資安攻防協作 ▪國際資安人才合作培育 ▪資安國際情勢觀測及研析 ▪關鍵基礎設施資安防護研析 ▪資安標準與規範研析

單位	職掌
	▪其他有關國際合作及資安治理事項
人才培力中心	▪資安人才職能發展框架及評量機制研析與推廣 ▪資安人才培訓課程規劃及開發 ▪關鍵基礎設施培訓課程開發及維護 ▪資安實戰課程開發及維護 ▪資安認知意識與防護實務推廣 ▪其他有關資安人才培育事項
綜合管理處	▪組織人事、採購、文書、印信、出納、財產及總務等業務規劃、推動與營運管理相關事項 ▪人力資源規劃管理與執行 ▪組織財務整體規劃，包含年度收支預、決算之籌劃，預算管控，財務規劃擬定 ▪計畫之規劃、審查、管制考核及績效評鑑 ▪計畫管理運作相關制度與程序之建置及組織發展規劃 ▪組織各項資訊作業與網站之規劃、維護、管理及整體資訊系統維運管理與各類資訊應用支援 ▪民意機關、新聞媒體間聯繫及服務業務辦理 ▪全院法制業務及涉訟案件處理 ▪其他有關綜合管理業務

資料來源：國家資通安全研究院組織章程

參、發展目標

考量新興資通訊科技發展與駭客攻擊手法日趨多元，世界各國均朝向將資安提升至國安層級方向發展，加強資通安全防護，以維護國家安全。囿於資安威脅情勢日趨嚴峻，近年先進國家均在資安防護基礎上投入大量資源。我國政經情勢特殊，長期遭受網路駭侵，為確保民眾數位生活福祉、新興資安產業發展及數位國土國家安全，持續落實並精進各項資通安全防護工作實屬必要。

依「資安即國安」政策，資通安全已提升至國家安全層級，本院以「打造國際級資安韌性科研團隊，建立安全、安心及安穩的數位環境」為願景，專注國家整體資安科研及服務工作，面對外部資安威脅及與日俱增之駭侵趨勢，訂定「強化國家資安防護機制，提升智慧國家資安韌性」、「建立國家級資安團隊，確保數位國土安全」、「推動資安技術研發，促進產業資安發展」等 3 項目標。

配合國家整體資安推動策略方向，強化國家資通安全防護、資安人才培力及資安關鍵技術發展，並協助公私部門加速建構完善之資安環境，落實資安管理，帶動整體資安產業向上發展，本院 5 大核心價值(START)如下：

(一) 安全(Security)：為建構國家全方位資安防護網，透過情資整合分析、跨域聯防及事件通報協處等方式強化。

(二) 技術(Technology)：透過與產學研各界共同合作研發，期帶動國家資安關鍵技術發展。

(三) 主動(proActiveness)：持續觀測國內外資安情勢發展，擔任國家資安研發幕僚。

(四) 韌性(Resilience)：提供政府機關資安服務，強化機關資安韌性，成為國家資安技術服務標竿。

(五) 信賴(Trust)：強化人才培力能量，培育國家頂尖資安人才與資安防護團隊。

本院依願景、目標及 5 項推動策略，建構發展藍圖(詳見圖 3)，以執行各項資通安全任務，包含事前、事中、事後各項資安技術服務，並針對資安前瞻技術進行研究，以及持續培育高階實戰人才。

資料來源：本院整理

圖3　國家資通安全研究院發展藍圖

本院以 3 項目標為依歸，採下列 5 項推動策略實踐 5 大核心價值：

(一) 建構資安防護聯網，強化資安預警能量。

(二) 研發資安前瞻技術，帶動自主創研能量。

(三) 觀測各國資安情勢，深化國際合作交流。

(四) 推動公私協同治理，提升關鍵設施韌性。

(五) 培育資安實戰人才，推廣全民資安意識。

依本院業務範圍與 5 項推動策略，擬訂 11 項具體作法，包含推動資安防護機制、執行重大事件應變處置、支援敏感性政府機關資安防護、研發資通安全科技、推動產學合作與技術移轉、研析各國資安趨勢、擴展國際合作交流、推動資安技術應用、支援產業資安重大發展、培育資安人才及推廣全民資安意識等。

肆、推動作法及計畫

透過 11 項具體作法，期能完善資安聯防體系，提升資安應變能力與

資安防禦技術，並打造系統之安全性與韌性，協助加速建構完善資安環境，促進政府數位系統安全與整備韌性環境，落實公私部門資安管理，帶動整體資安產業向上發展，11 項具體作法與公私協同合作方式詳見圖 4。

資料來源：本院整理

圖4　具體作法與公私協同合作方式

依本院 11 項具體作法之執行重點，訂定業務計畫說明如下：

一、推動資安防護機制

掌握我國資安威脅情資，進行情資整合應用，強化黑名單自動化部署、政府領域資安情資掌握、惡意電子郵件威脅資訊蒐整，產製自主威脅聯防情資，掌握組織型駭客手法與影響範圍，協助機關阻擋惡意郵件攻擊，建構完整防禦陣線，以強化我國資安聯防體系。

二、執行重大事件應變處置

全時監控機敏機關網路，維運政府機關資安通報應變機制，掌握資

安事件發生與處理狀況，提升緊急應變處理能量，降低資安事件衝擊，並研析與精進國家重大資安事件應變。

三、支援敏感性政府機關資安防護

擴大追蹤高風險機關資安防護情形，強化組織型駭侵偵測防護，規劃擴充政府骨幹網路流量偵測與分析機制相關硬體效能，升級各重點機關監控設備，提升機關預警正確性與時效性。

四、研發資通安全科技

掌握新興技術發展趨勢，進行前瞻研究及資安技術應用，擬定研發策略與設計機制，以形塑國內良好資安技術研發環境。同時利用本院核心技術能量，蒐集政府、學術及民間網路資安威脅情資，建立跨政府機關資安聯防監控機制，研析國內外資安威脅，建立預警機制，並透過公私協同合作進行資安情資分享，降低我國資安風險。

五、推動產學合作與技術移轉

依據政府資安需求，研擬產學研合作規範，建立合作管道，並盤點研究成果與預期可供技轉技術項目，研議資安相關技術標準與規範，使研發技術得以落地，推動資安技術應用。

六、研析各國資安趨勢

研析各國資安法規體系，制定政府機關資安規範與指引，並透過資安服務共同供應契約與廠商評鑑改善供需環境生態，以完善資安法規與標準，健全國家資安整體生態體系為目標。

七、擴展國際合作交流

參與國際資安相關重要會議與活動，建立跨國資安情資交流與合作管道，持續加強國際合作夥伴連結，及時掌握全球資安威脅趨勢，並整合國內外資安情資，成為國內主要情資彙整與分享平台。

強化國際資安技術交流，提升國際參與成效，辦理跨國攻防演練，促進國際資安交流與合作。

八、推動資安技術應用

定期檢視政府與關鍵基礎設施之網路與資訊系統安全性，及早發現政府與關鍵基礎設施資安問題，降低資安弱點與設定產生之系統風險。

為建構政府安全與韌性環境，建構軟體物料清單、擴充政府設計系統元件與開放原始碼詮釋資料，盤點民生關鍵資訊系統，執行數位韌性巡防服務，提升整體政府機關資通系統數位韌性。

九、支援產業資安重大發展

配合國家資安政策分享資安技術，加速資安產業框架與應用情境，提升台灣資安產業之自主能量，積極推動產業導入資安防護機制，以確保我國整體資通安全。

十、培育資安人才

因應國家發展需求，為充實各領域資安人才，設置資安人培實體場域，強化工控領域訓練，並設置虛實整合競賽平台，提供學習與演練管道，孕育優質資安人才。

十一、推廣全民資安意識

辦理政府資通安全防護巡迴研討會與資安競賽，與相關部會合作透過資安政策宣導及資安威脅趨勢與案例分享，強化政府機關資安意識，提升政府機關資安人員之資安技術與管理能力，並藉由不同主題活動、遊戲及競賽等方式，推動資安技能向下扎根，強化全民資安意識，提升資通安全之素養與水準。

針對最新資安案例進行研析，並提出法律分析與管理建議，評估並摘選重要資安相關法規加以彙編，或編撰相關文件，供機關參考利用，

以提升機關對資安法規之瞭解。

伍、績效指標

依據「資安即國安 2.0 戰略」政策方針與「國家資通安全發展方案(110 年至 113 年)」各項推動策略，並參照本院目標與推動策略，擬訂 4 年績效指標(詳見表 2)，同時滾動式檢討績效指標合宜性。

表2　112 至 115 年績效指標

推動策略	112 年	113 年	114 年	115 年
建構資安防護聯網強化資安預警能量	▪ 強化資安聯防，完善資安情資分享網：建構情資自動化分享機制，協助政府機關與關鍵基礎設施維運者及時接收警訊並應變處理，5 家 A 級關鍵基礎設施維運者納入情資自動化分享服務網 ▪ 提升政府骨幹網路資安威脅防護：建置政府骨幹網路流量分析平台，建立萃取與威脅分析機制，產製中介分析	▪ 強化資安聯防，完善資安情資分享服務網：協助政府機關與 A 級關鍵基礎設施維運者納入情資自動化分享服務網 ▪ 提升政府骨幹網路資安威脅防護：提升政府骨幹網路流量分析平台資料儲存容量，確保 100% GSN 骨幹網路流量均納入分析，資料收容儲存量達 1 年	▪ 強化資安聯防，完善資安情資分享服務網：協助政府機關、A 級關鍵基礎設施維運者， 以及 50% B 級關鍵基礎設施維運者納入情資自動化分享服務網 ▪ 提升政府骨幹網路資安威脅防護：提升政府骨幹網路流量分析平台運算量，確保 6 個月內資料均完成分析索引	▪ 強化資安聯防，完善資安情資分享服務網：協助政府機關與 A、B 級關鍵基礎設施維運者均納入情資自動化分享服務網 ▪ 提升政府骨幹網路資安威脅防護：持續提升政府骨幹網路流量分析平台運算量，研發常規資安大數據分析項目 10 項

推動策略	112 年	113 年	114 年	115 年
	資料，並建置分析索引系統，進行網路威脅感知與分析，確保 50% GSN 骨幹網路流量均納入分析，資料收容儲存量達 6 個月			
研發資安前瞻技術帶動自主創研能量	▪研發 3 個資安技術應用系統並完成 PoC ▪導入 1 個資安技術應用系統並完成 PoS ▪推動 2 個單位採用或技轉相關研發成果	▪研發 4 個資安技術應用系統並完成 PoC ▪導入 3 個資安技術應用系統並完成 PoS ▪推動 3 個單位採用或技轉相關研發成果	▪研發 4 個資安技術應用系統並完成 PoC ▪導入 4 個資安技術應用系統並完成 PoS ▪推動 4 個單位採用或技轉相關研發成果	▪研發 4 個資安技術應用系統並完成 PoC ▪導入 4 個資安技術應用系統並完成 PoS ▪推動 5 個單位採用或技轉相關研發成果
觀測各國資安情勢深化國際合作交流	▪建立與國外資安技術、研究機構、NGO/NPO 合作管道，簽訂 MOU 或合作案至少 2 件 ▪媒合國內外資安學研單位合作案 1 件	▪建立與國外資安技術、研究機構、NGO/NPO 合作管道，簽訂 MOU 或合作案至少 3 件 ▪媒合國內外資安學研單位合作案 2 件	▪建立與國外資安技術、研究機構、NGO/NPO 合作管道，簽訂 MOU 或合作案至少 4 件 ▪媒合國內外資安學研單位合作案 3 件	▪建立與國外資安技術、研究機構、NGO/NPO 合作管道，簽訂 MOU 或合作案至少 5 件 ▪媒合國內外資安學研單位合作案 4 件

推動策略	112 年	113 年	114 年	115 年
	▪打造跨國攻防演練為亞太前三大演練之一	▪完成國際資安合作成果 2 項	▪打造跨國攻防演練為國際十大演練之一	▪完成國際資安合作成果 2 項
推動公私協同治理提升關鍵設施韌性	▪協助所有 A 級關鍵基礎設施提供者工控資安治理成熟度達第 2 級以上 ▪協助 80%之 A 級機關資安治理成熟度達第 3 級以上 ▪協助 50%之 A 級關鍵基礎設施提供者資安治理成熟度達第 3 級以上	▪協助所有 A 級關鍵基礎設施提供者工控資安治理成熟度達第 3 級以上 ▪協助所有 A 級機關資安治理成熟度達第 3 級以上、80%之 B 級機關資安治理成熟度達第 3 級以上 ▪協助所有 A 級關鍵基礎設施提供者資安治理成熟度達第 3 級以上、50%之 B 級關鍵基礎設施提供者資安治理成熟度達第 3 級以上	▪預計協助 50%之 B 級關鍵基礎設施提供者工控資安治理成熟度達第 2 級以上 ▪預計協助所有 A、B 級機關資安治理成熟度達第 3 級以上 ▪預計協助所有 A、B 級關鍵基礎設施提供者資安治理成熟度達第 3 級以上	▪預計協助所有 B 級關鍵基礎設施提供者工控資安治理成熟度達第 2 級以上 ▪預計協助 50%非向上集中之 C 級機關資安治理成熟度達第 2 級以上
培育資安實戰人才推廣全民	▪參考國際資安人才框架(如 ENISA)發展職能地圖與我國資安人才需求，協助完成	▪協助新增完成 3 類資安人才職能基準，規劃各類能力評量機制	▪協助新增完成 3 類資安人才職能基準，持續進行各類別資安課程與評量開發能量	▪協助新增完成 4 類資安人才職能基準，持續進行各類別資安課程與評量開發能量

推動策略	112 年	113 年	114 年	115 年
資安意識	2 類資安人才職能基準 ▪ 發展頂尖產業資安人才培訓實作環境，培育國內高階實戰人才 125 位 ▪ 推動全民資安意識達成虛實整合全年 10,000 人次參與；實體各項競賽與活動全年 650 人次	▪ 精進攻防平台之環境開發，培育國內高階實戰人才 125 位，試辦跨國人才參與 ▪ 推動全民資安意識達成虛實整合全年 12,500 人次參與；實體各項競賽與活動全年 750 人次	▪ 精進攻防平台之環境開發，培育國內高階實戰人才 150 位，提高頂尖跨國人才參與培訓比例 ▪ 推動全民資安意識達成虛實整合全年 15,000 人次參與；實體各項競賽與活動全年 1,000 人次	▪ 精進攻防平台之環境開發，培育國內高階實戰人才 150 位，形成國際知名資安人才養成中心 ▪ 推動全民資安意識達成虛實整合全年 20,000 人次參與；實體各項競賽與活動全年 1,200 人次