

中華民國 115 年 10 月
立法院第 11 屆第 6 會期交通委員會

數位發展部 業務概況報告

(書面報告)

部長 林宜敬

目次

壹、推進國家數位發展政策，建構數位韌性社會的跨域治理能 量，促進民間參與數位公共建設.....	1
貳、建構海陸空多元通訊應變網路，加速高速寬頻網路建設，提 升整體通訊網路韌性.....	3
參、前瞻規劃管理數位通傳資源，確保資源使用符合公共利益...	6
肆、強化數位應用，打造高效便捷的智慧政府.....	9
伍、強化數位發展國際合作，共同提升網路數位韌性.....	12
陸、發展資料運用，打造資料創新應用生態.....	15
柒、加速產業數位創新與轉型，帶動數位相關產業發展.....	22
捌、建構智慧化資安治理與跨域資安防禦生態系，推動資安法規 調適與資安人才培力.....	38
玖、打造國家資安科研團隊，建構全社會資安韌性.....	43

數位發展部業務概況報告

本部主要負責推動我國數位政策的創新與變革，整合電信、資訊、資安、網路與傳播五大領域；自本部成立以來，隨著大眾所關注的社會議題變化，對本部期待益加殷切，期本部能發揮更重要、積極的角色。為此，本部亦深切檢討施政重點，務求契合社會需求、邁向實現智慧國家的願景。

為落實建構「信任平權、韌性永續、自由多元、創新成長」的數位臺灣之數位政策目標，並扣合落實五大信賴產業及 AI 新十大建設等上位政策藍圖，本部以「加強打詐」、「發展軟體產業」、「強化資安韌性」、以及「建構數位政府」為四大主軸，攜手產官學研，打造創新、安全且以民為本的數位國家。

以下謹依 115 年本部施政目標之重要業務工作詳述於後：

壹、推進國家數位發展政策，建構數位韌性社會的跨域治理能量，促進民間參與數位公共建設

一、數位發展治理之研析與創新

(一) 研析國際數位發展及 AI 治理趨勢、國際數位競爭力評比、社會關切議題等，系統性建構本部中長期施政關鍵策略，並辦理政策溝通，以納入利害關係人意見。優先推動與民眾攸關之 AI 治理議題，透過指引規範、技術或商模等方式形塑治理框架，並與公協會合作推廣擴散。

(二) 完善本部總體施政策略框架及引導資源配置，導入外部專家協助優化本部總體施政目標與關鍵成果設定，提升計畫規劃品質與前瞻性，並加強 PDCA 循環機制，確保計畫符合長期政策願景。

二、人工智慧法規調適作業

- (一)本部已於 115 年 7 月 7 日函頒公告「人工智慧風險分類框架」，該框架將透過盤點應用情境、識別風險、評估風險、應對風險等操作步驟，協助各目的事業主管機關盤點所管產業 AI 應用情境、提出風險評估考量因素及訂定管理規範之建議。
- (二)為於《人工智慧基本法》所訂 2 年期限內（即 117 年 1 月 13 日前）完成法規調適，本部將透過「數位政策法制協調專案會議」下設之「AI 法制工作分組」，輔以協作會議、系統引導及線上諮詢等方式，協助各目的事業主管機關訂定以風險為基礎之管理規範，已與衛福部、經濟部、法務部、金管會、教育部、交通部、通傳會、勞動部凝聚共識，預計於 115 年底前完成 AI 風險分類框架所定流程；其餘機關則追蹤系統填報情形，並適時邀集召開會議討論，預計於 116 年 6 月前完成各部會第一輪法規調適；同時針對政府應用 AI 涉及法規部分，定期召開跨部會協調會議，推動相關法規調適作業與跨部會研商。

三、重要施政追蹤管制考核

- (一)為落實重要政策之列管追蹤，本部已訂定「數位發展部及所屬機關個案計畫管制評核作業要點」，並針對 115 年管制計畫強化推動列管個案計畫之管制評核；定期追蹤審視執行進度，以期計畫如質如期完成，並提升個案計畫執行成效。
- (二)持續辦理數位轉型與數位創新事務等相關財團法人之督導與管理，並配合國家科學及技術委員會辦理研究機構能效評估，以健全本部主管財團法人之組織及運作。

四、推動民間參與數位建設

- (一) 配合《促進民間參與公共建設法》明定數位建設類型，本部以 AI 算力中心作為優先推動案源，將 AI 算力設施納入重大數位公共建設範圍之標的，以租稅優惠提升民間投資誘因。本部業於 115 年 4 月 15 日辦理第 1 次政策公告，完成可行性評估報告審查會議，並分別於 115 年 7 月 17 日及 21 日各完成 1 場公聽會。同時於 115 年 8 月 7 日辦理第 2 次政策公告，期更進一步結合民間資源持續擴大 AI 算力規模。
- (二) 依據「兆元投資國家發展方案」，持續盤點數位公共建設之具體項目，評估納入重大公共建設範圍之可能性，以增進民間自提促參規劃及投資誘因。同時成立本部單一窗口，確保民間專業資金能精準對接國家重大建設，擴大民間投資國家建設之效能。

貳、建構海陸空多元通訊應變網路，加速高速寬頻網路建設，提升整體通訊網路韌性

一、海—提升我國海底通訊電纜韌性

- (一) 首次發布 114 年「臺灣海底通訊電纜損害原因分析及策進報告」：鑒於我國地緣政治情勢及灰色地帶等非傳統安全威脅日益嚴峻，為系統性檢視海底通訊電纜損害根本原因、掌握風險特徵，以據以推動相關安全防護策進作為，本部業彙整海纜障礙數據及應處紀錄，並於 115 年 4 月 7 日於官網公布「114 年度臺灣海底通訊電纜損害原因分析及策進報告」。藉由資訊公開透明，降低資訊落差與不實訊息傳遞，全面強化我國海纜通訊防護韌性及維運效能。
- (二) 鼓勵電信業者擴增海纜建設：持續鼓勵電信業者新設國內、

外海纜，國際海纜-東南亞日本二號海纜（Southeast Asia-Japan 2 Submarine Cable, SJC2）與杏子海纜 Apricot 已於 114 年投入營運，臺菲美海纜（Taiwan-Philippines-US Cable System, TPU）亦已於 115 年投入營運；國內海纜「臺馬第 4 號」已於 115 年 6 月底完工、「臺澎第 4 號」及「澎金第 4 號」預計於 115 年 10 月底完工。同時，亦補助業者建置或擴充微波建設 46 區間，強化偏鄉與離島地區通訊網路韌性。

- (三) 強化海纜設施與應變韌性：透過公私協力機制，持續輔導電信業者強化海纜登陸站防護措施，並增加多元通訊路由，114 年起已核定 9 案補助案申請，並進一步擴大補助範圍，納入海纜預警系統精進及加速斷纜修復流程等措施，強化事前預警與事後復原能量。

二、陸—強化災時通訊網路持續運作能力

- (一) 強化行動網路災時韌性：本部運用前瞻基礎建設預算，補助電信業者建置高抗災通訊平臺、行動基地臺車及移動式發電機等。至 115 年 9 月，已於偏遠、易成孤島地區及丹娜絲颱風災區等，完成建置 93 座高抗災通訊平臺，並增購 16 臺、優化 39 臺行動基地臺車(目前計有 52 臺搭載低軌衛星)，及購置 46 臺對微波系統、947 臺移動式發電機，提升重大災害期間行動通訊網路之持續運作能力。另 115 年將持續透過社會發展計畫，補助電信業者加速建置高抗災通訊平臺及優化行動基地臺車等。
- (二) 加速完備 5G 基礎建設：採取公私協力模式，鼓勵電信業者於交通樞紐、重要交通沿線及人潮密集區域，加速布建 5G 基礎設施，提升整體網路涵蓋率，114 年起補助電信業

者在交通樞紐、隧道等區域完成設置 5G 基地臺 1,123 臺。

三、空—布建多元衛星應變通訊網路

(一) 維運既有衛星應變網路：本部已完成「115 年政府非同步軌道衛星通訊及維運服務」共同供應契約，委由 OneWeb 及 SES 衛星服務獨家代理商，維運 196 個政府關鍵站點，並開放政府機關、學校及公營事業依需求訂購相關衛星通訊服務，強化緊急狀況下政府重要節點之備援通訊能量。

(二) 導入新興衛星通訊網路：因應國際低軌通訊衛星快速發展，本部自 115 年起辦理 Amazon Leo 新一代政府衛星專網落地介接先期研究。115 年上半年已依國科會指導完成政府關鍵節點需求盤點及初步配置作業，後續並將辦理 Amazon Leo 衛星服務可用性實測，作為 116 年布建政府衛星專網之基礎。

四、防護—強化通傳網路安全防護

(一) 督導通傳領域關鍵基礎設施 (CI) 落實安全防護：本部秉持行政院「全災害」思維 (涵蓋天然災害、人為破壞及資安威脅)，督導通傳領域關鍵基礎設施 (CI) 業者滾動修訂安全防護計畫。另配合 115 年城鎮韌性演習，上半年共辦理 2 場次安全防護演習、1 場次防護檢視、1 場次資安教育訓練及 1 場次情資分享會議；同時透過資安稽核落實法令遵循，並列管改善缺失，以強化通傳 CI 之防護能量與持續營運韌性。

(二) 推動電信資通設備資安防護措施：持續盤點並研析國際電信設備資安管理機制與設備適用資安標準 (如 Common Criteria, CC、歐盟 CRA 等)，滾動檢討電信設備資安相關要求。透過國內標準與國際加速對接，全面強化通訊網路

整體防護量能。

參、前瞻規劃管理數位通傳資源，確保資源使用符合公共利益

一、規劃與整備次世代無線電頻率資源

(一) 掌握國際 B5G/6G 頻譜發展趨勢與候選頻段實證量測

追蹤國際電信聯合會 (International Telecommunication Union, ITU)、亞太電信組織 (Asia-Pacific Telecommunity, APT) 及第三代合作夥伴計畫 (3rd Generation Partnership Project, 3GPP) 等重要國際組織，另亦掌握美、日、韓、歐洲等主要國家之 6G 技術、頻譜政策及商用發展進程，聚焦 WRC-27 候選 6G 頻段以及衛星直連手機 (Direct-to-Device, D2D) 等最新趨勢，並針對國際關注之 6G 候選頻段辦理實證量測，就 U6 頻段 (6425-7125 MHz) 既有微波鏈路與行動通信系統，以及 U4 頻段 (4400-5000 MHz) 既有 5G 專網與行動通信系統之共存情境，實測不同頻率配置、保護頻帶及保護距離下之干擾影響，作為研提頻譜整備及評估既有使用者移頻之政策依據，進一步提出頻譜政策規劃及釋照準備規劃。

(二) 衛星頻段釋出

本部自 111 年開放受理衛星通信頻率以來，每年穩定吸引業者遞件申請，截至 115 年 9 月底，已陸續完成隴華電子、愛爾康、台亞衛星、中華電信及遠傳電信等 5 家業者，共計 9 件申請案之審查。多家業者也已完成網路設置，正式於國內提供衛星服務，包括中華電信於 114 年 6 月及 10 月啟用的 OneWeb 與 SES O3b 服務、台亞衛星於 115 年 1 月開通的 Eutelsat 服務及隴華電子於 115 年 5 月開通的 Eutelsat 服務。

二、管理與提升電信資源使用效益

(一)精進頻率使用費制度及優化偏遠地區通訊品質

1. 精進電信資源規費制度

本部藉由使用費折抵機制，引導電信事業持續提升 87 個法定偏遠地區及山林區域之通訊服務品質，另促成包含智慧工廠在內等 37 案數位應用落地，持續提升頻率使用效益。另亦提出「頻率使用費收費標準」修正草案，透過差異化費率與折抵機制，期望鼓勵電信事業提供 5G SA 電信服務，進一步孵化應用創新之電信環境。

(二)促進新興技術蓬勃發展

在確保頻譜和諧共存前提下，透過嚴謹的干擾評估與資源調度，有效地支援產業研發之用頻需求。115 年截至 9 月底，審查通過累計 32 件產業研發頻譜申請案件，其中涵蓋低中高軌衛星、無人機反制雷達、車聯網及 6G 等關鍵技術領域。

三、推動近地高空通訊平臺創新應用與技術驗證

為強化災害應變及偏遠地區通訊韌性，本部推動高空基地臺整合驗證，透過大型無人機搭載行動基地臺及專用天線，結合地面後傳與既有行動通訊網路，建構可快速部署之空中通訊補位能力。115 年 3 月已完成高空基地臺專用天線及對準模組製造，並依實驗室測試結果持續優化；搭載系統之特種無人機於 8 月 13 日通過交通部民航局地面機體檢驗，並展開實地試飛及通訊整合測試。本部並與國內三家電信事業合作推動整合驗證，已於 9 月 23 日至 30 日完成第一階段基本效能測試，檢視高空基地臺之通訊涵蓋、資料傳輸效能及整體系統運作情形。

四、積極參與國際，保障數位通傳資源使用權益

(一) 深化頻譜國際交流與合作

積極參與世界無線電通信大會（World Radiocommunication Conference, WRC-27）、亞太經濟合作（Asia-Pacific Economic Cooperation, APEC）、世界行動通訊大會（Mobile World Congress, MWC）及亞洲頻譜管理會議（Asia-Pacific Spectrum Management Conference）等重要國際相關會議，掌握全球頻譜政策及新興無線技術發展趨勢，並辦理第3屆「頻譜政策領航(Spectrum for Tomorrow)」國際研討會，充分與重要國際主管機關與國內外產官學研交流，以利我國頻譜政策整備及國際接軌。

(二) 掌握關鍵議題，維護我國權益

本部為網際網路網域名稱及號碼指配機構（Internet Corporation for Assigned Names and Numbers, ICANN）/政府諮詢委員會（Government Advisory Committee, GAC）之主政機關，114年至115年7月底已會同外交部、內政部刑事警察局等機關深入參與ICANN 82至86計5場國際會議，維運涉我國主權域名（.政府）1筆；並協助我國擔任國際要職人士參與國際網路技術治理重要會議計17人次，成功爭取國際網路技術治理重要組織要職席次6名，充分展現我國數位量能。

(三) 培育次世代網際網路技術治理人才

為提升各界社群對網際網路技術社群公共事務之認知與專業知識，114年至115年9月底，共編訂電子報計21份，協助各界提升對ICANN及國際網際網路技術治理之最新政策發展；辦理公共政策研習營2場、研討會議5

場，持續擴大我國相關領域之人才庫，延續我國長期參與國際網路技術社群之策略。

肆、強化數位應用，打造高效便捷的智慧政府

一、積極參與國際數位政府活動，掌握全球政府數位轉型與政策發展趨勢，擴大我國數位政策規劃前瞻視野。例如持續參與國際組織會議（如 IAC 國際資訊長協會）分享我國發展數位政府服務之創新思維與實作情形；另外透過擔任 ICA 計畫委員會策劃委員角色，與各會員國間進行數位轉型經驗交流。為深入了解我國數位發展動態，已於 114 年完成我國數位近用調查報告，並於 115 年 1 月將調查結果公布至本部官網。

二、善用新興科技與政府資料，打造便捷高效的智慧政府

- (一) 為提升政府網站服務品質，115 年已完成 15 個機關網站易用性測試作業，及 5 個機關使用者中心設計（UCD）工作坊。為精進網站檢核作業，115 年上半年已完成政府網站智慧檢測工具試辦作業，各機關可藉由此工具檢測網站是否符合版型規範、並且一鍵生成報告檢核機制，優化檢測回應品質，並透過說明會分享試辦成果。
- (二) 為縮短各縣市政府資訊建設發展落差，本部徵選數位轉型成功典範案例，並透過研析方式，找出個案成功推動因素與做法，提供其他縣市參考。
- (三) 為協助各機關落實人工智慧基本法第 19 條及附帶決議，本部擬定「政府人工智慧應用風險評估檢核表」及「人工智慧應用內控管理要點（範本）」，並於 115 年 6 月 1 日發函行政院所屬各機關及地方政府評估其服務風險，以強化公部門人工智慧系統之風險治理與內控機制。

三、掌握政府數位人才供需，完備資訊職能基準與培力機制；並且推動政府服務單一入口機制，提升民眾使用政府服務體驗

(一)強化政府資訊人員數位能力，積極培力公務同仁之數位職能，並依循 AI 公務人才認定指引規劃，廣續推動資訊人才職務職能訓練，115 年協同保訓會，已完成 3 梯次新進資訊同仁資訊專業實務訓練，增設 AI 實機操作課程，奠定 AI 職能基礎；持續辦理 30 班次（約 450 小時以上）資訊人員實體在職訓練，課程納入 AI 賦能主題，助益日常業務推展；規劃 2 場次中高階資訊主管研習，以議題導向 AI 研習工作坊，引導主管運用 AI 技術解決機關實務議題，培養科技決策領導能力。

(二)本部與人事總處於 114 年 7 月共同成立 AI 公務人才發展辦公室，統籌培力資源，於 115 年 6 月 9 日發布「AI 公務人才認定指引」試行版，透過職能角色分類、學習路徑規劃及能力認證登錄，系統性培育政府所需人才，並以雙軌認證方式，對接本部數產署「AI 產業人才認定指引」民間既有的培訓與認證資源。

(三)完善政府數位首選服務入口，截至 115 年 9 月「我的 e 政府」已完成 99 項依主題彙整不同服務的整合性網頁，提供如兒少保護、就學補助、急難救助等政府服務整合資訊，並已提供超過 4,821 項網路申辦項目，116 年將聚焦以人生曾經歷的申辦事件為基礎，優化入口網功能，提升民眾使用政府服務體驗。

(四)本部推動政府無障礙網頁標章認證檢測服務，115 年截至 8 月之有效標章數量計 7,587 筆、人工檢測 3,595 件、身障人士檢測 632 件，受理無障礙申訴案件 63 件。

四、厚植政府資通訊環境量能，增進政府數位發展基礎環境效率與韌性運作

- (一) 為深化政府數位韌性運作，本部推動資安 A 級機關導入零信任架構。截至 115 年 9 月底，已全數完成 A 級機關導入零信任身分機制，並已協助累計 20 個機關導入零信任設備鑑別機制。
- (二) 輔導各級機關透過 T-Road 進行資料傳輸，截至 115 年 9 月底，已有 67 個機關與 210 項服務介接 T-Road，每月逾 210 萬筆傳輸量，將持續協助各級機關輔導作業及提供相關技術諮詢。
- (三) 本部政府骨幹網路防護措施，115 年平均每月攔截超過 8.6 億次攻擊、阻擋 168 萬次惡意網頁及 74 萬封垃圾郵件，通報 15 起 DDoS 攻擊事件，透過更新核心防禦組件與精進動態路由與備援機制，強化服務承載能力，確保在面對常態性攻擊時，系統仍能保有充裕的處理資源，維持服務不中斷的穩定品質。
- (四) 政府短網址服務截至 115 年 9 月底已超過 5 萬 5,000 筆短網址，逾 1 億 1,600 萬使用人次，預計 115 年達成 1 億 2 千萬人次使用。
- (五) 為提升政府簡訊識別度，避免有心人士偽冒政府簡訊詐騙民眾，各中央、地方機關以及公營事業已透過 111 短碼服務，發送簡訊予民眾，並於簡訊內容開頭新增「用戶手機門號末三碼」及「發訊機關具名」等明確辨識資訊，協助民眾快速判斷訊息真偽。統計 115 年截至 9 月底止，逾 600 個機關單位使用，累計發送逾 8,000 萬則簡訊。

五、建立「政府韌性服務環境」機制，並推動機關資料傳輸安全

及建置政府各類發放作業共用基礎平臺

(一) 為強化政府數位韌性，本部針對民生關鍵資訊系統及機關主要業務系統進行數位韌性健檢作業，112 年至 114 年完成共計 104 項政府資訊系統數位巡航健檢；115 年完成 39 項民生關鍵資訊系統、關鍵基礎設施等政府資訊系統數位韌性健檢，透過實地輔導協助機關落實數位韌性，並針對各系統提出精準建議，例如引導機關建構當外部語言模型中斷時，可轉由本地模型或專人接手的 AI 服務備援機制；建議機關於 AI 應用規劃初期即導入提示詞注入（Prompt Injection）防禦與個資遮罩機制；提醒機關須於契約中明訂資料再訓練條款及生成式 AI 再製授權範圍。透過精準且有效的輔導作為，實質協助機關緩減 AI 品質失控風險，厚植政府創新資訊系統的運作韌性。

(二) 為強化政府關鍵民生系統之韌性與整體服務能量，本部與 9 個執行機關共同推動「行政部門關鍵民生系統精進雲端備份及回復計畫」。114 年 9 個機關均已完成至少 1 次公有雲備份作業；115 年截至 6 月底，累計已有 3 個執行機關完成當年度跨境公有雲備份作業，並辦理回復至地端之演練；且依計畫期程 115 年底前將全數完成演練以及關鍵民生系統核心功能開發等工作。本部已完成對前述機關辦理 CompTIA Security、AWS Cloud 及 Google Cloud 等國際專業課程，超過 50 人次參與，提升政府機關人員對雲端服務的管理能力。

伍、強化數位發展國際合作，共同提升網路數位韌性

一、連結國際數位同盟：為連結國際數位發展理念與價值，彰顯政府開放及數位軟實力，規劃與推動下述業務

- (一)積極促成國際數位合作，本部 115 年持續參與亞太經濟合作（Asia-Pacific Economic Cooperation, APEC）之數位經濟指導小組（Digital Economy Steering Group, DESG）及電信暨資訊工作小組（Telecommunications and Information Working Group, TELWG）。於 115 年 7 月在中國舉辦之 APEC 數位及 AI 部長會議中，與亞太地區各經濟體發表「數位及 AI 部長聲明」及「促進亞太地區人工智慧發展聲明」等 2 項聯合聲明，並分享我國推動數位憑證皮夾、寬頻網路普及化、提供新創與中小企業算力、培育 AI 人才等成效，透過與各國分享我國數位科技發展策略，並吸引區域夥伴推動合作。另本部積極參與數位經貿諮商工作，115 年 4 月與歐盟重啟第 3 屆臺歐盟數位經濟對話會議（Taiwan-EU Dialogue on Digital Economy, DDE），就半導體、人工智慧（AI）政策、數位平台規範、資料治理、海底電纜、資安、5G/6G 發展、數位技能及影音政策等議題深度交流。
- (二)為持續深化臺美數位科技合作，本部於 115 年參與臺美「經濟繁榮夥伴對話」(Economic Prosperity Partnership Dialogue, EPPD)，與美方高階官員就 AI 治理、通訊韌性及數位產業發展等多項領域達成深化合作共識；並受邀赴美參加「矽盛世峰會」(Pax Silica Summit)，與美方就強化可信賴的 AI 供應鏈及算力基礎設施合作等議題進行深度交流。
- (三)為促進數位夥伴同盟，彰顯我國數位主權，我國已於 112 年 2 月成為自由線上聯盟（Freedom Online Coalition, FOC）國際組織觀察員，115 年 5 月及 7 月分別出席 FOC 策略協調會議計 2 次，並就推動 AI 等新興數位科技發展趨勢及

威脅進行交流，賡續強化數位同盟基礎，促進將我國數位發展重點議題納入國際數位相關聲明。

二、促進跨國公民科技發展：為建立多元共創開放環境，落實智慧國家願景，規劃與推動下述業務

- (一) 為落實智慧國家願景與開放治理精神，本部積極推動「公民科技試驗場域」計畫，促進政府與公民科技團隊協作開發創新數位服務，迄今已累計實作 8 項在地議題。115 年進一步以科技防災為主題，並與國家災害防救科技中心合作，邀集新北、基隆、苗栗及南投等 4 縣市提出弱勢機構災時回報、防災士資訊整合、志工與物資管理及災情通報等實務議題，目前正由公民科技團隊進行開發作業；另推動防災數位元件開發，逐步累積可供政府及社群再利用之防災數位工具，強化公私協力防災應用能量。
- (二) 我國公民科技能量廣受各國矚目，透過辦理防災積木元件創新競賽，匯聚科技社群創新能量，促進民間技術成果與政府防災需求接軌，強化公共服務之數位韌性與創新應用。另結合大型科技社群活動推廣本部數位憑證皮夾政策，於活動期間發行約 400 張數位憑證，擴大政策觸及與實際應用，促進科技社群與民眾對數位信任服務之認識。

三、規劃多元化數位驗證藍圖：為因應全球數位治理趨勢，創造韌性網路發展環境，規劃與推動下述業務

113 年開始建置符合分散式驗證及授權機制之數位憑證皮夾關鍵基礎建設，已於 114 年 12 月開放超商取貨試營運，115 年完成交通部駕照驗證卡、經濟部工商憑證電子卡、多所大學學位證書（台大、成大、台科大、雲科大及中國醫大）；私部門則與 3 大電信及統一和全家 2 大超商於 114 年 12 月

開放超商取貨試營運，後續也針對訪客、門禁、租車、求職等情境進行合作。APP 下載量已超過 13 萬次，並持續將該技術擴大國際合作事項，對接國際標準，促進全球憑證技術互通並得串接我國政府已發行之各式憑證，115 年亦逐步擴大應用場域及建立治理框架，以營造數位憑證生態系，也會透過社會溝通活動，提升民眾對數位憑證皮夾理解，希冀便捷我國民眾日常生活。

四、規劃淨零數位轉型政策：為加速實現我國 2050 淨零碳排目標，規劃與推動下述業務

- (一)營造國際對話與參與機制，115 年賡續辦理第 8 屆總統盃黑客松國際松，以「Digital Inclusion in the AI Era（數位共好：打造 AI 新未來）」為題公開徵件，致力打造永續數位典範。本屆於 115 年 5 月啟動活動宣傳，並對外公告徵件；7 月 2 日徵件記者會邀請到 15 國駐臺大使或代表現身支持，成功提升國際能見度與影響力。本屆收到逾百件提案，預計 10 月底前完成評選，12 月辦理頒獎典禮。
- (二)打造淨零數位典範，鑒於國際推動節能減碳數位科技以落實淨零永續發展之趨勢，本部參考國際標準 ISO 21031:2024 之軟體碳強度(Software Carbon Intensity, SCI)籌畫推動綠色軟體，並研擬適用於我國軟體產業之因應對策，115 年業獲得 9 家軟體業者共 18 款產品自願參與試評，預計將於年底完成彙整試評結果與產官學研參與經驗，選出標竿示範案例，滾動式調整政策推動路徑，以奠立後續綠色軟體及數位應用服務基礎。

陸、發展資料運用，打造資料創新應用生態

一、強化資料協作環境

推動政府資料開放，提升資料流通及格式品質，發展契合民間需求之高應用價值主題，並將平臺容器雲端化、平臺開源，構築多領域協作創新環境，重點如下：

- (一) 平臺運作使用人次持續成長：政府資料開放平臺集中列示各機關資料集，至 115 年 7 月底逾 5 萬項，瀏覽量達 1 億 9,941 萬人次、下載量達 2,274 萬人次。
- (二) 推動政府領域資料標準：本部推動各部會共同訂定政府領域資料標準，截至 115 年 7 月底已推動 26 項領域、2,157 項資料標準，開放資料集符合「機器可讀、結構化、開放格式」金標章比率超過 85%；資料集符合「領域資料標準」白金標章比率超過 50%。將完善資料流通利用環境，活絡整體資料經濟之發展。
- (三) 聚焦推動高應用價值主題：發展契合民間需求之高應用價值主題活化應用，主題包含氣候環境、災害防救、交通運輸、健康醫療、能源管理、社會救助、農業永續、空間資訊、企業永續等，計 9 項高應用價值主題，由 171 個機關，共開放 1,646 項資料集，截至 115 年 7 月底，該高應用價值主題專區總瀏覽量達 549 萬次。
- (四) 資料活化應用建構多領域協作環境：本部協同各部會持續開放具民生需求及潛在應用價值之資料，透過政府資料開放促進民間加值應用。例如「親子出遊趣」、「TaiwanLive／生活 168」、「ChargeSmith 充電地圖」等生活資訊服務，提供親子景點活動、餐飲住宿、交通動態、停車位，以及電動車充電站位置、充電槍數量與即時使用狀態等資訊，協助民眾即時掌握出遊、日常生活及電動車充電所需資訊。相關應用可支援休閒旅遊、行程安排及綠色交通等多元生

活情境，降低資訊取得門檻，並透過民間創新服務提升政府開放資料之應用效益與公共價值。

- (五) 精進資安防護，強化入侵檢測與防禦機制：「政府資料開放平臺」採雲原生服務，充分運用容器化技術與微服務設計，提升系統的彈性與擴展性。為進一步精進資安防護，強化容器安全性設置與入侵防禦，導入容器安全掃描機制與入侵威脅偵測防禦機制，並新增網頁置換通知功能，防範平臺遭惡意置換或竄改，同時建立平臺主機用量提醒機制，持續監控主機資源使用狀況，確保平臺的服務穩定性與安全性。
- (六) 促進開放資料轉化為 AI-Ready Data：為促進政府開放資料轉化為符合 AI 應用需求的高品質訓練資源，研訂 AI-Ready Data 詮釋資料框架指標指引，建立通用性之詮釋資料衡量架構，透過揭露資料來源與描述，包含資料收集方式、時間範圍、區域、類型等，減少資料於應用上可能存在的偏差，115 年優先導入高應用價值主題試行，推動機關提供高品質資料，增進跨域資料交換應用。

二、強化個人化資料自主運用機制（MyData）

打造個人化資料自主運用平臺，以「民眾自主同意、資料安全取得」為核心理念，強化各領域個人化資料自主運用，輔以資料自主應用資訊安全機制與管理制度，以提升資料運用價值，重點如下：

- (一) 服務效益與使用量顯著成長：MyData 平臺自 110 年 4 月正式上線，持續推動創新及多元的數位公共服務，提供民眾更便利的申辦服務。截至 115 年 7 月底已介接 84 個機關（包含中央及地方政府及金融機構），提供 1,224 項服務

申辦與資料下載，累計使用量已超過 1,216 萬餘次(較 114 年同期成長 1.3 倍)、會員數已突破 207 萬人；此外，平臺之身分驗證方式由保存民眾資料的權責機關依機敏程度決定，目前提供 10 種驗證方式，如自然人憑證、晶片金融卡、雙證件驗證等。

(二) 發展「主題服務」，貼近日常需求：MyData 平臺持續規劃推動主題式服務，以貼近民眾生活領域所需服務、豐富各類主題服務項目為目標，藉以擴大使用族群並優化民眾的使用體驗。目前平臺已涵蓋便利生活、生活扶助、家庭照護、社會福利、教育學習、稅務服務、婦幼關懷、消費金融及職能發展等 9 個主題。例如「生活扶助」主題類的「安居好室社會住宅申請」，累計使用次數已逾 2 萬餘次、「便利生活」主題類的「有條件式線上申換護照」，累計使用次數已逾 26 萬餘次。

(三) 跨機關推廣與地方政府交流：為促進地方政府介接 MyData，發展貼近在地民眾需求之線上服務，本部持續與各縣市政府攜手推動 MyData 便民服務，並赴地方政府辦理服務推廣說明會，透過雙方的實例分享與經驗交流，瞭解重點線上申辦服務及 MyData 介接情形，進而協助地方政府推動服務介接，例如新北市住都中心「新北市青年社會住宅線上申請」、新竹市政府「育兒津貼加碼補助申辦」、屏東縣政府「未滿一歲嬰幼兒營養補助」等，共同發展貼近在地需求的優質政府服務。

三、建構可信任之資料合規運作機制及創新環境

參酌國際最新資料政策及法制趨勢，完善資料創新相關推動制度，積極推動「促進資料創新利用發展條例」立法；

並發展政府資料匯流機制及開發資料隱私保護技術工具，推廣隱私強化技術多元應用，以厚植政府資料隱私技術韌性。重點如下：

- (一) 推行促進資料創新利用法制：為進一步擴大資料開放、共享及再利用，提升 AI 使用資料之可利用性，打造友善可信任之資料流通及創新應用環境，研訂「促進資料創新利用發展條例（草案）」，內容包含提升開放資料品質、促進政府機關間及產業資料共享、建立基於公益之資料利他環境、鼓勵機關提供激勵措施促進產業創新、強化資料創新利用諮詢機制等，草案已送行政院審議，持續依行政院審議意見與相關單位會商討論修正草案內容及辦理法制作業。
- (二) 發展政府資料匯流機制：採聯邦式系統設計，規劃發展政府資料匯流分析協作機制，運用動態假名化、k-匿名化、差分隱私等新興隱私強化技術，進行資料隱私保護處理，打造可信任且高效運作的政府資料共享環境。
- (三) 推廣隱私強化技術應用及國際合作
 1. 為推廣及激勵大專校院師生投入資料隱私保護技術發展與應用，培植隱私強化技術人才與實力，已於第 31 屆大專校院資訊應用服務創新競賽設置「資料隱私保護創新應用組」，並配合賽事主辦單位辦理推廣活動，強化賽事參與動能。
 2. 持續接軌國際最新隱私保護技術發展趨勢，於 115 年 8 月底完成新版「隱私強化技術應用指引」初稿，強化指引與國際規範及國家標準之一致性與適用性，以提升實務操作性，後續將諮詢專家學者意見，據以修正指引內

容，以提供機關導入相關技術之參考。

3. 為提升政府資料隱私技術韌性，刻辦理資料隱私保護技術工具開發，預計於 115 年底與醫療及學術機構合作完成場域實證，共同驗證技術可行性及保護力，以提供政府機關導入運用。

四、推動非政府及民間組織發展數據應用創新

為推動非政府及民間組織發展數據應用創新能力，並鼓勵建立跨域數據合作夥伴關係，擴大數據創新協作生態，重點如下：

- (一) 為強化國內非政府及民間組織之數據應用與創新能力，自 112 年 3 月起，依實務需求辦理多元數據培力課程，以提升數據素養與認知，內容涵蓋 AI 應用、AI 倫理與風險、數據知能、資料治理與資料盤點、服務與資料流程優化，以及循證治理的數據決策分析，截至 115 年 7 月底止，已辦理 34 場次線上與實體數據培力課程，參與組織達 470 家，參訓人數達 1,588 人次。
- (二) 為鼓勵非政府及民間組織活用數據創新公益服務，本部已完成為期 8 個月的第 3 屆 NGO/NPO 數據創新應用輔導，協助 3 家非營利組織及社會企業實踐資料創新解方概念驗證，亦提供 17 家 NGO/NPO 團隊專家諮詢服務，協助組織釐清資料癥結或指引資料創新方向，帶動非政府及民間組織發展數據應用創新。

五、建構臺灣主權 AI 訓練語料庫

為完善 AI 國家基礎設施，提供 AI 發展所需的環境，強化 AI 訓練語料基礎，重點如下：

- (一) 優先推動中央機關語料釋出，建立示範模式及標準作業流

程

為推動政府機關擴大文本資料開放，以及加速機關享有著作財產權語料釋出，本部研擬十大文本資料類型，作為政府機關盤點及釋出 AI 訓練語料之參考，並優先推動中央二級機關先行，建立示範模式及標準作業流程，作為後續擴大至地方政府及民間語料釋出之基礎。「臺灣主權 AI 訓練語料庫」自 114 年 12 月底上線，截至 115 年 9 月底，已超過 200 個政府機關投入，合計逾 5,000 筆資料集，超過 24 億 tokens 語料規模。

(二) 持續擴大語料募集範疇，逐步納入地方政府及民間語料

將持續推動地方政府與民間單位共同參與，已召開多場地方政府、民間單位之說明會及研商會議，促進交流與討論，各地方政府刻正進行語料盤點與上架，逐步擴充語料來源範疇。後續將持續與文化、教育、客家、原住民族等領域主管機關合作，推動各該領域提供具臺灣文化、社會及語言特色之高品質語料，逐步形成可長期運作之臺灣主權 AI 語料生態，支援我國主權 AI 發展。

(三) 強化公私部門語料釋出動能，輔導與獎勵並進

1. 推動政府機關釋出高品質正體中文語料，召開多場研商會議、說明會及實作工作坊，協助政府機關上架語料，透過具體操作手冊與實務輔導，持續強化各機關語料釋出動能；針對民間語料募集，舉辦座談會，邀集民間相關單位就語料募集、授權模式及應用需求共同交流與討論，瞭解民間內容釋出之需求、疑慮及合作條件，作為後續完善語料募集機制及推動公私協力之參考。
2. 為持續強化政府機關及民間語料釋出動能，本部刻正規

劃相關語料提供獎勵機制，透過公開表揚或其他適當方式予以鼓勵，期引導各界積極盤點及釋出更多具臺灣文化特色之高品質語料，持續擴充語料庫內容。

六、推動各部會設立資料長

依行政院 115 年 6 月 23 日國家人工智慧戰略特別委員會會議結論，推動各部會設置「資料長」，以推動政府資料開放、擴大政府資料共享、擴大 AI 訓練語料釋出為優先任務，加速資料創新利用發展；並於 115 年 10 月 7 日由行政院召開「主權 AI 與資料治理專案會議」第 1 次會議，邀集各部會資料長就 115-116 年度重點工作規劃、擴大推動主權 AI 訓練語料、國內整體算力供需管理機制，以及政府導入 AI 法規調適規劃等議題進行研商。

柒、加速產業數位創新與轉型，帶動數位相關產業發展

一、布建 AI 算力資源，推動資服產業「產品化」

本部自 113 年建置 AI 算力池（包含 NVIDIA 及 AMD），提供資服業者申請使用，協助 AI 新創團隊進行模型訓練及技術開發，至 115 年 9 月已累計協助 320 家業者使用，且已累計開發至少 266 個模型與 AI 應用服務，其中 80 家資服業者完成 AI 服務產品化，應用涵蓋醫療、防災、金融、製造、零售、教育及公益等領域，不僅加速 AI 應用服務的開發，亦有效降低研發成本，讓業者能更快速將創新應用服務推向市場。

115 年預計擴充 AI 算力，累計達到 120 片 GPU。另本部配合金管會修法，訂定保險業投資 AI 算力屬策略性產業、基礎建設或公共投資之明確定義（如 1,000 PetaFLOPS 以上及對外開放使用率超過 50% 等），以鼓勵保險資金投入 AI 算力公共投資，公私協力共同發展 AI 產業。

二、認定標準與多元培育模式並進，完善 AI 人才發展生態系

(一) 強化 AI 人才認定標準，串聯生態系夥伴加速供需媒合

1. 因應 AI 應用需求日增，為協助產業辨識 AI 人才與能力，本部發布「AI 產業人才認定指引」，提出三種「AI 人才分類」及五種「AI 能力類型」，以對接產業實際用人需要，並彙整相關認證及課程資訊，供各界參考運用；人事行政總處「AI 公務人才發展辦公室」亦將本指引納入公務人員培訓參考。
2. 115 年 5 月因應「人工智慧基本法」與 AI Agent 等技術趨勢，將「AI 治理素養」與「AI 協作與開發」納入指引，預計於 115 年 11 月辦理第 4 次更新。
3. 已累計串聯 25 個生態系夥伴並盤點 15 項認證項目，未來將持續與民間認證、培訓單位與人才媒合平臺進行合作，彙整相關認證及課程資源供各界參考運用，營造正向循環的 AI 人才發展生態系。

(二) 鏈結產業創新需求，培育多元數位人才

針對產業需求迫切之 AI 人才，本部建構了從「向下扎根」到「在職賦能」的完整培育體系，強化學界與產業界的鏈結。包括：

1. 新世代 AI 人才：培育高中職生應用 AI 能力，截至 115 年 9 月共計 677 名完成線上 AI 課程，全年預計累計達 1,000 人。
2. 跨域 AI 應用人才：結合大專院校培育跨領域 AI 應用人才，截至 115 年 9 月培訓 595 人，全年目標 500 人，並輔導取得「AI 產業人才認定指引」認列之專業證照以銜接職場。

3. 資服開發人才：透過 Vibe Coding 課程協助掌握 Claude、Codex、GitHub Copilot 等各類 AI 開發工具，培養自然語言程式開發與 AI Agent 建構能力，截至 115 年 9 月培育 896 人。
4. 產業應用人才：經由出題解題機制培育產業 AI 應用人才，截至 9 月辦理 27 場工作坊、培育 1,222 人，並彙整 67 項產業需求，串聯業者導入 AI 解方。
5. 數位創新人才：以數位創新與新創企業需求為導向推動共育模式，114 年合作 19 家企業培育 76 人，並促成 35 人留用；115 年與 19 家企業合作，完成培育 80 人，並促成 55 人留用，116 年預計培育至少 70 人。

(三) 健全地方數位驗證，培育偏鄉在地種子人才

本部為培養偏鄉在地數位種子人才，透過串連偏鄉在地組織與數位人才，針對數位發展分群二、三、四級地區場域問題，提出數位解決方案，並結合陪跑教練輔導機制及線上學習資源。自 113 年推動以來，已經累積完成 34 件在地數位解方驗證案例，培育 284 位偏鄉在地數位種子人才，並協助 16 個縣市偏鄉場域完成數位解方導入。115 年持續推動相關計畫，預計培育至少 90 位偏鄉在地數位種子人才，促進偏鄉在地數位化應用的長期發展。

(四) 延攬國際數位人才來臺，驅動產業創新與國際化

為改善國內 AI、資安與軟體高階人才缺口，本部自 112 年公告增訂「外國特定專業人才具有『數位領域』特殊專長」，藉由吸引具備實務技術與國際經驗的海外專家來臺，加速國內產業升級與新創國際化。截至 115 年 9 月，數位領域就業金卡核發張數已逾 1,558 張。未來將持續延攬具

代表性國際專業人才，並優化留臺配套，奠定臺灣在國際數位經濟中的核心競爭力。

三、推動 AI 應用與數位產業創新發展，健全多元應用生態系

(一) 以 AI 場域驗證與示範案例帶動應用擴散

1. 落地實證創造商機，聚焦三大領域打造應用典範：為強化產官學研合作，本部持續推動「AIDemo Day」媒合機制。自 113 年至 115 年 9 月底，已吸引 418 家企業參與，成功促成 38 件跨業導入案例，帶動潛在商機達 1,547 萬元。115 年進一步以「場域導向、產業聚焦、區域串聯」為核心，鎖定健康照護、智慧製造、農畜牧等產業辦理 12 場交流活動，並結合徵件與媒合機制引導 AI 技術進行場域實證，打造產業應用典範。
2. 情境體驗加速供需對接，精準轉化技術為實質商務合作：115 年辦理「AI 任意門」產業需求與技術交流系列活動，依產業痛點每場邀集 8 家 AI 資服業者參與，透過「依實際情境體驗 AI 工具」的互動模式，協助國內資服業者優化 AI 工具並推廣各產業領域企業，由體驗進一步轉化為訂閱、導入或合作；截至 115 年 9 月底，已有 67 家需求企業實質訂閱或簽訂合約。

(二) 以百億元基金帶動民間資本，活絡 AI 新創投資動能

本部推動之「加強投資 AI 新創實施方案」已獲國發基金 100 億元支持（期程 10 年），並於 114 年 3 月起受理申請。截至 115 年 9 月底，已經完成 4 梯次搭配投資人遴選共計 46 家，並核定投資國內 AI 新創及數位經濟相關產業計 10 家，方案投資金額約 2.55 億元，帶動民間投資約 5.7 億元。後續將結合 AI 產業輔導政策，為國內 AI 新創挹注

成長動能。

(三) 深化場域實證及接軌國際，加速 AI 應用落地

為促進產業 AI 導入與數位轉型，本部透過技術盤點及國際交流等面向，持續整合各界資源，並推動相關計畫，擴大產業應用 AI 方案於各產業之導入與應用。

1. 擴大技術供給與場域實證，加速解決方案規模化落地：
為降低企業導入 AI 門檻，本部已輔導 156 家廠商通過 251 項 AI 技術服務能量登錄項目，取得 2 年期能量登錄證書；更透過辦理「AI 新銳選拔」媒合大廠需求與跨界團隊，經專業委員遴選 43 個團隊進行 AI 創新解方共創與驗證，預計產出至少 10 項具潛力案例；其次，推動「企業 AI Agent 產品化示範案例」，由專業委員審查後協助 12 家資服業發展 AI Agent 產品，並導入 25 個企業進行落地實驗，以達成產業擴散。此外，辦理「2026 GenAI Stars 百工百業應用選拔」，透過廣徵、輔導與推廣三階段加速規模化，115 年共 275 隊報名、25 組晉級決審，後續將進行深度輔導，預計促成至少 20 組解決方案於企業內部成功落地應用。
2. 舉辦國際展會帶動商機鏈結，推升臺灣 AI 產業全球能見度：為展現臺灣 AI 實力並促成實質商機，本部於 115 年 7 月 30 日至 8 月 1 日辦理「AI WAVE SHOW 2026」，匯聚日本軟銀、台智雲、中華電信、Raccoon AI、台塑、甲骨文、AMD、台灣微軟、西門子等逾 200 家國內外業者、觀展人次達 5.2 萬，並成功創造約 3,000 次商洽機會，深化供應端與應用端之鏈結。此外，本部持續與國際指標大廠聯手合作，已於 115 年 9 月 21 日至 9 月

23 日攜手台灣微軟舉辦「DevDays Asia 2026 亞太技術年會」，透過技術活動串聯在地社群與開發者，創造共計 115 萬人次的線上交流、線下 8 個技術社群、600 位以上開發者齊聚一堂，首創「政府專軌」匯聚 134 位代表探討智慧公部門與 AI 治理，成功串聯在地社群與開發者，持續擴大臺灣 AI 產業的國際影響力。

(四) 輔導資服業者發展 AI Agent 產品服務，促進營收成長

1. 本部推動臺灣資服產業由專案開發邁向產品經營，辦理工作坊促使軟體及資服業者運用 AI、AI Agent 等創新技術，發展具市場競爭力及可規模化推廣之 AI 產品與服務，協助百工百業導入智慧應用，加速數位轉型，提升營運效率與產業競爭力。115 年持續推動 AI 創新服務研發主題型計畫，聚焦 AI、AI Agent 等智慧應用與產品服務，並透過 Demo Day、成果展示及商務媒合等多元推廣機制，加速 AI 技術擴散及創新方案落地。預計推動至少 10 項 AI 服務產品方案，帶動資服業者新增投資 6 億元，持續提升我國資服業 AI 產品創新及市場拓展能量，並輔導 4,200 家次中小企業導入 AI 應用，促進產業營收成長達 7 億元，強化我國數位產業競爭力與產業轉型動能。
2. 在軟硬體融合與邊緣運算趨勢下，本部以「促進 AI Agent 產品化、帶動資服軟體業升級轉型」為核心目標，發揮我國資通訊硬體產業優勢，建置符合國際標準的 AI-to-Network 開發與合規驗證環境。積極引導資服廠商投入垂直場域 AI Agent 開發，並打造包含電信 API 服務、AI-RAN 及 AI 算力等工具調度之試驗沙盒與協

作應用。同時，鏈結國際大廠資源辦理實作工作坊，降低業者研發門檻，加速 AI 應用服務落地與商業化；並透過照護、大型展館、智慧防救災，以及產業建築與工廠之智慧電能調度及能耗管理等 5 大場景案例共創，推動 Edge AI Agent 協作創新應用之實地測試。

3. 研發符合國際標準的 MCP（模型上下文協定）與 AI Agent 模組化工具，緊扣產業痛點需求，深入垂直領域進行應用驗證。透過試行合規驗證機制，將技術成果轉化為可上架、可部署的軟體產品；並搭配競賽實作與社群交流，逐步建構與完善我國 AI 代理人的產業發展生態系。

（五）完善 AI 評測制度，助攻業者發展可信任 AI 解決方案

1. 為完善我國 AI 評測環境與驗證機制，本部持續維運 AI 產品與系統評測中心（Artificial Intelligence Evaluation Center，以下簡稱 AIEC），推動具在地化特色的評測項目與工具（如繁體中文語境），提供第三方評測服務，協助業者的 AI 應用產品對齊臺灣市場需求，截至 115 年 9 月底，累積完成業者送測的產品與模型共計 144 項。
2. 發展臺灣主權 AI 基礎評測指標，包括：高中學測國文與社會，以及臺灣價值題型，另就國內外開源與指標語言模型進行測試，作為各界建構在地模型或調校國際模型之參考依據，截至 115 年 9 月底，累計完成測試與公布 203 項國內外開源語言模型的基準評測結果。
3. 因應《人工智慧基本法》，本部與相關部會協作（如陸委會、金管會、衛福部、法務部、教育部等），由部會

依主管目的事業提供之專業題庫，由 AIEC 進行開源/指標模型評測基準研究 (benchmark)，透過客觀、科學化的數據，作為臺灣主權 AI 發展、AI 治理與資料建置重要參考。

4. 在國際接軌方面，採雙軌並進策略，串接歐洲（如法國 LNE）與美國（如 NIST、UL Solutions）的評測體系或驗證機構，協助廠商對齊國際標準與合規要求。與法國 LNE 合作，針對雙方 AI 理解方言/諺語能力的評測項目研究成果，預定共同進行國際發表。

(六) 推動 5G 專網垂直領域驗證，加速產業轉型

1. 截至 115 年 9 月底，本部依「行動寬頻專用電信網路設置使用管理辦法」辦理，累計完成審查 166 案，其中已經核發行動寬頻專用電信網路執照 147 案，持續協助潛在案件轉化落地，相關應用包含石化廠區、儲油場等場域，應用情境涵蓋 AI 影像辨識、無人自走車巡檢、環境感測、人員定位及即時通訊等智慧工廠運用。如中油公司結合室內攝影機與室外無人自走車，將巡檢影像及感測資料回傳 AI 系統分析，於發現異常時即時通報，提升高風險場域之工安管理效率及災防應變能力。
2. 與公協會及系統整合商(SI)合作持續落地擴散前期 5G 成熟技術，累積整合 20 家以上通傳應用方案供應商，發展共通應用服務設計規格，並推動 B5G/Pre-6G 通傳創新應用的深耕與實證，研發建構通感算網路與應用整合平台，透過導入 AIRAN、5G/5G-A 專網、次世代通感融合 ISAC 及邊緣 AI 等前瞻通傳科技，於「沉浸式智慧互動（展館）」、「智慧醫療（ICU/急診）」與「智

慧化港口碼頭」等垂直指標場域進行實證，積極引導電信與網通業者深耕 AI 內容訂閱與專業通感服務等新型態商業模式。同時提升資服業者的整合服務能力，驅動 SI 角色升級為「場域需求定義者」與「高價值通感服務供應商」，打造 6G 時代全自動化網路部署與自主營運的環境基礎。

(七) 推動新聞業與大型平臺分潤機制，健全媒體生態系

為落實政府對新聞產業之支持，本部規劃推動「臺灣優質媒體共同分潤平臺」，作為先行策進作為。同時，本部持續扮演溝通平臺角色，促進新聞媒體與數位平臺間的合作與對話，鼓勵並支持新聞產業探索多元化發展路徑；亦引導國際資源與產業對接，例如 Google 與金融時報共同推動「台灣 AI 實驗室」，成功協助 8 家新聞媒體建立 AI 發展願景與倫理準則，並探索 AI 實際應用情境。

(八) 深耕關鍵資安技術，接軌國際信任供應鏈

1. 為加速後量子密碼（PQC）關鍵技術研發與國產化，本部協助業者於 115 年 6 月順利量產首批 15,000 顆國產後量子密碼晶片。該晶片支援美國國家標準暨技術研究院（NIST）的 FIPS 203、204 及 205 等三大標準，可廣泛應用於網通、安控及資安設備，落實關鍵資安晶片自主化。此外，本部亦積極前瞻布局，投入 NIST 最新選定之 HQC 演算法矽智財（IP）研發，協助國內產業率先掌握新世代核心技術，厚植產業競爭力。
2. 在產業推廣與落地應用方面，本部透過補助計畫引導國內業者研發 PQC 解決方案，並優先導入高科技園區、醫療與金融等關鍵基礎設施以建立典範案例。為加速

產品上市，本部自主研發「晶片安全」與「場域應用安全」檢測工具，協助廠商預先補強漏洞，成功降低 30% 檢測時程與 50% 重複送測成本。另本部已輔導 2 家國內醫學中心進行後量子遷移實證，並持續推動金融與醫療體系進行密碼資產盤點，提升我國關鍵產業抗量子攻擊之韌性並與國際標準接軌。

3. 為回應國防資安技術發展需求及強化國內關鍵技術自主能力，本部自 112 年起推動軍民通用資安技術研發，截至 115 年 6 月底，已透過補助機制累計推動 44 案計畫。其中，115 年核定 9 案計畫刻正辦理簽約及研發執行階段，後續將持續推動技術輔導、成果驗證及交流展示作業，促進研發成果與國防單位、產業界及潛在應用場域對接，以及配合國防部「產業化圓桌會議」研議 116 年國防資安需求，作為後續徵案及技術布局依據。
4. 因應日益嚴峻的網路威脅，本部透過補助機制與跨域合作，深化我國整體產業資安防護能量。115 年本部積極推動具國際供應鏈能量之場域業者與本土資安廠商合作，共同研發符合實務需求的「零信任解決方案」，並帶動上下游供應鏈協同導入。此外，本部持續與公協會籌組「產業資安強化工作小組」，115 年媒合 90 家企業與資安顧問對接，運用資安評級問卷與網站曝險分析等工具，精準協助企業掌握防護弱點，除可有效提升中小企業資安意識與韌性，更為本土資安產業創造實質市場商機。
5. 為協助我國資安產業掌握國際商機，本部透過辦理國內展會與海外拓銷活動協助我國資安產業拓展全球國

際市場。國內部分，本部於 115 年 5 月 5 日至 7 日「臺灣資安大會」中打造臺灣資安館，輔導 59 家本土資安廠商展示自主研發的解決方案，於展會期間辦理亞洲買家參訪暨媒合活動，邀請來自星、馬、泰、越等 27 家企業來臺，對接 85 場媒合活動；此外，本部亦同步帶領臺灣資安廠商走向國際市場，115 年上半年已累計率領 17 家本土資安廠商參與美國 RSAC 及日本 IT Week 等國際指標型展會並設置臺灣資安館，其中美國 RSAC 更為我國首度設立專館，提升臺灣資安品牌能見度與競爭力，並為本土資安產業拓展海外商機奠定基礎。下半年除持續深耕既有資安產業市場外，另於 10 月 5 日至 8 日帶領我國 6 家資安業者赴荷蘭參與 ONE Conference 資安論壇，並與當地業者辦理媒合交流，擴大我國資安產業在歐洲市場的布局。

6. 為確保我國高科技與國防產業與國際標準接軌，本部積極完善半導體與晶片安全之認證生態系。在半導體設備資安方面，繼 114 年底發布 SEMI E187 驗證制度後，115 年已成功輔導資策會與工研院成為首批具 ISO 資格的檢測實驗室，並將於年底成立驗證機構、頒發全球首批驗證標章，宣告標準實務落地；同時，本部亦輔導建置國內晶片安全檢測實驗室，成功協助晶片產品 2 案次通過標準檢測。此外，為協助國防及關鍵產業接軌美國 CMMC 規範，本部持續深化臺美政策交流，推動成立 CMMC 第三方評鑑機構 (C3PAO)，並輔導 9 家航太工業、電子設計與精密加工等關鍵業者導入合規，提升我國供應鏈的國際信任度與競爭力。

四、健全數位防詐治理，構築可信任產業生態

(一) 強化跨域聯防，提升「網路詐騙通報查詢網」防詐效能

1. 「網路詐騙通報查詢網」，自 113 年 9 月 30 日至 115 年 9 月 30 日止，共有 7 萬 5,613 位民眾下載使用，3 萬 9,254 人使用 APP 通報案件，總計通報 148 萬 7,699 則疑似詐騙訊息。其中 79 萬 9,828 則經由被偽冒公眾人物本人或主管機關確認為詐騙訊息，平均每個月超過 3 萬則詐騙訊息依本部通知要求下架。
2. 本部自 112 年 12 月起推動「詐騙樣態分析」，於網路廣告平臺掃描高風險詐騙案件並應用於「網路詐騙通報查詢網」。截至 115 年 9 月底，整體高風險金融投資廣告掃獲案件數已自 113 年單週最高 7 萬 7,484 件下降至 115 年 9 月平均每週 1,041 件，降幅達到 99%；身分冒充詐騙廣告掃獲案件數已自 113 年單週最高 3 萬 8,139 件下降至 115 年 9 月平均每週 727 件，降幅達到 98%。
3. 為擴充 AI 掃描機制之應用範疇，115 年已陸續與趨勢科技、Gogolook、中華電信、台灣大哥大、工研院、資安院及集仕多等跨領域產業與研發機構建立合作機制。目前 AI 掃描量能已全面涵蓋 Meta、Google、LINE 及 TikTok 等四大網路平臺業者，持續提升數位聯防效益。
4. 已結合民間業者（中華電信、台灣大哥大、遠傳電信、趨勢科技及 Gogolook）網路安全技術，在完成封鎖網域行政程序前，於用戶端即時彈出警示頁面，將防護模式升級為「發現、通報確認、同步警示與下架」。

(二) 健全網路平臺防詐治理，降低詐欺廣告與涉詐帳號危害

1. 本部依《詐欺犯罪危害防制條例》授權訂定子法並公告

納管 4 家網路廣告平臺業者共 7 個平臺 Google(Google、YouTube)、LINE(LINE)、Meta(Facebook、Instagram、Threads)、TikTok (TikTok)，並持續關注詐欺風險變化、網路廣告平臺業者規模更迭及詐騙目標轉移可能，檢討更新納管業者名單，以降低詐欺廣告擴散及移轉。

2. 4 家納管業者皆依《詐欺犯罪危害防制條例》規定訂定詐欺防制計畫及執行身分驗證相關措施，並於 114 年 12 月發布詐欺防制透明度報告，以利公眾瞭解業者對於詐欺所採取之因應策略及相關措施落實情形，依據 4 家業者發布之透明度報告統計，依通知下架 14 萬 6,638 則廣告、依法停權 10 萬 4,785 個涉詐帳號。
3. 115 年亦持續輔導業者落實法遵，於 2 月 9 日、3 月 25 日、5 月 22 日邀集 4 家業者召開研商會議，請業者視詐騙風險變化滾動式檢討修正防詐作為，業者均向本部表示願意主動配合防詐政策，自律精進防詐計畫及滾動式檢討相關措施；並於 6 月份分別輔導業者防詐計畫更新方向、透明度報告內容及成效呈現方式等。本部將持續透過定期會議請業者精進防詐作為，期有效降低網路詐欺風險。
4. 此外，倘網路廣告平臺業者有違反《詐欺犯罪危害防制條例》之情事，均依法裁處。114 年針對 Meta 已裁罰 4 次，合計罰鍰新臺幣 1,850 萬元；115 年針對 Meta 已裁罰 2 次，合計罰鍰新臺幣 1,000 萬元，並持續審理相關案件，凡業者有違反情事，一律依法嚴懲辦理，以督促業者恪遵法規，確實履行廣告資訊揭露與源頭防詐管理責任。

(三) 強化第三方支付實質監理，降低洗錢與詐欺風險

1. 本部建立「提供第三方支付服務之事業或人員洗錢防制及服務能量登錄制度」(下稱三支能量登錄)，並公告提供第三方支付服務的事業或人員洗錢防制及服務能量登錄辦法(下稱洗錢防制及服務能量登錄辦法):
 - (1) 本部與金管會達成部會聯防共識，未完成三支能量登錄的第三方支付服務業者(下稱三支業者)，銀行在其開戶時就不會受理；若是銀行現有客戶，未申請三支能量登錄通過的三支業者，銀行將會視為高風險不再提供虛擬帳戶服務；此外，亦與經濟部達成部會聯防共識，四大超商業者於合作契約簽訂前審核檢視，如為三支業者應檢附三支能量登錄通過的證明文件。
 - (2) 另依據法務部修正公告《洗錢防制法》第六條規定，三支能量登錄已屬類許可制度，針對未完成能量登錄的三支業者不得提供第三方支付服務。截至 115 年 9 月底，通過能量登錄業者 53 家，廢止登錄 26 家，有效期屆滿失效 2 家。
2. 為精進三支能量登錄，防範犯罪集團進入產業並取得能量登錄資格，本部已經將能量登錄作業升級為「事前、事中、事後」三階段控管
 - (1) 事前防範：申請登錄者須檢附公司、負責人、合夥人及實質受益人的聲明書，確認未違反《提供第三方支付服務之事業或人員洗錢防制及服務能量登錄辦法》第 3 條規定。
 - (2) 事中查證：發函法務部查證聲明內容真實性；辦理

現場審查，確認實際營運狀況；同步啟動企業徵信作業。

- (3) 事後查核：與法務部調查局、財政部國稅局辦理跨部會聯合查核，要求業者落實內控制度、內部稽核及客戶身分確認(KYC)。113 年及 114 年對通過登錄業者均達成 100%查核覆蓋率。114 年共查核 57 家、廢止登錄 3 家、裁罰 10 家，裁罰金額合計新臺幣 283 萬元。115 年截至 9 月底，已查核 39 家。
3. 已經建置「第三方支付服務業虛擬帳號查詢平臺」協助檢警調快速查找虛擬帳號所屬第三方支付業者。自 113 年 3 月上線，金流圈存時程由 7~30 天縮短至 1~3 天。截至 115 年 9 月底，累計查詢約 4 萬 4 千餘筆。
4. 已經建置「第三方支付服務業產業聯防平臺」，並於 113 年 8 月 30 日上線。該平臺透過與產業共享情資，得以快速識別並防堵來自高風險商家的詐騙行為，協助三支業者落實聯防詐騙。平臺亦提供網頁偵測工具，協助業者落實審查客戶網站(URL)義務及確認實質交易內容，以降低三支業者遭利用於犯罪活動的風險。
5. 透過法制明確化、跨部會聯防與高強度查核，三支能量登錄制度已經從形式審查轉為實質管理，本部將持續滾動檢討制度與查核機制，確保第三方支付服務不成為詐騙與犯罪工具。115 年將持續針對第三方支付查核機制，透過法遵科技與情資聯防的深度整合，全面提升監理效能。

(四) 強化遊戲點數跨域聯防，攔阻異常交易

1. 自 111 年 8 月起至 115 年 9 月底，本部邀請行政院洗錢

防制辦公室、臺灣高等檢察署、內政部刑事警察局與五大遊戲點數業者召開 30 場阻詐執行成效會議，透過跨部會聯防機制檢視阻詐成效並要求業者自律。

2. 輔導業者配合提出阻詐措施，包含「點數業者端」導入 FIDO 驗證機制、「線上遊戲端」監控異常儲值情形、「四大超商端」依營業額規模進行限額並設置警語、「線上客服端」增加客服處理人力等，另輔導業者推出延遲入點與線上鎖卡機制，推出後至 115 年 9 月底已經凍結異常帳號數逾 7 萬 1,440 件，攔阻總金額逾新臺幣 4 億元。

(五) 落實電商個資法遵與違禁品聯防，提升平臺治理效能

1. 本部積極辦理電商業者行政檢查，檢視業者個資保護及資安防護落實情形，已於 111 年 12 月至 115 年 9 月底，針對重大矚目、高風險、保有大量個資的業者累計辦理 68 家次行政檢查。另針對電商業者辦理個資防護及法遵輔導系列活動與輔導業者進行個資健檢，以強化從業人員之法規認知與應變能力、提升產業資安防護韌性以及強化電商個資保護。
2. 為協助各主管機關處理違禁品下架事宜與強化業者法遵意識，本部定期邀集作用法之目的事業主管機關、3 大電商公協會、4 家大型 C2C 電商平臺業者及 4 家納管之網路廣告平臺業者等，召開「網路平臺刊登或販售違法商品下架處理聯防平臺」聯繫會議，自 113 年 11 月起至 115 年 9 月底，共計召開 9 次會議，處理 75 項提案，使平臺業者依各部會提供之違法商品資訊，進行商品上架審核、上架後巡查及違法商品下架處理，有效

提升違禁品下架處理效率。

(六) 完善電子簽章法制與能量登錄機制，促進普及與應用

1. 本部已經於 113 年完成《電子簽章法》及相關子法的修正與訂定，包括《電子簽章法施行細則》、《數位簽章憑證實務作業基準應載明事項》及《外國憑證機構許可辦法》等，使法制架構更符合實務運作需求，並擴大電子簽章應用範疇。
2. 為持續輔導及協助各機關因應《電子簽章法》修法後的數位相關支援，並鼓勵各機關運用數位簽章，提升服務便捷與效能。本部自 113 年底公告電子簽章解決方案服務能量登錄制度，截至 115 年 9 月底，已經核准 10 家廠商通過登錄，並公布於本部數產署官網「電子簽章法規」專區，期藉由具公信力的登錄機制，逐步完整國內的電子簽章產業地圖，並促進產業發展與跨界採用。

捌、建構智慧化資安治理與跨域資安防禦生態系，推動資安法規調適與資安人才培力

一、推動第七期「國家資通安全發展方案（114 年至 117 年）」，建構信賴安全之數位社會

(一) 因應地緣政治衝突與日益嚴峻之資安威脅，第七期「國家資通安全發展方案（114 年至 117 年）」旨在實踐「強化全社會資安防禦韌性」、「豐富資安產業生態系」與「構築新興科技防禦技術」三大目標，並採「化被動為主動」之防衛模式，結合公私協力與新興科技導入，厚植國家資安防護能量，方案四大推動策略重點如下：

1. 全社會資安防禦：輔導政府機關導入零信任架構，增強政府機關防護能量及應變機制；並系統化培植高階與工

控場域資安實戰人才，結合防詐與媒體素養宣導，全面提升全民防護意識，建構堅實之全社會防護網。

2. 提升關鍵基礎設施資安韌性：建置關鍵基礎設施資安防護體系，並針對能源、通訊等九大關鍵基礎設施領域落實工控防護基準與治理成熟度評估；另引進主動威脅監控與自動化情資分享以建立跨域防護，定期辦理實地稽核與跨國網路攻防演練(CODE)以強化實戰應處能量。
3. 壯大我國資安產業：推動物聯網裝置與數位服務資安檢測機制接軌國際標準，精進政府採購之供應鏈風險管理，並積極扶植資安新創及研發零信任物聯網安控產品，以及推動具備國際競爭力之資安解決方案。
4. AI 新興資安科技應用與合作：研發 AI 主動式防禦與威脅情資自動化分析技術，建置高可視性國家資安治理情資平臺以精確掌握威脅態勢，推動可信任 AI 評測制度並研析無人機、後量子密碼等前瞻科技，持續深化國際交流以落實跨國聯防。

(二) 本方案 114 年各項重要績效指標均已如期如質達成，並於 115 年 7 月 9 日「國家資通安全會報第 1 次委員會議」進行成果報告。具體成效包含培訓政府機關專職資安人力逾 2,000 人次，並落實關鍵基礎設施核心系統之試行檢測與標準作業流程建置；同時，促成我國資安產業年產值達新臺幣 912.4 億元，另成功開發骨幹網路 AI 威脅預警與攻擊酬載來源鑑定技術，從技術源頭構築主動防衛基石。

二、優化資安聯防機制，提升國家資安防護

- (一) 透過國家資安聯防監控通報機制，分享國內外資安訊息、漏洞通告及資安監控資訊、潛在資安威脅、惡意電子郵件、

惡意程式及網路黑名單等情資，並積極辦理資安事件協處、協助外交部外館資安健檢等作業，並於我國重要活動期間，執行資安警戒專案，重點強化國家資安防護作業。

- (二) 持續推動關鍵基礎設施領域之工控系統資安防護基準，目前已核定能源、水資源、交通、緊急救援與醫院，及通訊傳播等 45 領域之防護基準。發展並精進工控領域資安治理成熟度評估機制，每年依最新法遵規範或機關回饋建議，檢討、調修評估檢核內容，並透過評估結果分析，綜整 CI 領域共同發現事項提供機關資安強化精進方向。
- (三) 為即時攔阻惡意網路連線並提升政府資安防護能量，已於 114 年推動「黑名單自動化部署服務」，協助政府機關定時自動化更新 IP 及 DN 黑名單，截至 115 年 9 月底，已有 274 個機關申請黑名單自動化部署服務，強化政府機關之資安防護措施。
- (四) 持續推動公務機關導入零信任網路架構，並提供零信任架構產品功能符合性驗證流程，鼓勵產業發展合規產品，已有 40 項產品通過驗證。
- (五) 持續深化與全球理念相近國家合作夥伴關係，114 年 11 月辦理前瞻資安探索會議，與 10 餘國資安專家學者，就資安韌性、威脅應變、新興科技等資通安全與政策治理議題進行交流，115 年 5 月與巴拉圭及波蘭兩國簽訂資安合作備忘錄，奠定臺巴與臺波未來深化合作基礎。
- (六) 積極運用先進 AI 檢測漏洞挖掘工具，並成立「先進 AI 資安風險因應小組」，推動公務機關及國家關鍵基礎設施重要系統導入先進 AI 技術，加速漏洞挖掘及修補，強化整體資安防禦效能。

三、深化資安稽核與攻防演練，提升整體防禦能量

- (一) 參考當前威脅情勢，調修年度資安稽核重點，邀請產官學研外部專家協助檢視受稽機關法遵落實情形及整體防護作為，115 年預計完成 30 場資安實地稽核；此外，為了減少傳統稽核人力與時間成本，115 年將運用 AI 技術，試辦 30 場 AI 輔助場外稽核作業，擴大稽核範圍，提升稽核效率。截至 115 年 9 月底，已完成 25 場實地稽核及 30 場 AI 輔助場外稽核作業。
- (二) 辦理 115 年政府機關網路攻防演練，包含社交工程演練、資通系統實兵演練等，強化機關資安事件應變、復原及管控等能力，預計演練對象包含中央及地方等 72 個機關，同時擴及關鍵基礎設施提供者，以強化整體資安韌性。
- (三) 為減少各機關辦理委外廠商稽核所增加行政成本，並解決資訊服務業者因面臨不同機關頻繁稽核，造成冗長作業時間與人力資源成本等問題，115 年由本部資通安全署主政，協同行政院所屬機關推動受託者資通安全聯合稽核計畫，115 年預計完成 16 家重要資訊廠商實地稽核，截至 115 年 9 月底，已完成 16 場次聯合稽核作業，已全數完成。

四、增進資安職能培力，強化人員資安意識

- (一) 攬才：推動於公務人員高等考試三級考試資訊處理職系增設資通安全類科，透過考試遴選制度增加政府機關選才管道，提供資安人力穩定來源；推動「政府資安人力職能轉換訓練」，協助各機關現職未具「資訊處理職系」且「有意願」者，參加該職系專長訓練，於取得資訊處理職系資格後，能優先投入資安工作。截至 115 年 9 月已投入資安工作約計 171 人。

(二) 育才：本部資通安全署為完善資安人才培訓生態系，建立以需求為導向之資安人才培訓體系，115 年持續辦理資安職能訓練課程，截至 9 月底已培訓逾 1,778 人次；另 115 年辦理資安長共識營、資訊（安）主管資安研習、資安人員專業訓練、政府資安防禦實戰菁英班等，累計培訓逾 2,100 人次。

(三) 留才：為利延攬及留任公務機關資安專業人才，本部資通安全署業辦理重點資安業務機關資安人員增支專業加給，適用機關自 115 年 8 月 1 日起擴增至 56 個，包含全部資安責任等級 A 級公務機關及直轄市政府所屬資訊機關；此外，並設置績效評核獎勵機制，期藉由鼓勵績效優良之公務機關及資安人員，提升資安人員士氣與整體待遇，吸引優秀資安人才投入公務機關服務。

五、精進調適資安法規，完備資安基礎環境

(一) 資通安全管理法修訂業於 114 年 12 月 1 日施行，修正重點包含主管機關權責調整、強化納管機關資安管理及精進資安人力策略等，以符實需。為利資通安全管理法修法施行實務運作順利及因應國內國外資安威脅情勢發展，本部亦同步完成資安法相關子法修法作業，相關 8 部子法亦於 114 年 12 月至 115 年 3 月期間陸續發布施行。

(二) 為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，現行資安法增修第 11 條限制公務機關及發配供業務使用之資通訊設備，均不得下載、安裝或使用危害國家資通安全產品（包含大陸地區、香港或澳門地區廠牌資通訊產品）；其自行或委外營運場所提供公眾視聽或使用之傳播設備及網際網路接取服

務，於維護資通安全之必要時，亦同。另依資安法第 27 條，中央目的事業主管機關對特定非公務機關得予以限制。

(三) 另，為妥適評估機關所使用資通訊產品對於國家資通安全之威脅，訂定「危害國家資通安全產品審查辦法」，藉由收受各機關提供的情資，與會商相關機關研商，且將研商結果快速分享予其他機關，以利各機關即時應處，將所遭受之危害風險降至最低。

玖、打造國家資安科研團隊，建構全社會資安韌性

一、打造 AI 賦能之主動防禦與 CI 韌性基礎

(一) 可視化主動防禦與 CI 場域威脅獵捕

1. CI 場域威脅獵捕與 OT 可視化防護

資安院持續建置專業防護檢測團隊，深入關鍵基礎設施(CI)場域進行資安評估、威脅狩獵、事件調查與 OT 流量分析。透過資產盤點、通訊基線建立與異常行為辨識，有效提升場域潛伏威脅之可視性，並將檢測弱點回饋至防護策略，建構「偵測、應變、調整」之持續防護閉環。同時，推動 AI 導向自動化工具研發，聚焦流量異常與日誌關聯分析，降低人工負擔，後續將模組化導入所有 CI 場域，建構可複製之主動防禦體系。

2. 政府機關實兵演練與弱點修補閉環

資安院由外部攻擊測試(社交工程與實兵演練)及內部技術檢測(含端點主機、網路架構、核心系統及資料庫等 8 大面向)雙向切入，協助公務機關及 CI 提供者檢視資安韌性。針對檢測發現之 SNMP 設定與弱式加密等常見漏洞，本院持續透過警訊通知與修補追蹤，輔導機關形成「發現、通報、修補、驗證」之弱點治理閉環。

3. 高風險漏洞預警、VANS 與產品弱點治理

資安院持續蒐集國內外之資安弱點情資，即時發布重大弱點警訊，協助機關及早因應與防護，115 年迄今已發布 116 篇漏洞警訊、43 篇漏洞新聞及 2 份漏洞風險預測報告。同時持續維運「資通安全弱點通報系統(VANS)」，協助機關自動比對資產弱點。另在協調揭露(CVD)業務中，共發布 82 篇公告、涵蓋 146 個產品漏洞；並協助進行國家資安危害產品檢測，已完成 2 台 DVR 錄放影機及 12 支 App 檢測與報告產出，強化產品風險管控。

(二) AI 化營運流程與自主防禦

1. AI 主動式防禦關鍵技術落地

結合惡意郵件誘捕、蜜罐分析及大語言模型(LLM)之漏洞 PoC 初判技術，建構情資自主智慧分析機制。115 年迄今已完成逾 500 萬筆惡意郵件分析、蒐整 8,721 筆蜜罐攻擊日誌(收斂 13 個代表性攻擊群組)，以及 1,451 筆軟體資產評估。同時完成「AI 主動戰情平台雛形」，並順利推廣至國家圖書館、經濟部水利署、交通部中央氣象署等 8 個政府核心機關試用。

2. 資安治理 AI 化平台與週報系統

整合事件通報、聯防監控、蜜罐誘捕與外部曝險等多元數據，導入 AI 分析技術。目前平台已建置 4 項視覺化儀表板與 6 項治理施力清單(如通報時效性、高風險曝險等)，將分散資安數據轉化為可行動之治理項目，並規劃進行機關試用與動態調校。

3. AI 威脅內容鑑識與數位訊息分析

為因應 AI 生成深偽內容、錯假訊息及詐騙訊息等新

興數位訊息威脅，資安院承接資安署「數位訊息分析技術研發」及數產署「精進詐騙樣態分析」專案，開發多來源訊息分析與 AI 內容鑑識平台，累計處理逾 250 萬筆開源情資，並開放 7 個外部單位調用，有效提升政府對深偽（Deepfake）與錯假訊息之自動化研判能量。

二、建構產品資安與供應鏈信任生態系

（一）產品資安生態系與供應鏈信任機制

1. 國家級漏洞獵捕與產品資安驗證

辦理首屆產品資安漏洞獵捕活動，共計 20 項產品參展並發掘 20 項漏洞（已全數修補完畢）。第二屆活動聚焦政府常用軟體，刻正邀請藍隊廠商報名，並規劃擴大總獎金池，建立制度化之產品資安驗證機制。

2. PSIRT、漏洞通報揭露與供應鏈信任機制

透過 TWCERT/CC 發布 PSIRT 建置指引與成熟度自評，截至 115 年 9 月已輔導 27 家重點產業企業自評（年底目標 30 家）。另因應歐盟《網路韌性法》及國際產品資安趨勢，完成 3 大公協會訪談、4 類產品（船舶、車輛、航空器、醫材）座談及 2 場 SBOM/PSIRT 工作坊，推動國內供應鏈信任無縫對接國際標準。

（二）AI 資安人才、國際鏈結與全社會資安意識

1. 資安人才職能基準與培育

精進資安人才職能訓練藍圖，規劃相關議題研析及推動。研發滲透測試、數位鑑識與情資分析等專業資安人才訓練教材，以培育具備檢測、分析與應變能力的高階專才，全面強化國家及企業資安韌性。

2. 全民資安意識推廣

為提升全民資安意識及基本防護能力，研發生活化、情境式教具原型，推動分眾全民資安宣導，降解知識門檻。以生活化、情境式方式協助民眾認識常見資安風險及建立正確數位安全觀念。

後續將依不同族群風險與需求推動分眾宣導，串聯校園、家庭、社區及民間組織，透過情境教材、體驗活動及行動引導，促進資安認知轉化為日常防護行為，深化全社會資安韌性。

3. 數位靶場與桌上推演強化 CI 實戰韌性

為提升關鍵基礎設施(CI)資安韌性，針對水、電力、石油及天然氣等領域進行業務風險訪談，據以設計資安桌上推演情境並辦理 6 場演練，強化 CI 資安長之決策判斷、跨單位協調及事件應變能力。

另運用能源與水領域數位靶場辦理實務演練，邀請 24 個 CI 單位資安人員參與，在不影響實際營運下進行擬真攻防，強化事件研判、防禦及應變處置能力。後續將拓展至通傳、交通等領域，持續精進推演情境與靶場腳本，落實「以戰代訓」，提升 CI 自主防禦與應變量能。

4. 國際合作、APCERT 演練與全球資安夥伴鏈結

資安院持續參與 APEC TEL、FIRST、APCERT 及漏洞協調全球實踐社群(CVD-COP)等國際組織及社群，深化跨國資安事件應變、關鍵基礎設施韌性及資安治理合作。

115 年迄今，參與 APEC TELWG 第 72 次及第 73 次會議，並擔任資通訊安全與信任指導分組召集人，與 11 個經濟體及 ICANN、ISOC 等組織交流 AI 安全、人才培

育、CI 韌性、反詐騙及 DNS 安全等議題。另擔任 APCERT 督導委員會委員及訓練工作組召集人，參與 APCERT 2026 亞太區資安演，並出席 FIRST 2026 年會及 NatCSIRT 會議，深化與國際資安夥伴之合作及跨國聯防量能。

三、成為國家資安治理、營運應變與政策支援智庫

(一) 通報應變、情資聯防與攻擊手法(TTPs)態勢分析

1. 公私領域資安事件通報、應處與技術支援

資安院綜整掌握資安法納管公務機關、特定非公務機關及民間企業之資安事件通報與應處情形；重大資安事件發生時，配合主管機關籌組應處小組，提供事件研判、技術分析及損害管制建議，協助降低事件衝擊並加速復原。

針對資安法納管機關，持續維運通報應變網站，受理及審核資安事件通報，提供技術諮詢及應處建議，並進行攻擊手法、來源及根因分析；必要時成立專案，提供遠端分析或現地查處，協助機關強化應變及復原能力。

針對民間企業，以 TWCERT/CC 推動公私協力聯防，收斂活動預警、駭侵事件、漏洞情資及入侵指標等 4 類情資，並視事件情形通報攻擊來源、協同警調調查或預警可能受駭單位。另配合重大或受矚目個資外洩事件，協助主管機關辦理行政檢查，強化民間企業資安事件應變及資料保護能力。

2. N-ISAC/C-ISAC 跨域情資分享與聯防監控

資安院持續營運國家資安資訊分享與分析中心(N-ISAC)，透過自動化機制推動跨領域資安情資分享。115 年 1 月至 9 月共分享 123,090 則情資，其中包括資安事件

119,027 則、漏洞公告 1,727 則、威脅預警 1,485 則、態勢感知 677 則及策略分析 174 則。另協助營運國家通訊暨網際安全中心(NCCSC)，提供 7x24 小時服務，並透過 C-ISAC 與 N-ISAC 進行雙向情資交換。同期 C-ISAC 分享至通傳領域 59,254 則、分享至 N-ISAC 35,245 則，C-SOC 蒐集情資 2,546 則，強化通訊傳播領域 CI 之早期預警及跨域聯防能力。

後續將持續拓展國際威脅研究合作及情資來源，深化跨域情資分享、態勢研判及聯防應用。

3. 攻擊手法(TTPs)分析、蜜罐誘捕與黑名單防護

資安院持續蒐整內、外網蜜罐威脅資料，結合攻擊指標(IoC)、偵測規則及威脅情資，分析攻擊手法、來源及惡意活動樣態，強化新興攻擊之預警與態勢研判。

截至 115 年 9 月，外網蜜罐已蒐集逾 163 億筆攻擊連線資料，掌握 IoT 設備、網路服務漏洞及 Mozi、Mirai 等殭屍網路攻擊；內網部分已導入 8 個向上集中政府機關之誘捕機制，蒐集逾 19 萬筆連線，經篩選均屬合法連線事件。資安院並持續分析蜜罐日誌、萃取攻擊特徵及建立偵測規則，提升威脅辨識能力。

建立黑名單自動化部署機制，整合威脅清單供機關應用於防火牆及 DNS。截至 115 年 9 月，共 196 個機關完成導入，包括 38 個 A 級、100 個 B 級、21 個 C 級公務機關，以及 37 個特定非公務機關。

惡意電子郵件偵測方面，115 年 1 月至 9 月已檢測逾 1 億封郵件，發現 144 萬餘件惡意電子郵件樣本；惡意檔案檢測服務共檢測 1,600 個可疑檔案，其中靜態掃描判定

具風險 512 個、動態分析具風險 632 個。後續將持續優化威脅偵測、情資回饋及聯防機制，提升政府與民間資安防護能力。

(二) 資安治理平臺與資料驅動決策

1. 國家資安治理平台與資料可視化

資安院持續建置國家資安治理平台，整合資安事件通報、聯防監控、蜜罐誘捕及外部曝險等跨來源資料，透過資料視覺化、AI 輔助判讀及治理施力清單，協助掌握資安風險態勢及施策優先順序。

115 年截至 7 月止，已收容 SOC 業者回傳有效資安監控情資 547,121 件，作為平台分析攻擊手法(TTPs)異常之基礎。目前平台已進入整合測試及功能調校階段，完成 4 項儀表板及 6 項治理施力清單，將分散資安資訊轉化為具體觀測指標及治理項目。

後續將邀請部分政府機關試用，依使用回饋精進儀表板、治理施力清單及 AI 輔助分析功能，強化國家資安治理與決策支援。

2. 政策法遵、AI 資安韌性與國際趨勢研究

資安院持續研析國際資安政策及法制趨勢，涵蓋關鍵基礎設施防護、個資與資安跨域保護、AI 資安韌性及國際 AI 安全研究機構(AISI)發展，支援我國資安政策規劃、法遵調適及國際合作。

自 115 年 1 月至 9 月，已出刊 37 期國際資安政策法制觀測週報，並完成 10 個國際 AISI 之組織類型研析與分類，作為掌握國際政策現況及研擬資安治理、國際合作策略之參據。

後續將持續深化 AI 資安韌性、AI 安全治理及國際參與研究，支援我國參與國際 AI 安全議題及合作機制。

3. 資安週報、治理施力清單與政策決策支援

資安院建置 C2MA Lite(Cyber Capability Maturity Assessment Lite)平台，導入 AI 技術解析資安中心成熟度評估題項，協助組織掌握治理、營運、技術及管理面向之成熟度，作為資安能力提升及政策決策參考。

115 年迄今，平台已進入整合測試及功能修正階段，可運用 AI 解析中英文評估內容，涵蓋 9 個評估領域、約 220 題。後續完成測試後，預計將開放資安院 MOU 簽約單位使用，並依實際回饋持續優化平台功能。