

中華民國 115 年 4 月
立法院第 11 屆第 5 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、推進黨家數位發展政策，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...5
- 肆、強化數位應用，打造高效便捷的智慧政府.....8
- 伍、強化數位發展國際合作，共同提升網路數位韌性.....13
- 陸、發展資料運用，打造資料創新應用生態.....17
- 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.....41
- 玖、打造國家資安科研團隊，建構全社會資安韌性.....45

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「推動 AI 產業發展」、「強化資安韌性」、「落實打詐作為」以及「強化數位政府建設」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) 根據國際數位發展及 AI 治理趨勢、相關國際評比、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、人工智慧立法作業

- (一) 本部依據 114 年 12 月 23 日經立法院三讀通過之「人工智慧基本法」調修「人工智慧風險分類框架」草案，並擴大徵詢專家與產業意見，草案預計提報行政院並於核定後對外發布，未來亦持續與相關目的事業主管機關進行就「人工智慧風險分類框架」進行協作，以協助其訂定以風險為基礎之管理規範，並依據協作情形滾動調修框架內容。
- (二) 「人工智慧基本法」業於 114 年 12 月 23 日經立法院三讀通過，其附帶決議請行政院科技政委督導本部會同國科會、教育部和衛福部及其他相關機關，於本法三讀通過後 3 個月內，完成「兒少影響評估」、「人權影響評估」、「性別影響評估」，並將評估報告公開發布，供社會各界參考。另請本部研議建立常設性評估機制，以定期檢視人工智慧應用對兒少權益、人權以及性別之影響，持續強化其保護措施。本部透過徵詢兒少、性別及人權等相關專家及權責部會之意見，完成影響評估報告，未來本部將持續提供人工智慧技術觀點與更新，協助我國相關單位或機關研議與其既有風險評估作業整合，以期循序發揮跨領域治理綜效。

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 年度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，修訂「研究機構能效評估作業-數位發展部自主評

估作業機制」，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 114 年 11 月 25 日將重大公共建設範圍草案及稅式支出評估報告函報財政部審核，財政部已於 115 年 3 月 30 日公告。
- (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) 整備《電信管理法》相關規定：本部於 114 年會同國家通訊傳播委員會，推動修正《電信管理法》第 72 條，增訂沒收及處置故意破壞海纜犯罪工具、船舶或其他機械設備之規定，並已於 115 年 1 月 5 日發布施行。藉由完善法制基礎，提升我國海纜安全防護效能。
- (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；國內海纜「臺馬 4 號」、「臺澎 4 號」

及「澎金4號」預計於115年6月完工。同時，亦補助業者建置或擴充微波等第二傳輸路由系統容量，透過增加多元通訊路由，降低斷纜事件對通訊服務之衝擊。

- (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，114年已核定4案補助案申請。自115年起，補助範圍進一步擴大，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：本部運用第五期前瞻基礎建設預算，補助電信業者建置高抗災通訊平臺、低軌衛星行動基地臺車及移動式發電機等。至115年3月，已於雲嘉南等地區完成16座高抗災通訊平臺建置，提升重大災害期間行動通訊網路之持續運作能力。另115年度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；同時，透過差別化補助機制，引導業者採用國產設備，促使新建5G基地臺之國產品牌使用比例提升至40%，兼顧通訊韌性與產業發展。

三、空—布建多元衛星應變通訊網路

- (一) 自115年起，本部透過「政府非同步軌道衛星通訊及維運服務案」共同供應契約，統一委託既有196個非同步衛星應變網路之衛星服務獨家代理商，辦理關鍵站點維運作業，

確保政府指揮體系於緊急狀況下，仍能維持基本且安全的通訊量能。前揭共同供應契約並開放政府機關、學校及公營事業等，依實際需求訂購 OneWeb 低軌衛星及 SES 中軌衛星通訊服務，藉由擴大運用場域，提升我國整體通訊網路韌性。

- (二) 導入新興衛星通訊網路：因應國際低軌衛星通訊技術快速發展，本部自 115 年起推動下一代政府衛星專網落地介接的先期研究。工作內容涵蓋衛星站點配置規劃、衛星服務可用性實測等，作為後續引進新興國際低軌衛星星系（如亞馬遜低軌衛星 Amazon Leo）之重要基礎。

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：持續以「全災害」思維（涵蓋天然災害、人為破壞及資通安全威脅），督導通傳領域關鍵基礎設施強化安全防護作為與應變能量。114 年度共辦理 3 場次安全防護演習、4 場次防護檢視及 6 場次資安稽核，藉以驗證與檢視通傳 CI 現行防護機制的有效性；並針對發現之缺失，督促業者改善，透過滾動式調整持續精進，全面提升通傳網路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：參考《資通安全管理法》相關規定，修正關鍵電信基礎設施資通設備（如防火牆、交換器及路由器）的資通安全檢測技術規範，並納入歐盟漏洞資料庫（如歐盟漏洞資料庫 EUVD）作為檢測參考依據，俾關鍵電信基礎設施設置者採購符合資安要求之設備，進一步強化通訊網路整體資安防護能量。

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、 規劃與釋出次世代無線電頻率

(一) 持續觀測國際行動通訊頻段規劃與釋出

1. 國際趨勢研析與政策建議

關注重點國際組織及先進國家 6G 技術最新進展，掌握頻譜政策、新興和諧共享機制與各國頻譜最新佈局，尤其針對行動通信與衛星通訊地空整合趨勢，梳理其管理架構、法規及執照管理制度，進而對我國 B5G/6G 頻譜規劃政策提出具體建議。

2. 6G 候選頻段實證與技術觀測

針對重要 6G 候選頻段 (Upper 6GHz, 指 6425 -7125 GHz 頻段)，已完成電視臺傳輸鏈路、跨海微波鏈路分析與自由空間光通信 (Free-Space Optics, FSO) 2 公里跨海測試，並依據分析與量測成果，研提 U6 頻段整備候選方案。

3. 深化頻譜整備與國際交流合作

完成輔導 AP 設備製造商導入中頻段 (Mid-band) 和諧有效使用機制，促進產業依循相關技術與管理要求提升頻譜使用效率；並辦理多場國際及產官學研交流活動，包括世界行動通信大會 (Mobile World Congress, MWC) 行前交流會、WRC-23 經驗分享會及第 2 屆「頻譜大未來」國際頻譜交流會議等，藉由跨域對話與經驗交流，強化我國頻譜政策整備能量及國際接軌。

(二) 衛星頻段釋出

累計至 115 年 2 月底，本部已完成隴華電子、愛爾康、台亞衛星及中華電信等 4 家業者共 8 件衛星通信頻率申請案之審查；其中，中華電信分別於 114 年 6 月及

10 月啟用 OneWeb 與 SES O3b 兩個衛星系統之服務，台亞衛星並續於 115 年 1 月啟用 Eutelsat 衛星服務，有效強化我國通訊韌性。

二、管理與提升電信資源使用效益

(一) 促進頻率使用效率

1. 精進電信資源規費制度

完成「頻率使用費收費標準」修正，將衛星行動通信服務納入頻率使用費調整的適用範圍，透過差異化費率與折抵機制，降低衛星網路建置與營運負擔，以鼓勵電信事業提供衛星行動通信服務。

2. 查核頻率使用效益並帶動數位應用落地

落實法定偏遠地區村里、山林區域及交通樞紐的頻率使用效益查核，確保規費折抵實質優化通訊品質；同時，藉由規費折抵方式，帶動電信事業參與 44 案數位應用服務，引導電信垂直場域應用服務落地。

(二) 促進新興技術蓬勃發展

115 年度截至 3 月底計有 9 件產業研發頻譜申請案件，涵蓋低中高軌衛星、無人機反制雷達、車聯網及 5G 等關鍵技術領域。透過嚴謹的干擾評估與資源調度，確保頻譜和諧共存，並有效支援產業研發之用頻需求。

三、積極參與國際，保障數位通傳資源使用權益

(一) 參與 APEC 數位部長級會議並共同發布部長宣言

本部出席「亞太經濟合作 (APEC) 2025 年數位及人工智慧部長會議」，並與韓國科學技術情報通信部等 21 個經濟體部長與代表共同發布 APEC 首份「數位及 AI 部長宣言」，展現我國積極參與區域數位治理與 AI 政策對話

之成果。

(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 年已會同外交部、內政部刑事警察局等機關深入參與 ICANN 82 至 85 計 4 場國際會議，維運涉我國主權域名（.政府）1 筆，截至 115 年 2 月底，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 12 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 至 115 年 2 月底，共編訂電子報計 13 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 1 場、研討會議 3 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。例如透過參與並擔任 ICA（國際政府資訊科技理事會）計畫委員會策劃委員，與各會員國交流數位轉型經驗；本部於 114 年 9 月 15 日至 18 日於臺北主辦 ICA 第 59 屆年會，邀請 17 個國家（組織）共 40 名代表參加，展現我國政府數位發展之具體成效，擴大本部與世界先進國家互動與合作。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 月將調查結果公告至本部官網。

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，114 年已完成 15 個機關易用性測試作業，目前刻正辦理 5 個機關使用者中心設計(UCD)工作坊及成果分享會，並完成 UCD 報告公告於政府網站營運交流平臺供各機關使用。為精進網站檢核作業，預計 115 年上半年完成政府網站智慧檢測工具推動規劃，推動一鍵生成報告檢核機制，優化檢測回應品質。

(二) 為縮短各縣市政府資訊建設發展落差，本部 114 年已挑選 5 個地方政府（花蓮縣、臺北市、桃園市、嘉義縣、雲林縣）推動數位轉型成功典範案例進行剖析，並完成 4 個典範案例成果分享會，致力將成功擴散。預計於 115 年上半年完成桃園市政府「孕產婦福利一站式服務」流程再造研析作業。

(三) 「公部門人工智慧應用參考手冊(草案)」已於 114 年底完成一年試辦，已於 115 年第一季函頒正式版；另為利各機關以更便捷的方式查詢手冊內容及取得最新資訊，本部已建置「公部門人工智慧應用參考手冊互動式介面」，彙整手冊內容並以 AI 技術提供智慧諮詢服務，業於 114 年 12 月完成建置並上架本部官網。

三、掌握政府數位人才供需，完備資訊職能基準、鑑定與培力機制；推展政府服務設計，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，辦理政府資訊人員法定訓練及在職訓練。114 年已完

成 2 梯次基礎實務訓練、3 場次中高階資訊主管訓練及跨域策略管理訓練，完成資訊職系 200 人次 7,000 多人時訓練，並開辦 600 小時以上資訊在職訓練課程，以養成 AI 的實戰力為首要目標。115 年持續辦理 3 場次中高階資訊主管訓練及跨域策略管理訓練、3 梯次基礎實務訓練，並辦理至少 30 門(約 450 小時以上)資訊人員實體在職訓練及導入 200 門線上資訊職能課程，持續培力我國資訊同仁數位能力。

- (二) 完善政府數位首選服務入口，截至 114 年 12 月「我的 e 政府」完成 89 項主題策展，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 3,043 項網路申辦項目，115 年將聚焦以人生事件為基礎，優化入口網功能，提升民眾使用政府服務體驗。
- (三) 本部推動政府無障礙網頁標章認證檢測服務，114 年截至 12 月之有效標章數量計 6,413 筆、人工檢測 3,773 件、身障人士檢測 930 件，受理無障礙申訴案件 110 件。
- (四) 本部與行政院人事行政總處於 114 年成立「AI 公務人才發展辦公室」，旨在統籌全國 AI 培育資源。本部核心任務為建立「AI 公務人才認定指引」、導入多元算力資源，並加速推動政府 AI 服務落地。預計 115 年底正式發布「AI 公務人才認定指引」，並推動全國性的 AI 訓練及認證機制。

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 114 年 12 月底，已完成協助 10 個機關導入零信任身分與設備鑑別機制，累計已有 39 個資安 A 級

機關完成零信任身分鑑別機制建置，並有 30 個機關完成零信任身分及設備鑑別機制之導入。另規劃於 115 年底前，持續完成 7 個資安 A 級機關零信任設備鑑別機制之建置，以逐步強化政府整體資安防護與數位韌性水準。

- (二) 輔導各級機關透過 T-Road 進行資料傳輸，截至 114 年 12 月底，已有 66 個機關與 200 項服務介接 T-Road，每月逾 180 萬筆傳輸量，115 年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措施，從 114 年平均每月攔截超過 5.8 億次攻擊、阻擋 212 萬次惡意網頁及 90 萬封垃圾郵件，通報 57 起 DDoS 攻擊事件，延續 114 年的防守成效，115 年將致力於優化現有防護措施，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 114 年 12 月底已超過 4 萬 5,000 筆短網址，逾 1 億 1,000 萬使用人次，預計 115 年度達成 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。截至 114 年 12 月底止已逾 600 個機關單位使用，累計發送逾 1 億則簡訊。另政府採購網共同供應契約已於 114 年 11 月 24 日完成上架作業，自 115 年 1 月 1 日起，各機關可依需求自行至共同供應契約訂購

與使用。115 年將依政府資安政策強化系統資通安全防護，優化系統存取管控、傳輸安全及異常監控等防護機制，以確保系統之完整性及安全性。

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 年將擇定 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巡航健檢，透過實地輔導協助機關落實數位韌性。
- (二) 為提升政府行政效率，本部就政府緊急臨時並因應政策性之紓困、振興、補助等措施，建置「政府發放共用基礎平臺」，介接中央銀行「數位公共建設金流平臺」，提供現金、數位券之發放，並協助發放機關處理相關的核銷及結算作業。發放平臺已於 114 年第 2 季上線試營運，支援客委會辦理客家幣發放作業；115 年預計辦理客家幣 2.0 發放作業。
- (三) 為強化政府關鍵民生系統之韌性與整體服務能量，本部推動「行政部門關鍵民生系統精進雲端備份及回復計畫」。截至 114 年 12 月底，參與執行之 7 個部會均已完成年度跨境公有雲備份作業，並辦理回復至地端之演練、簡易備份功能建置。本部完成至執行機關進行實地查證，協助各機關滾動檢討並調整相關執行措施。此外，本部亦辦理國際專業訓練課程，協助執行機關培育具備雲端服務管理及災害復原等專業能力之人員，累計培訓 40 人次。藉由每年定期辦理備份與回復演練，持續強化機關人員對演練流程與

操作內容之熟悉度，以全面提升各機關面對突發事件之應變與復原能力。115 年將依計畫辦理度跨境公有雲備份與回復演練以及實地查證等工作，預計年底前完成訂定政府關鍵民生系統核心備援指引文件提供政府機關參考。

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，本部於 114 年度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)，114 年度於 DESG 提案並分享我國推動數位發展現況、打詐、推動隱私強化技術計畫進程及開發數位憑證皮夾規劃等成果。於 114 年 8 月在韓國舉辦之 APEC 數位部長會議中，與亞太地區各經濟體分享我國推動數位經濟發展、強化數位韌性及積極打擊詐騙之成效，深化區域內各會員對我國數位成就之認識與肯定；115 年賡續透過 APEC 數位及 AI 部長會議、DESG 等場域，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，派員出席多項數位經貿相關談判，促成 114 年 6 月 30 日臺英雙方簽署臺英促進貿易夥伴關係 (Enhanced Trade Partnership Arrangement, ETP) 數位貿易協議及 12 月 4 日簽署「臺日數位貿易協議」。115 年將與歐盟共同推動臺歐盟數位經濟對話 (Taiwan-EU Dialogue on Digital Economy, DDE)，並與美國等夥伴就推動 AI 供應鏈發展、AI 人才培養、數位基

礎建設等議題進行對話。

- (二) 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，經過 2 年積極參與獲得各國肯定下，促成該組織於 114 年 2 月來臺舉辦策略協調會議，深化各國對於臺灣的印象，獲該組織認可我國成就並延長我國參與該組織權利 2 年，凸顯我國作為 FOC 成員的貢獻；114 年 10 月持續參與在愛沙尼亞塔林舉辦之部長級會議，與各國數位發展部長及外交部長，就數位時代之治理趨勢等重要議題進行交流，賡續強化數位同盟基礎，並共同聯署包含《人工智慧與人權聯合聲明》、《在武裝衝突時期保護人權與防止網路中斷聯合聲明》及《尊重權利的數位公共基礎設施原則》等 3 項聯合聲明；115 年持續參與 FOC 會議，並與外交部合作支持跟組織運作，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。114 年度成功媒合桃園、高雄、臺南與臺東共 4 縣市政府與公民科技團隊合作，針對「兒童早期療育」、「運動生活圈」、「災防啟動系統」與「消防行政流程」等民生議題，完成實驗型概念性驗證，並於成果發表會暨交流座談會邀請合作縣市政府與公民科技團隊共同展示執行成果與分享執行經驗。透過試驗場域機制，有效促成公私協作，提升民眾使

用體驗與參與感，進而展現以民眾需求為出發點的「人本數位」公共治理實踐。115 年度將著重應用公民科技防災之議題，與國家災害防救科技中心共同合作推動，強化我國防災韌性。

- (二) 我國公民科技能量廣受各國矚目，於 114 年成功爭取國際數位人權全球大會 Rights Con 2025 於臺北舉辦，外交部與本部攜手協助主辦單位處理來自全球 150 國參與人員之入境審查事宜，並由主辦單位邀請蕭美琴副總統及行政院鄭麗君副院長於開幕中致詞，活動議程亦安排本部專題演講 3 場次及推廣數位憑證皮夾，充分推廣我國數位韌性成果，增進國際交流。115 年將加強人工智慧領域國際專家之聯繫與合作，逐步建立我國人工智慧國際交流聯絡網，強化與各國政策對話與技術合作能量，提升我國於全球人工智慧治理與應用發展之能見度與影響力。

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

- (一) 112 年 1 月加入制定全球網路標準的「全球資訊網協會」(World Wide Web Consortium, W3C) 及國際身分識別標準組織 (Fast IDentity Online Alliance, FIDO)，取得各項標準的草案資訊，用以建置和測試分散式驗證及授權機制。
- (二) 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，並已完成數位憑證皮夾 APP 之核心系統及沙盒環境，其中數位憑證皮夾沙盒於 114 年 3 月 31 日開放，邀請企業、民眾、學術研究單位共同參與，迄 12 月底止，共有超過 2,200 個廠商、機關、團體及民眾申請帳號，另 114 年 12 月開放超商取貨試營運，APP 下載量已

超過 9 萬次，並持續將該技術擴大國際合作事項，期能對接歐盟、全球資訊網協會等國際標準，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，如駕照及工商憑證等，115 年將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) 營造社會對話與參與機制，114 年賡續辦理第 7 屆總統盃黑客國際松，以打造淨零數位典範，本屆競賽主題為「Digital Innovation for Resilience and Sustainability 以數位創新打造韌性與永續的未來」，已於 114 年 5 月啟動活動宣傳，並於 6 月 16 日正式對外公告徵件，期間完成宣傳活動逾 12 場次，成功觸及破千名國內外各領域潛在參賽者，為總統盃黑客國際松的擴大曝光與影響力。已於 114 年 12 月辦理頒獎典禮，邀請卓越團隊來臺交流，為我國網羅優秀人才，取得淨零科技發展先機，並持續深化與廣化多元領域實質關係。115 年國際松徵件主題將以「數位共好：打造智慧永續新生活」為目標，持續向國際徵求永續數位解方。
- (二) 打造淨零數位典範，114 年賡續辦理綠色數位服務規劃及推廣計畫，扣合行政院永續長聯盟擴大綠色採購之政策，連結國際發展趨勢，研析規劃綠色數位服務政策，以掌握未來綠色數位技術發展趨勢及新興數位行為對碳排之影響，協助各界推動淨零排放。115 年將以綠色軟體為核心，強調軟體永續設計與軟體碳排放計算基礎，辦理綠色軟體

宣傳說明會及工作坊，逐部完成產業溝通形成共識，採行穩健節奏，厚植實施基礎。

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式各機關資料集，至 115 年 2 月底逾 5 萬項，瀏覽量達 1 億 8,067 萬人次、下載量達 2,237 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 2 月底已推動 25 項領域、2,100 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、能源管理及社會救助等，113 年續增「農業永續」與「空間資訊」、114 年偕同金管會、環境部、經濟部等跨部會協力推動新增「企業永續」，強化企業永續資訊揭露，總計 9 項高應用價值主題，由 170 個機關，共開放 1,609 項資料集，截至 115 年 2 月底，該高應用價值主題專區總瀏覽量達 406 萬次。
- (四) 資料活化應用建構多領域協作環境：本部與各部會協力發展更具潛在價值資料之加值應用，例如「YouBike 站點搜

尋器」、「台灣下一班公車時刻表 APP」等交通資訊服務，提供站點位置、可用車輛數量及公車到站時刻查詢，協助民眾即時掌握通勤所需之交通資訊。相關應用可支援多元通勤情境下的運具選擇與路線安排，降低資訊取得門檻，並強化交通資料於日常通勤與城市交通服務中的實際應用價值。

- (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，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，以高應用價值主題為優先試行領域，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) 為提供民眾更便利的生活，持續推動創新數位服務，MyData 平臺截至 115 年 2 月底已介接中央機關、地方政府、金融機構等 84 個機關，提供 1,216 項資料下載與服務

申辦，累計超過 896 萬餘次使用量，相較於 114 年同期成長約 1.6 倍；會員人數逾 167 萬，相較於 114 年同期增加約 80 萬人；提供 10 種身分驗證方式，並由資料提供機關依資料機敏程度決定驗證等級。

- (二) 為擴大觸及使用族群、優化服務使用體驗，以 MyData 全局觀概念規劃「主題服務」，發展貼近民眾生活領域所需服務，並藉由延伸各類主題服務流程，豐富各類主題服務項目，包含社會福利、婦幼關懷等，除可橫向拓展至中央機關與縣市政府外，並將扎根延伸線上服務，提高申辦效率，更貼近民眾的日常需求。如國家住宅及都市更新中心聚焦「生活扶助」主題，於 114 年 6 月 9 日上架「安居好室社會住宅申請」，使用次數已逾 19,000 餘次，便利民眾可線上快速取得政府服務申辦所需個人化證明文件，貼近民眾日常生活需求。
- (三) 本部持續推動各機關新增 MyData 便民服務，114 年度共辦理 2 場次服務推廣說明會與 3 場次技術開發說明會，邀請中央、地方機關、金融機關與學員分享實際介接 MyData 過程與執行成果，建立服務典範案例；另為推動地方政府介接 MyData，發展貼近在地民眾需求服務，114 年度訪視 3 縣市地方政府，透過與地方政府交流，瞭解其線上申辦重點服務、MyData 介接情形、預計新增服務與宣傳推廣規劃等，並於 115 年 1 月至臺東線及金門縣當地舉辦服務推廣說明會，以實務案例分享與經驗交流，協助當地推展介接線上服務，激盪出更符合民眾期待的優質政府服務。

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；並發展資料分析隱私強化技術部署機制及驗證工具，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，草案已於 114 年 10 月 31 日送行政院審議。
- (二) 發展隱私強化技術驗證及部署機制：將就差分隱私、合成資料、同態加密等前瞻隱私強化技術持續深化研究其演算法及適用情境，精進相關技術驗證工具，建構資料分析隱私強化技術驗證場域及部署機制，以活絡資料合規創新應用。
- (三) 推廣隱私強化技術應用及國際合作
 1. 已辦理第 30 屆大專校院資訊應用服務創新競賽「資料隱私保護創新應用組」，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。
 2. 為與國際同步倡議隱私強化技術，推動國際隱私強化技術交流活動，已申獲 APEC 專案補助計畫，於 114 年 9 月 12 日辦理隱私強化技術國際研討會，邀請近 12 個經濟體成員來臺就政策與制度設計、技術創新及實務應用

等議題進行交流，提升我國國際能見度。

3. 為提升政府資料隱私技術韌性，已偕同政府機關（內政部統計處）及公私協力（金融機構）導入隱私強化技術工具，共同驗證技術可行性、保護力，活絡資料創新應用發展。會同專家組成技術團隊，輔導部會導入隱私強化技術，引入適當技術工具兼顧資料隱私保護及可用性，逐步擴大推廣至公部門應用環境，建構公眾信任之數據利用環境。

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，藉此擴大數據協作能量，展現社會共好，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，並提升數據素養與認知，已依實務需求辦理多元數據培力課程，內容涵蓋 AI 與數據轉型思維、數據治理與資料盤點、服務與資料流程優化、資料設計思考、數據視覺化、以人為本的數據應用，以及組織內部溝通協作，截至 114 年底止，已辦理 11 場次數據培力課程，參與組織達 350 家，參訓人數達 822 人次。
- (二) 為鼓勵非政府及民間組織活用數據發展創新服務，本部已啟動第 3 屆 NGO/NPO 數據創新應用輔導，邀請多元領域之數據專家共組數據教練輔導團，共同遴選出 3 組 NGO/NPO 團隊，提供 8 個月的專家深度協作輔導，協助組織運用數據，實踐資料創新解方概念驗證，亦提供 19 組 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) 鑒於大型語言模型 (LLM) 著重於自然語言表達能力，訓練資料應集中於語意連貫性、內容結構完整且流暢之高品質資料，本部規劃優先推動政府機關提供高品質正體中文語料，協同教育部、文化部、原住民族委員會、客家委員會等逾 200 個機關，共同打造臺灣主權 AI 訓練語料庫，包括非屬著作權標的之施政計畫、施政報告，以及政府享有著作財產權的研究報告、政府出版品等，支援我國主權 AI 的發展與應用。
- (二) 為加速完備 AI 訓練資料的多樣性與品質，並適當消弭 AI 訓練資料於著作權爭議，促進各機關擴大訓練資料釋出，本部研擬並發布《臺灣主權 AI 訓練語料授權條款-第 1 版》，協助資料提供者與 AI 模型訓練者之間建立一套可行的授權機制，進而促進資料的合法流通與技術自主，並會同經濟部智慧財產局研提相關授權適用案例，提供各機關參考，期能在擴大訓練資料釋出與維護原著作權人權益間取得平衡。
- (三) 臺灣主權 AI 訓練語料庫已於 114 年 12 月 24 日上線，迄今已上架逾 3,000 筆資料集、超過 11 億 tokens，可提供國內外 AI 模型開發者申請使用。未來將持續推動地方政府投入，擴大語料廣度與在地性，提供具臺灣觀點、文化特色高品質語料，支援主權 AI 模型訓練需求。

柒、加速產業數位創新與轉型，帶動數位相關產業發展

一、攜手資服產業運用 AI 算力走向「產品化」

本部自 113 年打造 AI 算力池（共 40 片 GPU，包含 32 片 NVIDIA H100、8 片 AMD MI300X），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，截至 114 年底，已經累計協助 242 家次（186 家）業者開發 266 項 AI 模型與服務，其中已經有 80 家業者將 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 年將持續輔導業者，預計擴充 AI 算力，累計達到 140 片最新 GPU，以協助超過 300 家次資服業者加速創新應用落地，並預期擴散服務至 1,000 家次企業。

二、持續推動 AI 產業人才認定指引，營造正向循環的 AI 人才發展生態系

（一）推動 AI 產業人才認定指引

1. 因應 AI 應用需求日增，為協助產業辨識 AI 人才與能力，本部於 114 年 7 月發布「AI 產業人才認定指引」，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」亦已經將指引納入公務人員培訓參考。
2. 另於 114 年 11 月，本部與 3 家人才媒合平臺（1111 人力銀行、Yourator、Cake）簽署 MOU，後續將進行數據交換作業，並逐步推動平臺職缺對齊「AI 人才分類」及「AI 能力類型」。截至 114 年 12 月底，已經有 21 家民間業者通過 AI 技術服務能量登錄，結合前述 3 家人才媒合平臺，共計 24 家業者成為生態系夥伴，共同推動 AI 產業人才認定指引。115 年將對齊「人工智慧基

本法」與 AI 技術發展趨勢，預計於 5 月更新指引，增訂「AI 治理」等相關能力內容，未來也將持續與民間認證、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訊供各界參考運用，營造正向循環的 AI 人才發展生態系。

(二) 培育具備數位科技與產業領域知識之數位人才

本部以數位創新企業需求人才類型為導向，推動企業共同培育模式，強化學界與產業的鏈結。114 年與 19 家數位創新企業合作，共同培育 76 位具數位科技與產業領域知識的數位創新人才，並促成 35 位見習生獲得企業留用；115 年將持續與數位創新企業合作，預計培養至少 70 位數位創新人才。

(三) 育成在地數位人才

本部為培養在地數位種子人才，透過串連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，整體縣市涵蓋率達 73%。115 年將持續推動相關計畫，預計培育至少 95 位在地數位種子人才，促進在地數位化應用的長期發展。

(四) 吸引國際數位人才來臺

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」。截至目前數位領域就業金卡核發張數已經逾 1,124 張。未來將持續延攬具代表性國際專業人才。

三、加速 AI 應用與數位轉型升級，打造產業創新發展典範

(一) 推動多元場域導入 AI 驗證及建立典範案例

1. 跨產業 AI 交流與媒合機制：透過辦理多場跨產業 AI Demo Day，促進產官學研合作對接。113 年至 114 年間，已經累積 370 家企業參與，促成 31 件跨產業合作與實際導入案例，並成功帶動合作簽約與訂單媒合，累計簽約金額達 1,284 萬元。115 年度將延續前期推動成果，以「場域導向、產業聚焦、區域串聯」為核心策略，規劃辦理 12 場跨產業 AI Demo Day，並以健康照護產業為推動主軸，結合智慧製造及智慧農畜牧等產業。此外，亦透過徵案、遴選與媒合機制，促進 AI 技術於多元場域導入驗證，建立具代表性的應用典範。
2. AI 應用的普及與擴散：114 年本部舉辦「AI 開箱日」系列活動，匯集 23 家資服業者展示智慧客服、行銷、餐飲服務類等微型化 AI 解決方案，並透過公協會（TeSA、無店面公會、臺北市商圈產業聯合會等）邀請到 204 家中小微商家參與，透過 AI 技術協助改善營運流程及提升服務效能的實際應用情境，同時協助資服業者拓展中小微企業市場。115 年將持續規劃辦理 AI 系列推廣活動，每場次邀請至少 5 家資服業者展示微型化 AI 解決方案，並促成至少 50 家需求業者參與體驗，深化 AI 解決方案與既有業務流程整合。

(二) 加強投資國內 AI 新創及數位經濟產業

本部規劃的「加強投資 AI 新創實施方案」已經於 113 年 8 月獲得行政院國家發展基金管理會會議同意通過，匡列總額 100 億元，辦理期程為 10 年（前 7 年投資期，後 3 年處分期）。目前已經完成作業要點訂定，並完成專案辦公

室及信託銀行遴選，並自 114 年 3 月起正式受理投資案件申請。截至 115 年 2 月底，已經完成 3 梯次搭配投資人遴選共計 36 家，並核定投資國內 AI 新創及數位經濟相關產業計 6 案，方案投資金額約 7,556 萬元，帶動民間投資約 3 億元。115 年預計辦理搭配投資人遴選 1 次，累計至少 40 家搭配投資人參與投資方案，並預估至 115 年底累計完成 8 案投資審查，後續將搭配 AI 數位產業相關輔導政策，強化 AI 新創與數位經濟產業發展動能。

(三) 加速 AI 應用擴散，帶動產業數位轉型

為全面促進產業 AI 導入與數位轉型，本部透過技術盤點、培育人才及國際交流等三大面向，持續整合各界資源，並推動相關計畫，擴大產業應用 AI 普及率

1. AI 技術盤點與導入推廣：本部盤點國內 AI 技術能量，協助 AI 業者提升產品及服務競爭力，依不同產業領域應用情境，與平臺業者合作，深入掌握產業需求，解決企業在資料、人力及工具等面向的不足，並推動 AI 解決方案導入企業。此外，因應生成式 AI 興起，透過選拔與深度輔導機制，協助創新應用落地，加速百工百業數位轉型。

(1) 盤點國內 AI 技術與服務能量，輔導 163 家廠商通過 251 項 AI 技術服務能量登錄項目，並取得兩年期證書。取得證書的廠商將獲推薦成為「共同供應契約建議名單」，且現行部分政府補助計畫已經將能量登錄證書列為加分項目，有助於廠商提案。

(2) 透過輔導方式，鼓勵平臺業者透過串接 AI 工具，發展創新應用解決方案，以協助平臺會員數位轉

型。114 年輔導 10 家平臺業者透過 AI 工具串接，發展 50 項創新應用解決方案，帶動超過 2,000 家平臺會員導入產業領域 AI 解方，促使 114 年度 AI 普及率提升至 37%。115 年規劃協助資服業者發展並推廣企業會員適用的營運、客服等需求 AI 工具外；同時輔導具備技術深度的資服業者，發展提供高度個人化與自動化的智慧解決方案，預計發展至少 15 項 AI 應用解方。

(3) 辦理「2025 GenAI Starts 百工百業應用選拔」，促成 AI 創新開發與落地應用，共計 269 隊報名，最終促成 2 隊進一步申請 SBIR 補助案、1 隊進入百億投資審查、1 隊取得國發天使配投，及共計 15 隊獲得創投關注與追蹤。115 年將持續舉辦選拔與深度輔導，並進一步強化 GenAI 創新生態系，提供更多元外部資源，預計提供至少 25 隊晉級團隊深度輔導，以加速 AI 創新應用落地。

2. 培育產業所需人才：本部持續投入資源，培育開發型及整合型 AI 專業人才，並推動 AI 教育向下扎根，為中小企業為主體的產業結構，提供所需人力支援。114 年透過產學研合作，培育 2,493 位技術開發型人才，並爭取到 Apache Local Community (ALC) 在臺設立分部；另結合產業問題導向學習與企業實作經驗，培育 1,749 位可將 AI 技術轉化並實際對接產業需求的人才；此外，辦理「高中生 AI 扎根系列活動」，結合國內外大廠資源，透過 AI 線上課程、實作體驗營及成果發表等三階段培育機制，共培育 1,011 人；累計培育 5,253 人。

3. AI 產業國際交流與合作：透過舉辦 AI 大型展會，提升我國 AI 產業應用的曝光度；同時，積極攜手國際標竿企業合作辦理國際產業趨勢及技術落地應用合作交流，為臺灣技術開發者搭建全球技術社群交流平臺：
- (1) 114 年 7 月 31 日至 8 月 2 日辦理「World AI Vision Exhibition (WAVE 2025)」，展出最新 AI 應用及多元商務模式，匯集 181 家 AI 產業鏈上下游企業與新創團隊參展，吸引逾 5 萬人次觀展，展出期間促成逾 200 家次媒合洽談，成功串聯技術供應與應用需求兩端。115 年將延續展會動能，預計擴大徵集逾 200 家次國內外企業參展，並促成 300 次以上跨國或國內商務媒合。
 - (2) 攜手國際大廠（如 GitHub、高通等），以論壇、講座及工作坊等多元形式，分享最新工具應用與開發流程經驗，累積觸及線上及線下約 156 萬人次參與。115 年預計持續與多元國際大廠合作辦理 AI 技術交流活動，藉由大廠資源串聯在地社群與臺灣 AI 應用廠商參與，預估活動觸及超過 100 萬人次線上線下參與。
 - (3) 115 年將持續從技術導入、人才培育及國際鏈結三軸並進，推動低門檻、可複製的 AI 解決方案於中小微企業落地，預計輔導企業發展至少 15 項 AI 應用解方，提供 GenAI Stars 深度輔導 25 組團隊，同步培育逾 3,500 名產業與青年 AI 人才，並透過 World AI Vision Exhibition 等國際交流平臺，促成 300 次以上商務媒合。

(四) 提升我國軟體與資訊服務業之數位創新動能

1. 本部透過補助資源引導軟體與資服業者投入創新研發，並藉由多元管道協助企業募資、交流合作。114 年強化企業提升募資能力，率領 8 家曾獲獎補助的數位新創企業參與「WAVE(World AI Vision Exhibition) AI 2025」展會，並同步辦理 16 場次募資媒合活動，促成潛在合作契機。
2. 世界創新科技與服務聯盟 (WITSA) 肯定我國於 AI 供應鏈中關鍵地位，特邀我國於 114 年 8 月 18 日至 21 日主辦全球首屆「全球 AI 高峰會 (WITSA Global AI Summit)」，強化數位產業國際交流合作。本部亦持續進行成效追蹤，盤點具實用性、技術創新性及產業應用潛力的軟體與資服業者，發展具潛力的數位創新技術與新興商業模式，作為後續產業推動及政策規劃的重要參考。

(五) 輔導資服業發展創新雲服務

本部透過協助資服業者發展產業需求 AI 雲服務產品方案，並藉由服務擴散機制，推動百工百業數位轉型。113 至 114 年底，已經輔導 88 家資服業者，新增投資金額達 7.55 億元，並帶動 4,614 家中小企業導入 SaaS 雲端服務，促成中小微企業新增營收累計達 8.86 億元。同時，透過 AWS、微軟、Google 等國際大廠合作辦理技術工作坊，協助 6 家資服業者成功上架國際雲平臺。

115 年將持續推動 AI 數位雲主題式輔導計畫、辦理 Demo Day 等推廣活動，並輔導我國雲服務業者拓展至國際雲平臺，協助百工百業導入 AI 工具，預計推動至少 10

項 AI 雲服務產品方案，帶動資服業者新增投資規模達 6 億元，促進資服業者上雲率逐年提升，並輔導 4,200 家次中小企業導入雲服務，促進產業營收成長達 7 億元。

(六) 推動 5G 專頻專網創新應用落地實證及擴散

1. 本部自 112 年 6 月公布施行「行動寬頻專用電信網路設置使用管理辦法」。截至 115 年 2 月底，累計完成審查 142 案，其中已經核發行動寬頻專用電信網路執照 127 案、免發照 32 案。
2. 持續推動通傳創新應用的深耕與擴散，透過導入 AI RAN、5G Advanced 等先進通傳科技應用，加速創新商業模式發展，同時整合 10 家以上通傳應用方案供應商，將通傳科技應用效益擴大至 100 家以上企業。

(七) 推動新聞業與大型數位平臺共榮機制

1. 本部與通傳會及文化部依據「國內產業與大型數位平臺共榮發展協調小組」會議決議，先後召開三輪、計 8 場大型數位平臺與新聞產業對話會議，促進各方交流與共識凝聚。Google「臺灣新聞數位共榮基金」亦持續協助新聞產業數位轉型，目前已經完成六梯次獎助計畫，共計 61 件計畫獲得獎助，其中影響力專案獎助 17 件、標準獎助 27 件、基本獎助 17 件。
2. 本部將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，包括運用新興科技、促進數位轉型及發展訂閱制等新型商業模式（例如 Google 協助新聞業發展訂閱制的「北極星計畫」）。

(八) 從基礎建設到實戰應用，建構臺灣 AI 代理人全方位布局

面對日新月異的 AI Agent 技術發展，本部將以 AI Agent 產品化帶動資服軟體業轉型，除賦能臺灣產業也能以輸出海外為目標，透過公協會整合產業需求與各領域場域實證，建立 AI Agent 技術從試驗、驗證到擴散之完整路徑，確保技術發展能實際回應產業與社會需求，奠定 AI Agent 應用落地之基礎，同時深化連結國際平臺與大廠，協助本土 AI Agent 解決方案，以硬帶軟模式進軍國際市場，並強化垂直領域之競爭力，形塑以出口導向為目標之 AI 產業生態。

另將協助資服業者提升模型輕量化技術能力，開發可模組化、快速部署的 AI Agent 解決方案，並透過垂直領域場域（健康照護、零售服務）進行應用驗證，形成可複製的產品或服務，進一步串聯公協會或系統整合（SI）夥伴建立推廣通路，加速產業應用規模化擴散。

(九) 掌握資安產業前瞻技術，推動資安產業發展

1. 本部聚焦後量子密碼關鍵技術研發及產業發展，已經完成符合國際標準晶片電路設計（IP），支援 3 項美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）公告演算法，並通過密碼演算法驗證計畫（Cryptographic Algorithm Validation Program, CAVP）認證，與業者合作推出具備後量子加密能力的資安產品。另自主研發「後量子晶片安全」及「後量子場域應用安全」檢測工具，可協助國內廠商縮減約 30% 的檢測時間與 50% 的檢測成本。114 年已發布我國首部「後量子密碼遷移指引」，透過輔導金融、軍工及醫療等 10 家大型機構進行系統盤點，加速產業

與國際接軌。115 年將持續推動後量子密碼晶片產品化及相關認證作業，深化後量子晶片錯誤注入及場域安全檢測技術研發，並輔導高隱私、高可靠性產業進行遷移實證。

2. 本部因應國防資安需求，推動軍民通用資安技術研發及應用，迄今已經透過補助機制累計推動 44 案計畫，有效強化我國資安技術的自主研發能量。115 年透過「需求導向」與「成果導向」雙軌方式進行徵案，除配合國防部「產業化圓桌會議」的國防資安需求外，亦同步鼓勵具備潛力的廠商投入軍民通用資安技術研發。
3. 為協助我國資安產業拓展全球國際市場，114 年本部於「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 31 家企業來臺並對接 85 場媒合活動，並率 29 家次我國資安廠商赴荷、日、馬、泰等國參加當地國際資安展會或媒合活動，累計促成 11 項跨國合作案。115 年除持續深耕既有資安產業市場外，更將首度率領 8 家本土資安廠商參與全球最具指標性之美國 RSAC 展會及設立「臺灣資安館」，協助我國產業拓展海外商機。

(十) 落實數位信任基礎，強化數位產業韌性

1. AI 評測促進可信任 AI 發展

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 114 年 12 月底，累積完成業者送測的產品與模型共計 90 項。另由 AIEC 自主評測國際大廠相關開源語言模型計 77 項，並結合高中學測與臺灣價值題型進行測試，作為各界建構在地模型或調校國際模型的重要參考依據。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。

115 年 AIEC 預計累計完成測試 145 項國內外開源語言模型的基準評測結果，藉由系統性揭露評測成果，降低產業導入人工智慧的試誤成本，協助企業依不同應用情境選擇適切模型。另因應 AI 基本法，AIEC 可提供各部會建立 AI 評測機制的專業諮詢、技術支援及評測服務，並針對兒少、性平、人權或臺灣在地化等特定應用領域，規劃與相關部會合作，提供或建議評估驗證的工具與方法。同時，將持續擴大國際 AI 評測合作網絡，規劃串接美國 UL Solutions，就 UL 3115 AI 驗證方案展開合作，協助於臺灣先行導入與測試相關驗證流程，作為我國建構 AI 評測機制與國際接軌的重要示範案例；並延續與法國 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。

2. 強化產業資安防護能量

- (1) 為強化國內半導體產業供應鏈安全，本部積極推動 SEMI E187 合規輔導機制，並於 114 年 12 月 18 日與國際半導體產業協會（SEMI）共同發布 SEMI E187 半導體設備資安標準認驗證制度，象

- 徵我國半導體設備資安正式邁入制度化及實務化推動階段。115 年將開放實驗室及驗證機構申請作業，並頒發國際首批 SEMI E187 資安驗證標章。
- (2) 因應資安威脅日漸升高，為強化我國產業資安防護能力，114 年已經媒合資安廠商協助場域業者導入具零信任三階段架構的解決方案，輔導 3 案場域業者及其 15 家供應鏈廠商共同提升資安防護能量。115 年將聚焦具國際級供應鏈地位的場域業者，持續媒合資安廠商擴大零信任解決方案導入規模。
 - (3) 為擴大產業資安意識的推廣與落實，114 年與國內產業公協會合作推動產業資安強化工作小組，整合資安顧問資源，透過資安評級與企業曝險分析機制，協助 108 家企業掌握資安自理成熟度。115 年將進一步納入資安曝險指標，協助企業能全面掌握資安風險，並引導企業需求轉化為國內資安產業潛在商機。
 - (4) 為協助我國國防及關鍵產業接軌美國網路安全成熟度模型認證（Cybersecurity Maturity Model Certification, CMMC）資安規範，114 年透過 3 月及 9 月辦理的臺美交流會議，建立與美方政策溝通及合作機制，即時掌握 CMMC 最新政策動向與實務要求；並於 9 月與美方國防工業基地網路安全評估中心（Defense Industrial Base Cybersecurity Assessment Center, DIBCAC）完成聯合評鑑作業，實際驗證國內業者導入成效。同時，輔導包括電子

產品設計、金屬加工等 7 家關鍵產業的業者完成 CMMC 導入，強化關鍵產業供應鏈的資安治理能力，並為我國逐步建構具可複製、可擴散的 CMMC 合規落地模式。115 年除延續既有推動工作外，另建置 CMMC 資安合規系統，提供國內關鍵產業廠商自評作業，強化稽核前的合規準備能力。

- (5) 本部於 114 年 8 月 6 日公告《資通訊供應鏈晶片產品資安驗證制度》，做為推動晶片安全驗證實驗室設立及產品驗證作業的核心依循文件，協助半導體產業落實晶片產品資訊安全合規要求，接軌國際標準。同時輔導推動業界成立首座晶片資安檢測實驗室及驗證機構，並向財團法人全國認證基金會（Taiwan Accreditation Foundation，TAF）申請 ISO 認證，作為晶片安全驗證生態系基礎；後續將輔導晶片業者導入晶片安全標準，強化產業實務應用，推動國內晶片產業拓展國際市場。

四、推動數位經濟防詐措施，建構可信任的產業發展環境

（一）精進「網路詐騙通報查詢網」

1. 本部已經建置「網路詐騙通報查詢網」，提供民眾即時查詢與通報可疑網路詐騙訊息的服務，以提升詐騙偵測效率及防範能量，持續守護網路環境安全。自 113 年 9 月 30 日至 115 年 2 月底，共有 5 萬 4,070 位民眾下載使用，1 萬 8,831 人透過 APP 通報案件，總計通報 62 萬 3,007 則疑似詐騙訊息。其中 30 萬 1,440 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 1 萬則詐騙訊息依本部通知要求下架。

2. 另本部自 112 年 12 月起推動「詐騙樣態分析」，針對網路廣告平臺進行高風險詐騙案件掃描，並導入「網路詐騙通報查詢網」作為案件比對與預警依據。截至 115 年 2 月底，掃獲高風險金融投資廣告案件數已經由單週最高 7 萬 7,484 件下降至平均每週 237 件，降幅達到 99%；掃獲身分冒充詐騙廣告案件數已經由單週最高 3 萬 8,139 件下降至平均每週 382 件，降幅達到 99%。
3. 為落實納管平臺下架詐騙廣告的義務，115 年「網路詐騙通報查詢網」將增設「詐騙訊息下架檢核功能」，為後續法規遵循及成效分析提供關鍵數據。此外，本部將建置「網路詐騙情資資料庫」，透過分析詐騙傳播鏈，以掌握其運作模式；同時導入「AI 詐騙情境感知對話系統」主動蒐集情資，並將資訊提供警政單位，強化跨部門防詐協作效能。

(二) 持續落實源頭防詐，打造安全的數位環境

1. 114 年依《詐欺犯罪危害防制條例》新增公告納管 Meta (Threads) 平臺，目前符合一定規模的網路廣告平臺業者名單計有 Google (Google、YouTube)、LINE (LY Corporation)、Meta (Facebook、Instagram、Threads) 以及 TikTok (TikTok) 等 4 家業者，共 7 個平臺。本部將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，滾動式檢討更新納管業者名單。
2. 114 年公告納管的 4 家業者皆依《詐欺犯罪危害防制條例》辦理身分驗證及訂定詐欺防制計畫，並於 114 年 12 月底公布詐欺防制透明度報告，以利公眾瞭解網路廣

告平臺業者對於詐欺所採取的因應策略及相關措施落實情形。115 年將持續輔導業者精進防詐計畫及身分驗證技術，要求業者依防詐計畫執行及定期發布透明度報告，並輔導業者落實法遵。

3. 相關配套子法發布後，可促使網路廣告平臺業者全面落實法遵義務，逐步達到「減少接觸、減少誤信、減少損害」的三減目標，從源頭防堵詐騙，建構更安全可信的數位環境。114 年針對 Meta 違反《詐欺犯罪危害防制條例》裁罰 4 次，裁處計 1,850 萬元罰鍰。115 年將持續督促業者恪遵法規，確實履行資訊揭露與源頭管理責任。

(三) 提升第三方支付環境安全與透明度

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，三支能量登錄已經屬類許可制度，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 2 月底，通過能量登錄業者 52 家，廢止登錄 24 家，有效期屆滿失效 1 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、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 2 月底，已查核 1 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 2 月底，累計查詢約 3 萬 9 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）防止遊戲點數成為詐騙工具

1. 自 111 年 8 月起至 115 年 2 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 27 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 OTP 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 2 月底已經凍結異常帳號數逾 5 萬 4,371 件，攔阻總金額逾新臺幣 3 億 4,630 萬元。

（五）加強電商業者資安維護及法遵輔導

1. 本部積極辦理電商業者行政檢查，已經於 111 年 12 月至 114 年 12 月底，針對高風險、保有大量個資的業者累計辦理 54 家次行政檢查。115 年將持續強化電商個資保護，預計辦理行政檢查 10 家次，並以輔導方式協

助至少 10 家中小型電商業者法遵。

2. 本部強化輔導電商業者資安防護能力已經具成效，114 年全年內政部警政署於 165 全民防騙網中所公告的高風險賣場名單中，已經無本部主管的大型電商業者。
3. 另為協助各主管機關處理違禁品下架事宜及輔導業者法遵，本部定期邀集作用法的目的事業主管機關、國內三大無店面公協會、4 家大型 C2C 電商業者及 4 家納管的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 114 年底，共計召開 6 次會議，處理 50 項提案，使目的事業主管機關與業者溝通，共同強化業者法遵意識。115 年本部規劃持續辦理，以提升下架處理效率。

(六) 完善電子簽章發展法制，打造可信任數位環境

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 2 月底，已經核准 9 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，建構國內完整的電子簽章產業地圖，並進一步促進產業發展與跨界採用。
3. 115 年將持續推動產業應用擴散，國內端規劃串連公協

會協力電子簽章業者，參與相關活動推廣電子簽章多元應用，以因應產業對於電子簽章服務的需求。在國外端規劃就臺日旅遊觀光、飯店與交通租賃、不動產、製造業供應鏈、保健照護等場域導入電子簽章技術產出典範案例，作為臺灣電子簽章國際化示範。在國際技術接軌方面，規劃推動電子簽章第三方符合性評鑑認證機制，開發電子簽章國際技術標準檢測工具，確保我國法規、制度及技術與國際標準對齊。

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) 第七期「國家資通安全發展方案（114年至117年）」作為我國推動資安防護策略與計畫之上位政策依據，藉由政府擴大資安產業規模，與產業共同培育資安人才，進而推動廠商提升資安產品防護效能；將培育後的人才重新投入政府及產業，串聯政府、產業、人才三要素之正向循環，構建全面的資安防護體系；本方案四大策略推動重點如下

1. 全社會資安防禦：完成政府機關多元儲備資安人才方式，並提升全民資安職能及意識，完善國家資安應變機制，建構全社會資安防護網。
2. 提升關鍵基礎設施資安韌性：強化我國關鍵基礎設施資通安全，提升關鍵基礎設施資安聯防能量，建立關鍵基礎設施資安防禦體系，強化關鍵基礎設施防禦綜效。
3. 壯大我國資安產業：推動資通產品檢測驗證制度、驗證標準接軌國際；強化政府採購供應鏈風險管理，降低風

險發生與衝擊；擴大資安產業規模與提高國內資安產值，並向國際輸出。

4. AI 新興資安科技應用與合作：透過 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，建立主動防禦機制提升資安防護能量，並強化新興資安科技前瞻研究，促進國際資安交流合作，鏈結國際夥伴信任關係。

(二) 本部偕同中央各部會推動資安防護，透過年度進程之蒐整與管考，藉以確保各項措施貼近實務需求與國家資通安全政策方向。在如期如質達成年度目標的基礎上，進而發揮國家整體資安聯防綜效，共同建構信賴安全之數位社會。

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 (CI) 領域之資安防護基準，已核定能源領域、水資源領域、交通領域及緊急救援、醫院等 4 領域資安防護基準。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 3 月底，已有

224 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 37 項產品通過驗證。

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。
- (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 15 家重要資訊廠商實地稽核。

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 3 月已投入資安工作約計 150 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，自 114 年辦理資安職能訓練課程培訓逾 2,917 人次；另辦理資安長共識營、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、資通安全防護巡迴研討會等，培訓共計逾 5,000 人次參與。
- (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，並擴大資安人員增支專業加給適用機關範圍及支給對象條件；此外，並設置績效評核獎勵機制，期藉由鼓勵績效優良之機關及資安人員，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子法修法作業，相關 8 部子法亦於 114 年 12 月至 115 年 1 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，以及公務機關發配供業務使用之資通通訊設備，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、構建國家數位安全防禦基礎

(一) 建立全社會資安防禦能力

1. 為協助我國建構全社會資安防禦能量，國家資通安全研究院（下稱資安院）自 114 年起推動建置 LLM（Large Language Model）資安報表產生器，運用 AI 技術實現資安分析自動化，期能將龐雜報告轉化為資安治理情報。本年度已完成「資安自評報告分析產製技術」開發，可分析機關自評表並自動產出資安輔導建議草案，有助提升資安服務團業務執行效率；另已完成 LLM 趨勢分析與研判能力驗證，確認 AI 具備比對多期檢測數據差異及產出資安治理情報之量能。
2. 114 年度已完成目擊情資 AI 關聯分析相關核心技術之研發，逐步建構由人工判讀轉向自動化分析之技術基礎。相關成果涵蓋酬載來源鑑別、蜜罐攻擊誘捕、惡意郵件誘捕、威脅態勢預警、新興漏洞概念性驗證（PoC）初步判別，

以及資安檢測與資安鑑識之 AI 化，並納入開放來源情資 (OSINT) 之可信度判別機制，共完成 8 項關鍵目擊情資 AI 關聯技術，以提升我國對資安威脅之即時掌握與應變效率，並降低高度仰賴人工分析負荷與時效限制。

(二) 保護國家關鍵基礎設施

為強化國家關鍵基礎設施之資安防護能量，114 年度已成立關鍵基礎設施資安防護檢測團隊，並持續厚實檢測人員之專業技術與實務能力。同步推動關鍵基礎設施資安防護檢測作業，依風險導向原則執行相關檢測，並完成檢測標準作業程序之建置，以確保檢測流程具備一致性。另為因應資安威脅樣態快速演變，亦同步調查導入 AI 導向自動化檢測工具之需求，作為後續提升檢測效率與擴充防護量能之重要參考。

(三) 推動數位訊息分析技術研發

1. 資數位訊息威脅情資研究

為提升詐騙威脅資訊之共享與分析效率，114 年度已制定詐騙威脅情資描述與交換框架 FIST (Fraud Incident Structured Threat Framework)，標準化詐騙威脅情資的描述方式，使相關情資更易於比對與分析，作為推動自動化分析與防詐機制之基礎。同時，為減輕人工判讀大量數位威脅訊息之負擔，已完成數位訊息威脅情資識別技術之研發與建置，以系統自動整理與整合分散訊息，轉化為具脈絡之威脅事件分析報告。另就新型態訊息風險研析，完成錯假訊息公眾預測市場之概念性驗證，以分析群體對錯假訊息之認知與判斷趨勢，以提供政策研析與防制策略規劃之參考依據。

2. 多來源訊息傳播研究

為掌握數位訊息跨來源快速擴散之特性，114 年度持續推動多來源訊息傳播研究，強化多來源訊息分析技術與預警機制，以研判訊息於不同來源與管道間之傳播態勢及潛在風險。同時，完成簡體及繁體中文開源情資分析技術之概念性驗證，作為支援跨語系訊息分析與整合研判之研究基礎，強化我國面對跨境訊息影響之因應能力。

另就公共訊息傳播生態研析，研擬公共訊息分潤機制，並完成公共訊息閱聽行為之概念驗證，作為後續觀察公共訊息傳播誘因、理解閱聽行為特性以及相關政策之參考。

3. 人工智慧威脅研究

114 年度推動人工智慧威脅研究，聚焦於偽造內容之辨識與防制。相關研究建置可同時處理語音、文字及影音之多模態資料擷取與分析機制，作為人工智慧威脅偵測之前端引擎，以提升對深偽影音等詐騙手法之識別能力。另透過提供標準化介接機制，支援威脅偵測流程自動化與跨系統導入，作為強化防詐應變效率、降低民眾受騙風險之重要技術基礎。

二、公私協力建立人工智慧應用與服務能量

(一) 公私協力建立資安防護與服務量能

為協助機關與企業於採購資安服務時具備客觀評估依據，資安院於 114 年度完成具公正性與專業性的第三方資安服務評鑑機制規劃，針對資安健診、弱點掃描、滲透測試、社交工程及 SOC 服務等五類常見資安服務，研擬標準化之評估項目與分析架構，作為後續推動評鑑機制之基礎。相關規劃係彙整公協會訪談與產業意見，並據以界定

服務對象、角色分工及分階段推動方式，以兼顧制度可行性與資源運用效益。

(二) 厚植資安人才培育系統

1. 以「全社會防禦韌性」為目標，持續深化進階資安人才之實務培育模式。114 年度以關鍵基礎設施資安防護需求為主要實踐場域，推動數位靶場與資通安全桌上推演相關規劃，透過蒐集國內外 OT (Operational Technology) 情境案例與產業實務需求，完成數位靶場需求分析、架構規劃及演練腳本發展方向，作為分層培育資安專業人員及強化跨單位應變協作能力之重要基礎，形塑貼近實務的進階人才培育環境。
2. 有關產業資安人才的在職訓練，114 年聚焦能源、水資源及電力等關鍵基礎設施領域，完成多場資通安全桌上推演相關座談與專家諮詢，相關成果已納入桌上推演情境設計與演練規劃，作為後續提升在職人員風險辨識與決策判斷能力的核心訓練基礎。
3. 對於進階人才的培育強調「以戰代訓」的實戰精神，重點投入數位靶場與資通安全桌上推演的設計與驗證，成立專責演練團隊，完成多場演練驗證作業。

(三) 提升全社會資安動能

1. 為強化我國產品資安治理能力與國際競爭力，資安院以「產品上市前、產品上市中、產品上市後」三階段推動策略為主軸，推動產品供應鏈資安治理。114 年度已辦理我國首次大規模產品漏洞獵捕活動，聯合國內指標性資通設備廠商與本土資安研究社群，針對網通設備、儲存設備及工業通訊設備等關鍵產品進行實測，將過往以被動

修補為主的產品資安作法，轉化為主動風險發掘與提前修補之治理模式。

2. 透過推動漏洞獵捕制度，協助產業將資安納入產品研發與維運流程，並促進本土資安研究能量與產業實務接軌，形塑可持續推動之產品資安生態系。相關成果有助於提升「台灣製造」產品於國際市場之安全信任度，進一步提升全社會之資安防護動能。

三、成為國家資安治理政策智庫

(一) 建立資安政策研究團隊

為協助政府及早掌握國際資安政策趨勢與法制動態，資安院政策研究團隊持續每週產出「國際資安政策法制觀測週報」，彙整分析各國資安政策、法規與治理作為，作為政策研析與實務推動之參考。截至 115 年 3 月，已於官網累計發布 122 期，協助政府機關及各界即時掌握國際資安政策發展。國際資安政策法制觀測週報亦獲多家平面媒體轉載與延伸報導，進而擴大政策資訊傳播效益，促進社會大眾對資安議題之關注，提升整體國人資安意識。

(二) 打造國家資安治理情資平台

1. 為強化我國資安治理的整體掌握能力，資安院以「看得到，才治得到；治得到，才管得好」，推動建置國家資安治理情資平台。114 年度以奠定基礎能力為主，透過彙整事件通報、聯防監控、外部曝險與漏洞攻擊等關鍵資訊，進行統計分析與趨勢研判，協治理機關從分散資料中掌握整體資安態勢與風險輪廓，並以概念驗證方式逐步建置資安週報平台，導入 AI 輔助機制，支援重點議題彙整與趨勢判讀，建立後續制度化推動之基礎。

2. 資安院已規劃以資安責任等級為主軸，整合 IT 資安治理成熟度、法令遵循、事件通報與外部曝險結果，建立由全貌到明細的分層檢視架構，並同步推動資安治理 AI 化，協助治理者進行整體判讀與風險研判，也讓被治理者能清楚對照自身資安管理現況與精進方向。
3. 資安院自 114 年 7 月起定期發布資安週報，截至 115 年 3 月已發布 37 期，並獲多家媒體轉載報導，逐步累積治理觀測經驗，強化政策研判基礎，推動我國資安治理體系朝向更具韌性與前瞻性的方向發展。