

貳拾、數位發展部主管

數位發展部主管包括數位發展部、數位產業署及資通安全署等 3 個機關，掌理促進全國通訊、資訊、資通安全、網路與傳播等數位產業發展、統籌數位治理與數位基礎建設，並促進數位經濟發展及加速國家數位轉型等業務。茲將 114 年度決算審核結果說明如次（有關歲入、歲出決算之審定及各項差異之原因分析等詳細內容，請至審計部全球資訊網/總決算審核報告/總決算審核報告查詢平台查閱）：

一、計畫實施之查核

業務計畫 7 項，下分工作計畫 10 項，包括民主網絡之連結與創新、數位韌性之應用與強化、健全政府數位服務基礎環境及人才培力、深化政府資通訊應用建設、促進資料多元創新應用、資通安全業務、促進數位創新動能轉型升級等重要施政項目，其中已執行完成者 5 項，尚在執行者 5 項，主要係數位發展部補助辦理「維運並精進衛星緊急應變驗證網路驗證計畫」及「運用 MOCN 技術建置雲端核網提升行動通訊網路韌性計畫」等案尚未完成驗收；數位產業署辦理「DIGITAL+數位創新補助平台計畫」等案補助款為追加預算，須經公告徵案及審查等，合約皆為跨年度，相關經費須保留繼續執行。

二、預算執行之審核

（一） 歲入預算數 24 億 6,079 萬餘元，決算審核結果，審定實現數 24 億 9,151 萬餘元，應收保留數 30 萬元，主要係數位產業署核處第三方支付服務廠商違反洗錢防制法相關規定逾期未繳納之罰鍰；合計決算審定數 24 億 9,181 萬餘元，較預算增加 3,102 萬餘元（1.26%），主要係廠商違反提供第三方支付服務之事業或人員防制洗錢及打擊資恐辦法等規定之罰鍰收入，及收回以前年度委辦費結餘款等雜項收入較預期增加。

（二） 以前年度歲入轉入數計 3,239 萬餘元，決算審核結果，審定實現數 2,298 萬餘元（70.97%）；減免（註銷）數 539 萬餘元（16.65%），主要係應收業者頻率使用費怠金，移送行政執行取得債權憑證，經核定註銷；應收保留數 400 萬餘元（12.37%），主要係數位產業署應收回「中小企業行動智慧應用計畫」補助款。

（三） 歲出原編列預算數 50 億 7,734 萬餘元，經追加預算 7 億 4,479 萬餘元，合計 58 億 2,214 萬餘元，決算審核結果，審定實現數 49 億 4,871 萬餘元（85.00%），應付保留數 6 億 5,995 萬餘元（11.34%），保留原因詳「一、計畫實施之查核」說明；合計決算審定數 56 億 867 萬餘元，預算賸餘 2 億 1,347 萬餘元（3.67%），主要係數位產業署及資通安全署實際進用員額較少之人事費結餘。

（四） 以前年度歲出轉入數計 4 億 9,535 萬餘元，決算審核結果，審定實現數 4 億 7,551 萬餘元（96.00%），減免（註銷）數 1,218 萬餘元（2.46%），主要係「國際資通安全發展及我國未來推動研析採購案」契約變更後之結餘款；應付保留數 765 萬餘元（1.54%），主要係「分散式驗證及授權系統建置案」尚在辦理履約爭議調解，相關經費須保留繼續執行。

三、重要審核意見

(一) 人工智慧基本法已公布施行，確立我國推動人工智慧技術與應用發展之方向，惟各領域人工智慧應用之資訊揭露作法不一或未完整揭露應用項目，允宜研謀改善。

政府於 115 年 1 月 14 日正式施行人工智慧基本法（下稱 AI 基本法），推動人工智慧（Artificial Intelligence, AI）之研發與應用，應在兼顧社會公益、數位平權、促進創新研發與強化國家競爭力之前提下，發展良善治理與基礎建設，並遵循永續發展與福祉、人類自主、隱私保護與資料治理、資安與安全、透明與可解釋、公平與不歧視、問責等原則（圖 1）；明定數位發展部應參考國際標準或規範，推動與國際介接之 AI 風險分類框架，協助各目的事業主管機關訂定以風險為基礎之管理規範，各目的事業主管機關亦負有風險評估、資訊揭露及內部控制等法定責任。經查執行情形，核有下列事項：



資料來源：整理自 AI 基本法。

1. AI 基本法已明定透明揭露與加強管理高風險 AI 之法定義務，並課予各級政府風險評估與內控責任，惟我國相關產業現行 AI 資訊揭露作法不一：AI 基本法第 4 條第 5 款規定，政府推動 AI 之研發與應用，應遵循「透明與可解釋」原則，AI 之產出應做適當資訊揭露或標記，以利評估可能風險，並瞭解對相關權益之影響，進而提升 AI 可信任度。同法第 5 條第 2 項規定，AI 產品或系統經中央目的事業主管機關會商數位發展部認定為高風險應用者，應明確標示注意事項或警語。另依國家科學及技術委員會人工智慧科研發展指引，有關透明性與可追溯性係指 AI 所生成之決策對於利害關係人有重大影響，為保障決策過程之公正性，在 AI 系統、軟體及演算法等技術發展與應用上，進行最低限度之資訊提供與揭露，以確保一般人得以知悉 AI 系統生成決策之要素。經查，芬蘭赫爾辛基市政府建立 AI 登記平臺，主動揭露市政府使用之 AI 系統，包括數據使用、不歧視、人類監督與風險管理等細節；荷蘭政府設置演算法登錄平臺，要求公部門公布其所使用具影響力或高風險之演算法資訊；新加坡 2024 年發布之生成式 AI 模型治理框架，提倡類似「食品標籤」揭露方式，要求開發者應標準化揭露之資訊內容包含使用資料、訓練基礎設施、評估結果、緩解與安全措施、風險與限制、預期用途及使用者資料保護等 7 項核心資訊，上開國家標準化揭露 AI 應用資訊之作法可提升資訊透明度，亦有助於形塑可信任 AI 開發與部署。我國 AI 應用資訊揭露或透明化實務，於醫療器材產業，衛生福利部食品藥物管理署 114 年 2 月公告 109 至 113 年間核准應用 AI/ML 之國產及國外輸入醫療器材許可清單，計有 50 項國產、116 項輸入產品，使用者可透過「醫療器材許可證查詢網站」，查詢核定產品說明書，內容包括產品描述、預期用途、產品效能、警告及注意事項，屬醫療器材管理法規定應公開查驗登記資料；另在安全監控產業，已從傳統監視設備，轉型為結合 AI、物聯網與雲端運算之智慧安防，經濟部產業發展署推動「安全監控產業推動平台」，公開「關鍵元件查核

通過清單」，由廠商自願登錄並揭露安控產品之硬體與晶片來源、韌體版本、資安防護功能等，以事業單位自願揭露為主，顯示各產業別之 AI 應用產出尚乏標準化資訊揭露或標記機制。鑑於 AI 基本法已明確揭示 AI 之產出應做適當資訊揭露，經函請行政院督促數位發展部研議 AI 應用之標準化資訊揭露機制，優先適用於公私部門高風險 AI 應用，以落實 AI 基本法所揭示之透明與風險治理原則。據復：數位發展部已研議對於高風險 AI 應用訂定判定原則及例示參考，以協助各部會評估 AI 應用風險之類別，提醒部會依 AI 基本法辦理相關事項。

2. 部分機關未完整提報及揭露 AI 應用項目，不利各界瞭解政府整體 AI 應用情形：

本部前於 114 年 2 月間建請行政院通盤檢討政府機關應用 AI 之資訊透明度及完整度，據復數位發展部建議依循「智慧國家 2.0 新綱領（2025-2028）」現有機制，由各部會定期提報相關推動成果，供社會大眾查詢與監督。經查，行政院智慧國家 2.0 推動小組於同年月公布「智慧國家方案（2021-2025）2024 年階段成果報告」，數位發展部於該報告彙整揭露行政院所屬機關計有 47 項 AI 應用項目，惟該部為推動政府部門導入 AI 及自動化決策技術之透明機制，提升民眾對政府應用 AI 之信任，於同年 4 月函請五院及所屬機關、地方政府及所屬機關查填 AI 應用調查表，據該部彙整清單，行政院所屬機關計有 151 項 AI 應用項目，與「智慧國家方案（2021-2025）2024 年階段成果報告」揭露 AI 應用項目僅 47 項，差異項數高達 104 項，顯示該報告未完整揭露各機關 AI 應用項目，不利各界瞭解政府整體 AI 應用情形。另查環境部已於其全球資訊網公告，所屬環境管理署應用 AI 技術建置「環保清運車輛裝置智慧物聯網」與「海岸廢棄物 AI 影像辨識」等 2 項資訊系統；化學物質管理署應用空拍遙測技術結合高光譜 AI 辨識技術，建置「戶外含石綿建材空間分布管理系統」，均與 AI 應用有關，惟未列入數位發展部彙整之 AI 應用清單；又農業部林業試驗所於其全球資訊網公告，採用空載高光譜結合 AI 辨識技術，建立「自動化偵測及分類樹種模型」，惟上述清單農業部無任何 AI 應用項目。經函請行政院督促數位發展部確實盤點及揭露 AI 應用情形，以確保政府機關 AI 運用資訊揭露之正確性與完整性。據復：「智慧國家方案（2021-2025）」年度成果報告旨在呈現政策執行績效，與數位發展部 114 年 4 月之 AI 應用調查統計基準不同，將持續關注國際 AI 應用資訊揭露發展趨勢，並研議相關盤點與揭露機制之必要性及可行性。

（二） 人工智慧應用日益普及，惟尚無風險評估及管理規範，允宜儘速依人工智慧基本法規定發布風險分類框架，強化人工智慧應用風險管理。

依人工智慧基本法（下稱 AI 基本法）第 16 條第 1 項規定，數位發展部應參考國際標準或規範，推動與國際介接之人工智慧（Artificial Intelligence, AI）風險分類框架，並應協助各目的事業主管機關訂定以風險為基礎之管理規範；同法第 19 條規定，政府使用 AI 執行業務或提供服務，應進行風險評估，規劃風險因應措施，並訂定使用規範或內控管理機制。又依立法院審議該法附帶決議，各級政府應於 AI 基本法公布後 6 個月內，檢討並完成已使用 AI 執行業務或提供服務的風險評估。經查，數位發展部已於 114 年配合 AI 基本法法制作業，參考主要國家、專業機構與智庫 AI 應用相關規範，研議「人工智慧風險分類框架」草案，並函詢各目的事業主管機關意見，惟截至本部查核日（115 年 4 月 20 日）止，尚未發布實施，各目的事業主管

機關因缺乏風險分類框架，致難以依 AI 基本法第 16 條第 1 項規定訂定以風險為基礎之管理規範，並影響各政府機關依同法第 19 條規定及上開立法院附帶決議，辦理 AI 應用風險評估及規劃風險因應措施等相關作業。另據該部提供中央各機關 AI 應用情形之彙整清單，計有內政部等 18 個部會及所屬機關（構）已推動 151 項 AI 應用項目，舉如：環境品質監測、天氣預測、稅務服務、差勤管理及公文寫作等，顯示各機關已陸續導入 AI 應用於施政服務或業務管理。另數位發展部於 115 年 2 月 3 日函頒「公部門人工智慧應用參考手冊」（下稱公部門 AI 手冊），內容涵括 AI 風險管理、治理架構及應用生命週期管理等實務指引，惟風險分類框架尚未發布實施，現行手冊內容有關風險評估部分，與未來正式框架恐有所落差，有待適時檢討修正。經函請行政院督導數位發展部儘速依 AI 基本法規定發布 AI 風險分類框架，並同步檢修公部門 AI 手冊相關規範，確保公部門 AI 應用有一致性風險分類標準及管理規範。據復：數位發展部已將 AI 風險分類框架草案報請行政院審議，俟核定後將對外公告並據以研擬風險評估檢核及內控管理範本供各機關參考。

（三） 運用人工智慧與大數據技術及透過公私協力推動數位經濟產業防詐工作，從源頭防堵詐欺犯罪降低民眾受詐風險，惟數產署及相關業者之管理及防詐機制，尚待檢討加強。

行政院自 114 年 1 月實施「新世代打擊詐欺策略行動綱領 2.0 版（114-115 年）」，由數位發展部負責數位經濟防詐工作，聚焦數位經濟產業，從源頭防堵詐欺犯罪，內容包含：透過源頭管理網路廣告平臺，從根本減少民眾接觸詐騙廣告機會；利用人工智慧（Artificial Intelligence, AI）與大數據技術降低詐騙廣告擴散；加強電商業者資安維護；串聯檢警調及公私協力產業聯防共同防堵第三方支付遭濫用；防制遊戲點數成為詐騙工具等。數位發展部為辦理相關業務，責由所屬數位產業署（下稱數產署）執行智慧防詐與數位信任應用發展相關工作，114 年度經費執行數 3 億 5,806 萬餘元。經查執行情形，核有下列事項：

1. 數產署已備查網路廣告平臺業者詐欺防制計畫，惟相關透明度報告未能揭示業者已落實執行主動防範詐欺廣告措施，主動識別並防堵詐欺廣告上架：依詐欺犯罪危害防制條例（下稱詐防條例）第 30 條第 2 項規定，網路廣告平臺業者（下稱平臺業者）應對其網路廣告服務遭利用為詐欺犯罪之風險進行分析及評估，據以訂定詐欺防制計畫，並每年發布詐欺防制透明度報告。數位發展部於 113 年 11 月 28 日公告，透明度報告內容應包含詐欺防制計畫實施摘要、依詐防條例第 32 條第 1 項規定移除廣告之統計數量及類型，與暫停提供用戶服務之統計數量，及其他數位經濟相關產業主管機關指定之事項。經查數產署已備查 Meta 等 4 大納管平臺業者提送之詐欺防制計畫，各業者均已訂定防堵上架等主動防範詐欺廣告措施，且依政府機關通報移除詐欺廣告及暫停提供用戶服務，並於 114 年底前發布透明度報告，惟僅有 TikTok 所提透明度報告揭露詐欺防制計畫所列主動防詐措施之成果，餘各業者尚未揭示，致無法確認是否已確實執行詐欺防制計畫相關防詐措施。次查數位發展部為降低民眾接觸網路詐欺廣告機會，責由數產署於 113 年 9 月 30 日建置「網路詐騙通報查詢網」，主動掃描監測網路詐騙訊息並供民

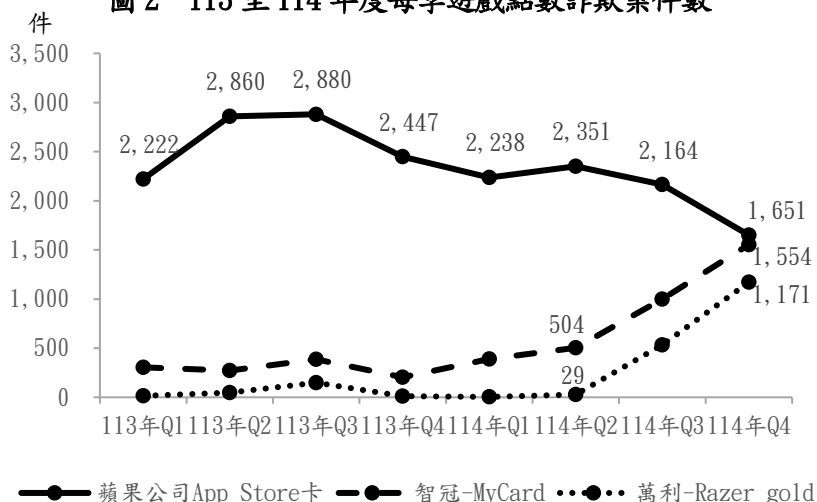
眾即時查閱及通報可疑網路詐欺廣告，截至 115 年 3 月 28 日止，共接獲疑似詐騙訊息 68 萬餘則，經分送各目的事業主管機關審核確認其中 32 萬餘則為詐欺廣告，已依詐防條例第 32 條規定通報 Meta 等 4 大平臺業者下架，顯示仍有大量詐欺廣告未能經由平臺業者主動防範措施於上架前發現，仍須耗費大量人力分送、審核確認、通報及追蹤下架詐欺廣告，增加相關人員工作負擔，經函請數產署督促納管平臺業者於第一道防線主動識別並防堵網路詐欺廣告上架，以提升防詐效能並減輕後端各機關人員工作負擔。據復：已邀集平臺業者召開研商會議，各業者均表示將精進主動防範詐欺廣告措施，並於透明度報告適時呈現防詐措施推動情形及具體成效，以利外界瞭解業者防詐作為。

2. 數產署建置「網路詐騙通報查詢網」執行民眾通報及運用 AI 自動掃描之詐騙廣告下架作業，惟自動掃描範圍不足且現行電子通報生效時程認定方式延後詐騙廣告下架期限：數產署建置「網路詐騙通報查詢網」供民眾即時查詢、通報可疑網路詐騙廣告，且於查詢網內運用 AI 自動化掃描機制監測網路詐騙訊息，過濾疑似詐騙廣告並通報下架。經查執行情形，核有：(1) 已建置「網路詐騙通報查詢網」通報下架詐騙廣告，並透過電子郵件及 API 串接方式，建立案件回報機制，惟就業者依限下架詐騙廣告之法遵事項落實情形缺乏主動監督查核機制；(2) 現行與業者協議以「次一日之翌日零時」為電子通報生效時程之認定方式，延後詐騙廣告下架期限；(3) 已建立 AI 掃描機制主動掃描詐騙廣告，惟尚未針對納管之 Google、LINE 及 TikTok 所營網路廣告平臺導入 AI 掃描機制，從源頭主動辨識廣告內容是否涉有詐欺；(4) 未導入 AI 掃描機制辨識各平臺業者是否確實揭露廣告委託刊播者及出資者相關資訊等情事，經函請數位發展部研謀改善。據復：(1) 將規劃建立自動化系統，定時掃描已通報下架之詐騙廣告連結，確保業者落實法遵依限下架，並於技術面持續透過功能開發以確保納管之網路平臺業者落實法遵事項；(2) 將檢討縮短原公告 24 小時內下架詐騙廣告期限之可行性；(3) 刻正規劃開發多平臺進件解析模組，逐步將納管網路廣告平臺導入 AI 掃描機制；(4) 目前針對 Facebook 網路廣告平臺積極開發數位工具主動掃描平臺廣告委託刊播者及出資者相關資訊，強化監管以減少民眾接觸及誤信詐騙廣告。

3. 數產署透過公私協力聯防機制推動遊戲點數詐欺防制措施，惟整體詐欺案件數並未有效下降，部分業者遊戲點數詐欺案件並有顯著提升情事：近年電玩遊戲產業蓬勃發展，遊戲點數在市場上大量流通，卻遭犯罪集團利用作為犯罪工具，成為洗錢及銷贓管道。數產署持續透過公私協力與所監管 5 大遊戲點數業者（遊戲橘子—Gash、智冠—MyCard、競舞—貝殼幣、網銀—遊 e 卡、萬利—Razer gold）合力推動身分驗證、一次性密碼、高風險帳號管理、延遲入點、防詐鎖卡平台等阻詐措施，並定期與蘋果公司及檢警調單位召開會議，檢視蘋果公司 Apple Store 禮品卡（下稱蘋果公司 App Store 卡）點數詐欺案件阻詐成效。在公私部門共同協力下，遊戲點數業者 113 及 114 年度協助攔阻詐欺金額超過 3.1 億元，然而遊戲點數整體詐欺案件數及金額雖於 113 年度下降至 1 萬 2,309 件、9 億 1,761 萬餘元，114 年度卻又再上升至 1 萬 4,727 件、10 億 8,115 萬餘元，其中蘋果公司 App Store 卡詐欺案件自 113 年第 1 季至 114 年第 3 季均大於 2 千件，至 114 年第 4 季始降至 1,651 件，惟仍占該季整體遊戲點數詐欺案件 4,517 件

之 36.55%；又智冠—MyCard 遊戲點數詐欺案件自 114 年第 2 季 504 件，大幅上升至 114 年第 4 季 1,554 件（占 34.40%），萬利—Razer gold 遊戲點數詐欺案件亦自 114 年第 2 季 29 件，大幅上升至 114 年第 4 季 1,171 件（占 25.92%）（圖 2），顯示蘋果公司 App Store 卡詐欺案件占比仍高，且智冠—MyCard 及萬利—Razer gold 遊戲點數詐欺案件均有大幅上升情形，數產署以公

圖 2 113 至 114 年度每季遊戲點數詐欺案件數



資料來源：整理自內政部刑事警察局提供資料。

私協力方式推動所轄遊戲點數業者執行之相關防詐措施，尚無法有效防制遊戲點數詐欺案件之發生，經函請數產署研謀因應改善策略，並督促遊戲點數業者及蘋果公司依據線上遊戲事業防制詐騙暨洗錢指引強化管控措施，以提升防堵遊戲點數詐欺成效。據復：針對詐騙案件數上升之業者，已加強每週召開阻詐成效檢視會議，加強輔導導入相關管控措施，並持續與蘋果公司及檢警單位共同研商更為有效之阻詐措施，定期檢視阻詐成效。

（四）數位發展部為數位經濟相關產業主管機關，督導社群媒體平臺及電商業者，惟部分社群媒體平臺之使用者帳號無預警遭停權；電商業者個資保護及跨境資料傳輸之監理機制未盡周全，高流量且未落地之跨境電商尚無監管規範，允宜研謀改善，以確保使用者權益並提升民眾個資保護。

數位發展部為數位經濟相關產業（下稱業者）主管機關，負責督導網際網路服務提供者，如 Facebook（下稱 FB）、Google、Instagram（下稱 IG）、YouTube 等，與電子購物及郵購業（下稱電商）相關產業之政策規劃、法規研擬、輔導及管理，已訂定「數位經濟相關產業個人資料檔案安全維護管理辦法」（下稱個資安維辦法），規範業者訂定個人資料檔案安全維護計畫及業務終止後個人資料處理方法（下稱個資安維計畫），並責由所屬數位產業署（下稱數產署）辦理行政檢查。經查執行情形，核有下列事項：

1. 部分社群媒體平臺之使用者無預警遭停權，尚待強化使用者權益保障措施：各國政府為保障民眾使用社群媒體平臺之權益及明確相關司法救濟及爭端機制，已陸續訂定關於社群媒體平臺之規範，國家通訊傳播委員會因應國際趨勢於 114 年 12 月 31 日發布網際網路服務使用者申訴及救濟機制指引（下稱申訴及救濟指引），做為網際網路服務提供者設計申訴及救濟機制之指南。經查，社群媒體平臺業者 Meta 運用人工智慧（Artificial Intelligence, AI）審查旗下 FB 及 IG 等平臺用戶行為，部分我國民眾帳號無預警遭停權，惟 Meta 通知停權違規事由過於簡化，且客服量能過低，致使用者權益受損且申訴困難，數位發展部為保障社群媒體平臺

使用者權益，已向 Meta 提出提高 AI 判別準確率、建立雙重確認機制、擴增客服量能、簡化公眾人物及網路意見領袖之藍勾勾驗證流程、強化社群守則之在地化教育與宣導及違規事由明確化等 6 大要求，惟 Meta 除已建立雙重確認機制外，餘就提高 AI 判別準確率等 5 項要求，尚未有具體精進措施或未改善完成，經函請數位發展部輔導相關網際網路服務提供者參考申訴及救濟指引建置申訴及救濟機制，並持續追蹤業者改善規劃及後續落實情形。據復：(1) 已邀集 Meta 及 Google 等四大平臺業者召開研商會議，促請業者參考申訴及救濟指引評估設立在地客服之可行性，其中 Meta 已建立跨國數位平臺常態化溝通與透明機制；(2) Meta 已承諾將持續投入資源改善其執行系統，及推出 AI 申訴輔助功能，提供 24 小時不間斷多國語言支援，並保留既有申訴管道，確保未復權用戶可獲得救濟，後續將持續督促業者完善相關平臺使用者之權益。

2. 數位發展部依法督導電商業者訂定個資安維計畫，並辦理行政檢查，惟尚無機制確認電商業者均已訂定個資安維計畫，部分大型電商業者近 3 年均未接受例行性行政檢查：數位發展部為促請電商業者落實會員個人資料（下稱個資）保護，依個人資料保護法（下稱個資保護法）第 27 條第 3 項規定訂定，並自 112 年 10 月 12 日公布施行個資安維辦法，依該辦法第 3 條規定，業者應於該辦法施行之日起 3 個月內，完成個資安維計畫之規劃及訂定，並據以執行之。經查數產署為了解電商業者個資安維計畫訂定情形，經評估電商市場後擇選 20 家電商業者，於 113 年 1 月 10 日函請業者提送個資安維計畫；並自 112 年至 115 年 3 月底止，依據個資保護法第 22 條第 1 項規定，辦理 31 家電商業者個資保護行政檢查計 65 次（包含個資外洩調查及例行性行政檢查），惟尚無機制確認其他電商業者均已訂定個資安維計畫。另有 7 家資本額 2 億元以上之大型電商業者，均保有用戶個資達 5,000 筆以上，惟數產署僅於 112 年曾因個資外洩事件進行檢查，尚未辦理例行性行政檢查，不易及早發現異常狀況並事先預警，以降低個資外洩風險，經函請數產署完善電商業者監理機制。據復：已針對國內電商平臺流量前 20 大之指標性業者逐步規劃實地查核，將持續要求大型業者落實個資安全維護。

3. 部分電商業者將保有之個資傳輸海外機房，依現行機制主管機關未能及時掌握電商業者保有之個資資料流向與風險變化：依據個資安維辦法第 10 條規定，業者將個資作國際傳輸者，應告知當事人其個資所欲國際傳輸之區域，同時監督資料接收方預定處理或利用個資之範圍、類別、特定目的、期間、地區、對象及方式等。經查，數產署主要透過辦理電商業者個資行政檢查，確認業者個資法遵落實情形，自 112 年至 115 年 3 月已檢查 65 家次，因個資安維辦法僅規範電商業者應訂定個資安維計畫，未要求業者於變更其個資之儲存地點、處理方式、委外對象或跨境傳輸範圍時，應提報主管機關更新個資安維計畫，爰現行機制未能及時掌握電商業者保有之個資之資料流向與風險變化，數產署須於辦理電商業者個資行政檢查時，始可確認業者個資儲存方式。114 年 11 月底酷澎韓國（Coupang Korea）發生個資外洩事件，引起國內外媒體關注及大幅報導，據數產署說明，酷澎股份有限公司（下稱酷澎臺灣）當時表示已由韓國政府及其委託之第三方資安公司調查中，尚無證據顯示臺灣用戶受影響，爰前於 114 年 12 月 24 日辦理酷澎臺灣之個資行政檢查，並持續進行調查該個資外洩事件，嗣酷澎臺灣至 115 年 2 月 23 日

向該署通報，確認涉及 20 萬餘名酷澎臺灣用戶之個資外洩，屬重大矚目之個資安維案件，該署遂將前次行政檢查未結部分併入於 115 年 2 月 25 日辦理酷澎臺灣個資外洩行政檢查，自事件發生歷經約 3 個月尚未完成調查。該事件顯示現況確有電商業者因機房設置海外，將個資作跨國或跨境之處理或利用，個資外洩事件發生時，處理耗時，主管機關不易即時掌握事故情形，致監管難度提升，經函請數產署強化電商業者跨境資料傳輸管理機制，以降低跨境個資處理所衍生之監管及事故查核困難與資安風險。據復：已正式要求酷澎臺灣評估用戶個資落地儲存之可行性，要求業者強化及精進個資保護，另將持續針對發生個資外洩、具高風險或保有大量個資之電商業者進行實地行政檢查，依循個資保護法相關規定，就電商業者資料安全管理、委託他人蒐集、處理或利用個資之適當監督等個資安全維護措施加強審視，以維國人權益。

4. 國人透過國外跨境電商平臺購物規模快速成長，惟高流量且未落地之跨境電商尚無監管規範：據未來流通研究所114年6月提出之跨境電商臺灣流量數據指出，臺灣已成為部分跨境電商之核心海外流量之一，舉如過去6個月間酷澎韓國（Coupang Korea）、中國淘寶海外站及美國亞馬遜（Amazon）來自臺灣之最高月流量達478萬人次、441萬人次及403萬人次（表1）。

另據該研究所115年3月提出之臺灣跨境電商進口數據顯示，2015至2025年近10年間臺灣進口小型包裹總量自1,883萬餘件上升至6,510萬餘件，增幅達245.8%；進口包裹金額自249億餘元上升至752億餘元，增幅達202.4%，進口總量及金額均創新高，且跨境電商進口規模已達境內電商市場之11.2%，均顯示消費者透過跨境電商平臺直購之跨境消費模式正快速普及。惟因相關跨境電商未在臺灣辦理公司登記，非屬數產署監管電商業者，尚無依據個資保護法及個資安維辦法等規範，針對業者進行

個資行政監督措施，以確認相關業者採取適當安全措施合理利用所蒐集之會員個資。經函請數產署研謀改善並適時揭露相關資訊，以提升民眾個資保護。據復：我國法令原則不具域外效力，對未在我國設立營業據點之境外平臺，尚難直接依我國法規進行行政管理或處分，已自113年起辦理友善電商甄選活動，將積極宣導消費者於網路購物時選擇有信譽之電商平臺，以保障消費者權益，糾紛發生時亦能有較妥適之處理機制。

（五）數位發展部推動智慧政府電子憑證及安全制度，維運政府機關憑證機構，惟管理傳輸層安全通訊協定（TLS）憑證有欠周妥，經主流瀏覽器取消信任，影響公共數位服務之穩定性與可信度，又尚未依據新版規範更新所管憑證實務作業基準（CPS），相關服務存有資安風險，允宜研謀改善。

表 1 高流量跨境電商業者名單

單位：萬人次／月

項次	業者名稱	電商平臺來源	臺灣流量	是否在臺灣辦理公司登記
1	蝦皮購物	臺灣	6,030	是
2	露天市集	臺灣	1,100	是
3	Coupang Korea	南韓	478	否
4	酷澎臺灣	臺灣	460	是
5	Pinkoi	臺灣	450	是
6	淘寶海外站	中國	441	否
7	Amazon	美國	403	否
8	樂天市場購物網	臺灣	400	是
9	Amazon JP	日本	200	否

註：1. 本表僅列出臺灣流量大於 200 萬人次／月之跨境電商業者。

2. 資料來源：整理自未來流通研究所 114 年 6 月「全球跨境電商臺灣流量產業地圖」。

政府為建立智慧政府電子憑證及安全制度，提供安全及可信賴之網路作業環境，設立行政機關電子憑證推行小組及維運政府機關公開金鑰基礎建設（Government Public Key Infrastructure, GPKI），相關業務自 111 年 8 月 27 日起由數位發展部承接，並擔任政府憑證總管理中心（Government Root Certification Authority, GRCA）、政府憑證管理中心（Government Certification Authority, GCA）、組織及團體憑證管理中心（mixed organization Certification Authority, XCA）及政府伺服器數位憑證管理中心（Government TLS Certification Authority, GTLSCA）之主管機關，及協調其他目的事業主管機關建置自然人憑證、工商憑證、醫事憑證等相關憑證機構（圖 3），另於 113 年 5 月 15 日修正公布電子簽章法，規定憑證機構應檢具憑證實務作業基準（Certification Practice Statement, CPS），載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關許可後，始得提供簽發憑證服務。又數位發展部於 111 至 114 年度辦理「政府公開金鑰基礎建設（委外）服務案」採購，採公開評選方式委由中華電信股份有限公司（下稱中華電信）辦理 GPKI 運作及管理業務（含維運 GTLSCA），決標金額 1 億 4,255 萬餘元。經查執行情形，核有下列事項：

圖 3 GPKI 架構圖



資料來源：擷取自數位發展部網站。

1. 數位發展部委託中華電信簽發之管理傳輸層安全通訊協定 (TLS) 憑證經 Google 取消預設信任，影響公共數位服務之穩定性與可信度：數位發展部負責 GPKI 業務，並連同 GTLSCA 委由中華電信營運，簽發與管理政府機關（構）之傳輸層安全通訊協定（Transport Layer Security, TLS）憑證，作為政府機關網站身分辨識及資料傳輸加密之數位基礎，並為確保所屬憑證機構之運作符合 GPKI 憑證政策與 CPS，及相關法規或規範，經建立稽核制度，每年委託第三方辦理憑證機構外部稽核作業。惟美商科高國際有限公司（下稱 Google）於 114 年 5 月 30 日聲明，因中華電信未能在期限內完成必要合規措施，導致信任度下降，因此最新版 Google Chrome 瀏覽器（下稱 Chrome）將移除預設信任該公司 114 年 7 月 31 日後簽發之 TLS 憑證，恐導致民眾連線政府機關網站受阻或誤判為不安全，衍生政府數位服務信任危機。經綜整原因，包含：（1）維運 GTLSCA 簽發之 TLS 憑證擴充金鑰欄位設定錯誤，且持續超過半年；（2）簽發憑證之延伸欄位屬性資訊不符相關規範，惟未依規定於 5 天內完成撤銷，且提出憑證用途與事實不符之解釋，損害其誠信與治理透明度；（3）辦理大規模憑證廢止作業，過程缺乏透明與追蹤紀錄，無法證明是否符合撤銷時限，違反憑證授權機制；（4）連續 2 年未依規定期限繳交合規性自評報告；（5）未依據 Chrome 根憑證政策完成提交憑證透明度日誌，致無法完整驗證憑證鏈，增加被攻擊風險；（6）過去 1 年處理公開事件，存有合規性未達標、改進承諾未兌現、缺乏持續且具體可驗證之改進計畫，亦未定期回報實際執行進度等問題，無法達到基本信任標準等。顯示中華電信管理維運 GTLSCA 持續未妥，且數位發展部辦理外部稽核與履約管理作業未盡周全，影響政府機關網站

於主流瀏覽器運作，及公共數位服務之穩定性與可信度，經函請數位發展部督促各政府機關網站完成憑證更新等因應措施，並檢討問題癥結督促改善，及研謀精進外部稽核及履約管理作業。據復：因應停止信任憑證，由中華電信協助各機關導入其他商業 TLS 憑證，並清查憑證更新情形，後續已提出建立跨團隊憑證檢核機制、稽核權利，及合約增訂罰則與違規衍生費用由承商承擔等履約強化措施。

2. 數位發展部已訂定新版數位簽章憑證實務作業基準（CPS）應載明事項，惟尚未更新所管 CPS，並影響其他部會 CPS 審查期程，致政府機關憑證機構相關服務存有資安風險：依據電子簽章法第 12 條規定，憑證機構應檢具 CPS，載明憑證機構經營或提供認證服務之相關作業程序，送經主管機關許可後，始得提供簽發憑證服務，前揭 CPS 應載明事項具體內容由主管機關公告之。數位發展部為促進數位簽章憑證實務作業接軌新版國際標準，於 113 年 11 月 14 日訂定數位簽章 CPS 應載明事項（下稱新版規範），嗣於 114 年 1 月 21 日函請經濟部等 6 個憑證機構於同年 5 月 16 日前，依新版規範調整所擬具之 15 個 CPS 送該部審查。截至本部查核日（114 年 11 月 19 日）止，中華電信等非政府機關憑證機構之 9 個 CPS，已依新版規範更新，並經數位發展部許可；內政部、衛生福利部及經濟部業分別於 114 年 6 月 4 日、6 月 11 日及 10 月 8 日提出 CPS 變更申請，據數位發展部說明，考量本次調整內容較為繁雜，將待各政府機關憑證機構提出 CPS 變更申請後，再併案共同審查。惟查該部迄未依據新版規範更新所管 3 個 CPS，致政府機關憑證機構仍持續依據舊有之 CPS 提供簽發憑證服務。鑑於新舊 CPS 應載明事項主要差異為明確數位簽章須具推定為用戶本人之效力，並參考國際標準新增相關作業流程、控管措施及個資保護措施等，包括：新增要求載明憑證用戶初始註冊之身分識別及認證程序所適用之保證等級強度須達國際標準、實體安全控管措施、危害及災變復原、電腦與網路安全控管措施及個人資料隱私保護等，憑證機構未依新版規範更新所管 CPS，恐致其提供之憑證服務存有資安風險，經函請數位發展部儘速更新所管 CPS，並加速政府機關 CPS 審查作業，以提升政府機關核發之憑證抗風險能力。據復：已完成更新轄下 GRCA、GCA 及 XCA 等所管 CPS，並納入後量子密碼學安全防護機制，以完善資安防禦體系及確保憑證服務穩健運行，尚待審查許可。

（六） 數位發展部為促進無線電頻率有效配置與合理運用，及因應 6G 發展之頻譜需求，辦理頻譜資源之整體規劃、整備、核配及管理，惟頻譜資源規劃透明度不足、已核配無線電頻率使用現況不明、行動寬頻單一業者可核配頻率上限未能切合產業現況、數位通傳資源管理系統效能尚待提升，允宜檢討改善。

無線電頻率之應用包含手機通訊、網路連線、電視廣播、災防無線電通訊、衛星訊號及智慧家庭裝置等，與民眾生活息息相關，無線電頻率資源之分配，並攸關我國資訊與通訊科技及通訊傳播等產業發展。數位發展部執掌通訊傳播與數位資源之整體規劃、推動及管理業務，負責國內無線電頻率資源管理、協調處理熱門無線電頻譜及頻譜供應政策，並委外建置數位通傳資源管理系統，辦理無線電頻率與電信號碼核配及收費管理等業務，114 年編列資源管理業務規劃及推動經費 7,669 萬餘元，實現數 7,157 萬餘元。經查執行情形，核有下列事項：

1. 無線電頻率資源分配 38 類用途，惟僅公告行動通信等 4 類用途之頻率供應規劃，尚有 34 類用途相關資訊未揭露，不利各界瞭解整體頻譜整備及供應規劃情形：依電信管理法第 52 條規定及其立法意旨，為整體通信與資訊發展之需要、促進無線電頻率之和諧有效共用，預留新技術發展空間，並因應國際趨勢，與世界接軌，使我國頻譜分配及規劃方向透明化，由行政院指定機關擬訂中華民國無線電頻率分配表（下稱頻率分配表）及無線電頻率供應計畫（下稱頻率供應計畫），其中頻率分配表應載明各類無線電用途之分配；頻率供應計畫應載明中長程頻率釋出、頻率重整、頻率共享及其他頻率供應之規劃。經查，數位發展部依國際無線電規則於 112 年 8 月修正頻率分配表，將無線電頻率資源分配予 38 類用途，惟僅將行動通信、衛星固定通信、衛星行動通信、廣播電視等 4 類主要商用無線電用途之頻率範圍與其使用現況，及短、中、長期頻率釋出規劃納入頻率供應計畫（114 年 2 月修正版），尚未就其餘 34 類用途揭露相關資訊，核與電信管理法第 52 條第 5 項公開頻譜資訊並提升規劃透明度及可預測性之立法意旨有間，不利各界瞭解整體頻譜整備及供應規劃情形。鑑於頻譜資源規劃透明化，可降低資訊落差，有助不同政府部門及早掌握頻譜釋出期程，強化跨機關協調與政策一致性；對產業而言，亦營造可預期之市場環境降低投資之不確定性，經函請數位發展部研議兼顧政策調整彈性之頻譜規劃發布範圍及機制，逐步落實頻譜資源規劃透明化。據復：將持續蒐研各類無線電用途之頻率使用情形及國際規劃趨勢，滾動檢討更新頻率規劃，並通盤審酌頻率供應計畫之內容及發布方式。

2. 無線電頻譜為有限資源，為因應 6G 發展之頻譜需求，允宜建立已核配無線電頻率使用現況盤點機制，適時辦理無線電頻率重耕，以提升頻譜資源利用效率：第六代行動通信技術（下稱 6G）為推動未來數位經濟、智慧城市與沉浸式應用的關鍵基礎，因應 6G 時代來臨，非地面網路（NTN）等新興應用快速崛起，對頻譜資源之需求日益攀升，爰須辦理頻譜重耕，重整及活化既有頻譜之效能。國際電信聯盟（International Telegraph Union）於 2023 年世界無線電通信大會研討 6G 使用頻譜資源，決議啟動 7—15GHz 頻段是否新增劃分給國際移動通信（6G）之研究，並將在 2027 年大會公布 6G 重耕頻譜及新頻段規劃，以厚植未來行動通訊基礎；另長期引領行動通訊標準的第三代合作夥伴計畫標準組織（3rd Generation Partnership Project）預期 6G 將於 2029 年第 4 季正式商用，爰我國已釋出之 700、900 及 1800MHz 等頻段，於 119 年屆期重新規劃釋出時，將為佈局 6G 發展資源之重要時點。經查，數位發展部重耕屆期頻譜先期規劃委託研究報告指出，2030 年合理情境之頻率需求介於 962 至 1,528MHz 之間，惟我國已釋出之低（1GHz 以下）、中（1—6GHz）頻段行動通信頻率共計 850MHz，低於未來合理情境之預估需求。又低頻段因其優越涵蓋能力與穿透性，被視為 6G 候選頻段中，支援廣域通信與非地面網路（NTN）之理想選擇，適用於偏遠地區、車聯網與物聯網等應用場景，為實現普及性行動通信之重要資源。惟行動通信潛在頻段中，低頻段多已核配，舉如警察、消防單位之部分專用電信頻率及提供「民生公共物聯網」等創新實驗網路使用。為因應 6G 發展之頻譜需求，及考量類比無線電提升為數位無線電等技術演進可降低專用電信之使用頻寬需求，經函請數位發展部研議建立已核配頻率使用現況盤點機制，據以滾動檢討特定實驗頻率需求，並適時辦理無線電頻譜重耕。據復：將通盤審酌低頻段創新實驗網路頻率資源之後續使用規劃，並於 115 至 116 年度盤點專用電信頻譜現況與需求，提出頻道規劃建議，以解決低頻段頻譜碎片化問題。

3. 為平衡資源分配與市場競爭，訂定行動寬頻單一業者可核配及使用頻寬不得逾1/3之規定，惟國內電信業者於112年由5家合併為3家，允宜因應產業現況檢討修正彈性上限規定：政府因應行動上網數據流量高速成長，辦理行動寬頻無線電頻率釋照作業，並為維持市場競爭，適當限制業者得使用頻率之頻寬，於104年7月16日修正發布行動寬頻業務管理規則第18條第2項規定，得標者或經營者申請核配總頻寬不得逾行動寬頻業務總頻寬之1/3；1GHz以下總頻寬不逾行動寬頻業務1GHz以下頻段總頻寬之1/3；另為維護市場公平競爭，促進頻率使用效益，於109年7月2日訂定發布無線電頻率使用管理辦法第12條第1項規定，電信事業實際可使用頻寬，1、3、6GHz以下分別不得逾該頻段經公開招標或拍賣可核配供整體電信事業使用頻率之總頻寬1/3。嗣後國內電信或行動寬頻業者於112年12月由5家合併為3家，遠傳電信股份有限公司合併後，於28GHz頻段實際可使用頻寬超出規定上限100MHz(下稱超額頻寬)；台灣大哥大股份有限公司(下稱台哥大公司)合併後，於900MHz頻段實際可使用頻寬超出規定上限10MHz，爰分別於113年5、9月繳回超額頻寬，惟數位發展部規劃俟該頻段使用期限於119年屆期後再統一釋出，致上開超額頻寬未能有效利用。據該部113年「無線電頻率需求及經濟效益資料模型建構」委託研究報告指出，各國為避免業者進行頻譜囤積等反競爭行為，多進行頻譜供需平衡評估措施，舉如：澳洲目前與我國同為3家主要電信業者，其於低頻設有82MHz或40%之上限規範，可避免頻譜資源過度集中單一業者，並保有適度競爭空間，以促進技術升級及產業發展，經函請數位發展部因應電信業者市場競爭狀況，參考先進國家作法，研議檢討單一業者可核配及使用頻寬上限之規定，並考量可因應市場變動之彈性。據復：將視台哥大公司超額頻寬繳回爭議之法院判決結果，適時檢討頻寬上限相關規定，另於辦理頻率釋出時，依據產業整併後之現況、市場競爭態勢及有無新進業者參進等因素，彈性訂定最合宜之頻寬上限。

4. 為促進資源有效配置及合理運用，建置數位通傳資源管理系統，惟對外服務網站建置完成後未上線提供民眾使用、對內系統管理及收費效能待提升：數位發展部為有效掌握整體數位通傳資源使用現況，促進資源有效配置及合理運用，於112年辦理數位通傳資源管理系統委外建置案，契約金額2,685萬餘元，並於113、114年辦理系統功能增修維運案，契約金額分別為469萬餘元及467萬餘元，服務內容包含建置數位通傳資源管理系統對外服務網站、電信資源(含無線電頻率及電信號碼)收費系統及無線電頻率管理系統等。經查執行情形，核有：(1)數位通傳資源管理系統對外服務網站建置完成後，並未上線提供民眾使用；(2)電信資源收費系統未因應行動通信頻率使用費計算基準修正，即時更正系統程式，且未善用系統線上繳費功能，仍以紙本方式寄發繳費通知書；(3)系統未登錄行動寬頻專用電信網路頻率核配資訊，亦未內建所有頻率用途類型之使用費調整係數，且已核配案件使用費調整係數存有錯漏，不利於頻率核配管控及收費管理等情事，經函請數位發展部檢討改善，以提升系統利用效能。據復：(1)後續開發相關系統將確實檢討需求，避免未發揮建置效益情形；(2)自115年起定期辦理系統版本更新，以確保各項功能配合法規修正即時調整並正常運作，另115年將開放電信事業線上繳費；(3)已完成系統調整及版本更新納入行動寬頻專用電信網路頻率核配資訊，並修正系統內26項頻率使用費調整係數。

(七) 數位發展部為因應數位憑證之使用情境需求日益增加，推動建立數位憑證皮夾系統，惟法制規範尚欠周全，且尚未串接發行數量眾多且民眾使用頻率高之證件，又已串接之數位憑證應用情境有限，允宜研謀改善。

數位發展部為因應數位憑證之使用情境需求日益增加，於數位憑證公共基礎建設計畫項下，推動建立用於數位證件發放、保存及查驗之數位憑證皮夾系統，奠定數位時代之公共基礎設施，以提供民眾更廣泛及便利之證件查驗服務，民眾可依照查驗場域需要，自由選擇欲揭露之數位證件資料(圖4)，113至117年度計畫經費共計5億8,900萬元，截至114年底止，累計實現數3億939萬餘元。經查執行情形，核有下列事項：

1. 我國數位憑證皮夾已正式上線供民眾使用，惟法制規範尚欠周全，恐影響其整體之信任及安全保障：依據數位憑證公共基礎建設計畫載述，為利各界佈建數位憑證皮夾及協助各政府機關推動數位憑證皮夾政策，規劃於114年訂定數位憑證皮夾佈建參考手冊，詳細說明各項技術及管理細節，並訂定數位憑證皮夾政府機關推動指引，協助政府機關逐步導入證件數位化；另將盤點並擬具法規調整建議，逐步完善我國法規，以利數位發展。經查，數位發展部建置之數位憑證皮夾系統已於114年12月17日正式上線供民眾使用，截至本部查核日(115年4月9日，下同)止，已完成串接三大電信業者電信門號電子卡、交通部公路局(下稱公路局)駕照驗證卡及數位發展部設計之訪客卡等3項數位憑證，提供民眾至便利商店領取免付費包裹、汽機車租賃及訪客登記等3項應用，惟尚未依原規劃期程訂定數位憑證皮夾之佈建參考手冊及政府機關推動指引，提供各界導入數位憑證皮夾之一致性標準，以減少爭議及風險，並提升導入數位憑證皮夾之意願。次查，數位發展部委託廠商辦理數位憑證皮夾相關法規調適研究報告載述，歐盟、紐西蘭及加拿大等國際組織或國家均已建立數位身分框架及數位憑證皮夾相關規範，針對相關服務提供者建立明確技術、信任服務及申請認證之細節要求與審查程序，並明定主管機關得採取之相關監管措施；暨於數位身分框架相關規範中明定，數位身分相關服務提供者應符合之特殊個資保護要求及資安防護義務，或要求相關服務提供者應公開揭露個資蒐集事項、目的及使用範圍等資訊。按我國電子簽章法偏重監管簽發數位簽章憑證(如自然人憑證及工商憑證等)之憑證機構，尚未涵蓋數位憑證皮夾及其所載未具數位簽章憑證(如健保卡及駕照等)之服務提供者；個人資料保護法尚無針對數位憑證皮夾相關個資保護之細節性要求，資通安全管理法亦僅列管公務機關及特定非公務機關，尚未涵蓋所有數位憑證皮夾之服務提供者，法制規範尚欠周全，恐影響其整體之信任及安全保障，經函請數位發展部研議健全相關法制規範，以利各界遵循。據復：刻

圖4 數位憑證皮夾系統特點及運作模式



資料來源：擷取自數位發展部及數位憑證皮夾網站。

正辦理法制化工作，持續進行內外部跨部會、跨產業溝通，預計於 116 年度發布數位憑證皮夾管理規範，以期兼顧安全保障並切合各界作業實務，建立可持續發展之信任生態系。

2. 數位憑證皮夾系統尚未串接發行數量眾多且民眾使用頻率高之證件，恐影響整體政策推動成效：自然人憑證、工商憑證、健保卡、技術士證及駕照等證件，為我國發行數量眾多且民眾使用頻率高之重要身分識別工具，廣泛應用於稅務申報、補助申請及就業求職等情境，數位發展部自 113 年起，已陸續與內政部、經濟部商業發展署（下稱商發署）、衛生福利部中央健康保險署（下稱健保署）、勞動部勞動力發展署（下稱勞發署）及公路局等發證機關協調，推動證件數位化及與數位憑證皮夾系統串接事宜，並於 113 年 12 月支應經費 3,746 萬元建置客製化

串接系統分別供商發署、健保署、勞發署及公路局等 4 個機關使用，以利後續串接數位憑證皮夾系統，惟截至本部查核日止，僅公路局之數位駕照（訂名為「駕照驗證卡」）已串接完成，供民眾應用於汽機車租賃時驗證身分及駕照相關資料；其餘機關囿於維運經費不足、法規配套未臻完備及評估推動效益有限等因素，尚未串接數位憑證皮夾系統（表 2），致部分已建置串接系統閒置，且恐影響數位憑證皮夾

表 2 已發行證件尚未串接數位憑證皮夾系統原因

發證機關	發行之證件	未串接數位憑證皮夾系統原因
內政部	自然人憑證	因現行內政部自然人憑證憑證實務作業基準之限制，尚未串接數位憑證皮夾系統。
商發署	工商憑證	尚與數位發展部研議民眾申請工商憑證納入數位憑證皮夾之流程。
健保署	健保卡	礙難支應系統軟硬體後續維運經費。
勞發署	技術士證	1. 現行數位憑證皮夾尚未訂定法律規範管理機制，且技術士證未綁定數位憑證皮夾持有者本人，恐有資安風險疑慮。 2. 驗證單位包含各級政府機關（構）、事業單位或公（工）協會等，現行尚無法全面就上開單位進行驗證系統開發，整體效益受限。 3. 115 年度勞發署技能檢定中心並未編列相關預算及配置人力辦理相關系統維運作業。

資料來源：整理自數位發展部提供資料。

整體政策推動成效及民眾使用意願，經函請數位發展部協同有關部會加速推動各類民眾生活常用證件之數位化與系統串接作業，以提升數位憑證皮夾之整體使用效益。據復：已加速推動多元證件串接工作，其中工商憑證電子卡已於 115 年 5 月正式上線，並就其餘證件尚未串接原因研擬相關解決方案，將持續與各部會、各產業商討並尋求合作意願及導入場域，以期將民眾使用頻率高之相關證件納入應用場景範圍。

3. 已串接數位憑證皮夾之數位憑證應用多侷限於單一場域及服務，應用情境有限：依據數位憑證公共基礎建設計畫載述，數位憑證皮夾推廣策略將採公部門與私部門雙軌併行，公部門方面將優先協助具高使用頻率之民眾端核心政府服務導入；私部門則以產業聚落為推廣重點，透過產業公協會管道擴散應用。經查，截至 115 年 3 月底止，數位憑證皮夾已完成串接三大電信業者電信門號電子卡等 3 項數位憑證，下載次數計有 100,096 人次，其中三大電信業者電信門號電子卡提供民眾至便利商店領取免付費包裹，已有 7-11 及全家等 2 家主要便利商店導入使用，累計使用次數 122,781 次，每下載人次平均使用 1.23 次；公路局駕照驗證卡提供民眾租車應用，已有國內 ZOCHA 租車（西門店）及華誼優盟股份有限公司板橋分公司導入使用，尚待擴及大型連鎖及國外汽機車租賃企業（如和運租車）；訪客卡提供訪客及合作廠商登記應用，已有數位發展部等 3 個單位導入使用（發證 712 次、驗證 522 次），尚待全面推廣或與門禁結合。鑑於現行已串接數位憑證皮夾之數位憑證應用多侷限於單一場域及服務，尚待推廣跨機關

服務及跨境應用，經函請數位發展部積極檢討推廣策略，拓展多元應用服務。據復：依循憑證發行機關之試辦意願與階段性目標，全力洽談跨機關與民間產業服務，115 年度將持續辦理數位憑證皮夾推廣活動，並規劃跨主管機關之多元應用治理政策機制。

(八) 數位發展部推動手機應用軟體與物聯網設備資安認(驗)證制度，惟手機內建軟體及物聯網資安標準推行停滯，又資安監理機制未完善，且部分公部門發行 App 未辦理資安認證或未即時更新公開資訊，允宜研謀改善。

數位發展部為配合政府五大信賴產業推動方案有關安控產業之政策目標，發展及落實資安產業標準規範及認(驗)證制度，作為我國資安產業基礎，112 至 114 年度於資安跨域整合聯防計畫項下，推動智慧型手機內建軟體、行動化應用軟體(下稱 App)與物聯網(Internet of Things, IoT)之資安標準、檢測基準與輔導產品檢測等業務，期能帶動相關產業發展及提升設備安全，經費執行數共計 1 億 1,605 萬餘元。經查執行情形，核有下列事項：

1. **數位發展部及所屬數產署推動手機應用軟體與物聯網設備資安認(驗)證制度，惟手機內建軟體及物聯網資安標準推行停滯：**依據行政院國家資通安全會報委員會議決議，手機之應用軟體基本資安規範由經濟部主管，其出廠時已內建之軟體併同硬體由國家通訊傳播委員會主管，並請二部會制訂資安檢測標準及鼓勵廠商自主驗證。另隨著 IoT 普及，前開機關合作自 107 年度針對 IoT 重點系統與設備，制定及推廣資安認(驗)證制度。數位發展部 111 年成立後承接手機內建軟體業務，數位產業署

表 3 資安認證項目概要

認證項目	認證標章	認證審定機構
手機內建軟體	E. S. S. 標章	中華民國資訊安全學會
自行下載 App	MAS 標章	行動應用資安聯盟
IoT 系統及設備	物聯網資安標章	

資料來源：整理自數位發展部及數產署提供資料。

(下稱數產署)承接 App 及 IoT 資安認(驗)證相關業務，並為協助資安產業發展，推動由民間組織自主辦理資安檢測及認證制度(表 3)。經查，智慧型手機系統內建軟體資通安全等級標章(Embedded Software Security, E. S. S.) 112 至 114 年度僅通過 2 件，最近一件取得標章時間為 112 年 9 月，113 及 114 年度均未有廠商送檢或取得標章，且截至 114 年底止，於認證有效期間之檢測實驗室僅 2 間，亦將於 115 年底屆期；又 IoT 相關產品 114 年度通過資安認證僅 5 件，較 113 年度之 27 件減少比率達 81.48%，其共計 7 項系統或裝置認證項目、20 項認證標準，僅影像監控系統之 4 項認證標準尚有檢測實驗室，餘消費性網路攝影機等 6 項系統或裝置、16 項認證標準之檢測實驗室均已終止服務(表 4)，經函請數位發展部及所屬數產署審慎掌握產

表 4 截至 114 年底 IoT 資安認證項目及合格實驗室概況

單位：項、間		
IoT 認證項目	認證標準項數	檢測實驗室數量
影像監控系統	4	9
消費性網路攝影機	1	—
空氣品質微型感測裝置	1	—
感測裝置	3	—
智慧路燈系統	2	—
智慧巴士資通訊系統	3	—
門禁系統	6	—

資料來源：整理自數產署提供資料。

業資安檢測需求，滾動調整推動策略，以完善整體資安認(驗)證制度。據復：將滾動檢討推動策略，並跟進產業國際趨勢與法規標準，如歐盟網路韌性法(Cyber Resilience Act, CRA)等最新規範，協助國內產業接軌國際資安準則，強化產品之國際競爭力。

2. App 資安監理機制未臻完善，部分領域尚無主動抽檢機制及高風險軟體因應措施：隨行動通訊技術發展與智慧型終端設備普及，App 已廣泛運用於民眾之食衣住行、金融支付、醫療掛號及政務申辦等各類生活場景與經濟活動。數位發展部為確保消費者使用智慧型手機安全，陸續於 112、113 年度針對市售 17 款熱門及中國廠牌手機內建軟體，挑選涉及個資、加密與付費安全等 12 項關鍵指標進行抽測。惟截至 115 年 4 月底止，除政府部門、金融機構及遊戲產業 App 之主管機關有強制辦理資安相關檢測外，其餘領域 App，舉如社交類、AI 生成式應用及非中資遊戲等，除由廠商自主申請檢驗外，尚無建立定期、常態化主動抽檢機制或常設監督措施，存有高度資安監管盲區。按「小紅書」等 App，前經國家安全局（下稱國安局）依據國家情報工作法蒐研各國資安調查報告及相關情訊，通報並統合由法務部調查局及內政部警政署刑事警察局抽檢後，於資料傳輸加密機制、系統權限過度要求及使用者個資存取路徑等方面存有顯著之資安風險，恐成為個人隱私外洩或國家安全資訊遭非法蒐集之管道，經函請數位發展部參酌手機內建軟體抽測之機制，建立 App 之主動抽驗機制及高風險 App 因應措施，以維護國家資通安全及使用者隱私。據復：已禁止公務機關下載、安裝或使用中製 App，又為強化我國民眾與企業資安防護意識，已與國安局等機關共同擬定中製 App 之資安檢測標準，針對高德地圖等 4 款高風險 App 進行資安檢測，並發布記者會勸導民眾避免使用高風險 App。

3. 部分公部門發行 App 未辦理資安認證或實際上架版本與認證版本不符，且未即時更新管理平臺資訊：依據行政院及所屬各機關行動化服務發展作業原則（下稱 App 作業原則）第 11 點規定，各機關開發之行動化服務應符合個人資料保護法及政府資通安全管理等相關規定，並通過數產署訂定 App 之檢測項目，始得提供民眾下載使用；第 12 點規定，行政院所屬二級機關應定期彙整其所屬機關（構）之行動化服務基本資訊，送數位發展部備查。數位發展部為利彙整行政院所屬機關（構）開發供民眾下載 App 之使用績效及資安檢測資料，於「我的 E 政府」網站建立管理平臺，並請行政院所屬機關（構）定期填報相關資料，維持 App 資安檢測之有效性及更新相關資訊。經查，截至 115 年 4 月底止，管理平臺上架 App 數量共計 127 個，其中 17 個為重複登錄或無效連結，餘 110 個中，有 9 個（8.18%）未有辦理資安檢測紀錄；22 個（20%）逾 1 年未辦理資安檢測；42 個（38.18%）於管理平臺未更新資安認證資料，顯示管理平臺提供民眾資訊正確性有待提升。又據行動應用資安聯盟揭露資訊，114 年 3 月至 115 年 4 月底止，公部門發行 App 取得資安認證共計 188 個，其中 75 個（39.89%）已公開發行且功能主要係提供民眾獲取政府服務，尚未上架於管理平臺，另 107 個（56.91%）上架於 App 商店供民眾下載使用版本與取得資安認證版本不符，經函請數位發展部研謀妥處。據復：已發函行政院及所屬各機關（構）依 App 作業原則落實辦理，並請未定期辦理資安檢測及未更新管理平臺資料之機關（構）限期完成改善，另規劃建置「MAS 資安標章版本異動監管系統」，針對取得資安標章之公部門 App，與 iOS 及 Android 雙平臺、管理平臺進行比對，針對版本不同者，鼓勵重新送測及取得標章，以提升我國行動化數位環境安全。

(九) 數位發展部及所屬補助地方政府資訊建設並推動配足資安專職人力，惟資訊建設相關補助計畫未妥訂效益管考規定，部分地方政府尚未配足資安專職人員；又已審查發現之危害國家資通安全產品未建置清單，部分地方政府仍使用大陸廠牌與已終止支援之資通訊產品，存有資安風險，允宜研謀改善。

數位發展部為推動地方政府優質資訊環境，提升地方政府資訊應用及服務之成效，補助地方政府資訊建設相關計畫；又為加速建構國家資通安全環境，依 108 年 1 月 1 日正式施行之資通安全管理法（下稱資安法），依該法授權訂定資通安全責任等級分級辦法，明定各公務機關應依其資通安全責任等級配置資安專職人力，並持續精進職能取得專業證照及訓練證書，以提升資安人力水準；復依 114 年 12 月修正施行之資安法第 11 條及行政院相關函令規定，公務機關不得下載安裝或使用危害國家資通安全產品，以落實資通系統之安全管理。經查數位發展部補助地方政府資訊建設及地方政府設置資安專職人員暨資通系統資安管理情形，核有下列事項：

1. 數位發展部為推動地方政府優質資訊環境，補助地方政府資訊建設相關計畫，惟未妥為訂定補助計畫效益管考規定：依據 114 年 8 月 29 日修正之中央對直轄市及縣（市）政府補助辦法第 11 條第 1 項規定：「中央各主管機關應就本機關與所屬機關補助款之執行，訂定共同性或個別計畫之管考規定；其管考內容及方式如下：……二、補助計畫執行之查核點及管考週期，並定期進行書面或實地查核。三、前款查核之項目，包括……執行完竣後使用之效益等。」數位發展部為推動地方政府優質資訊環境，提升地方政府資訊應用及服務之成效，訂定「數位發展部補助地方政府資訊建設計畫作業要點」（下稱資訊建設計畫作業要點），據以執行地方政府資訊建設相關計畫之補助作業，惟該要點未包含執行完竣後使用效益之查核相關規定，尚乏補助案件結案後之使用效益追蹤機制，經函請數位發展部檢討改善，以促請受補助單位審慎執行補助計畫，達成預期效益。據復：已修正資訊建設計畫作業要點，明定受補助機關應提報計畫執行完竣後之應用成效及分析，強化補助計畫管考強度。

2. 部分地方政府尚未配置足額資安人員、資安人員未全職執行資安業務，或以非資安專職人力補充資安人力缺口，且近 3 成資安人員取得之資安專業證照或職能訓練證書未達法定標準，有影響資安業務推動執行之虞：截至 114 年 9 月底止，各地方政府資安責任等級為 B 及 C 級機關者共計 608 個，

應配置資安人員人數下限 719 人(表 5)，其中 21 個機關以機關員額不足或資安人員離職尚未補足為由，未配置足額資安人員；已配置資安人員者計 588 個機關、698 人(含 587 個機關足額配置 697

表 5 截至 114 年 9 月底地方政府機關資安人員配置情形

單位：個、人

項目	合 計		B 級		C 級	
	機關數	人數	機關數	人數	機關數	人數
1. 應配置資安人員下限	608	719	111	222	497	497
2. 未配置足額資安人員	21	21	1	1	20	20
2.1 以機關員額不足為由未配置	15	15	1	1	14	14
2.2 資安人員離職尚未補足	6	6	—	—	6	6

資料來源：整理自各市（縣）政府查填調查表。

人，餘 1 個機關應配置 2 人，實際配置 1 人），惟經調查各該機關資安人員實際執掌業務，計有 548 個機關、共計 629 人（占各機關實際配置資安人數 698 人之 90.11%，下同），並非全職執行資安業務。另有 404 個機關未設資訊單位，其中 205 個機關以統計、綜合行政等非資訊處理職系人員擔任資安人員，共計 209 人（占 29.94%）；104 個機關以約聘僱、委外及約用人員擔任，共計 112 人（占 16.05%）；又各地方政府機關已配置資安人員 698 人，其中未依規定持有資安專業證照或職能訓練證書或兩者皆未持有者計 208 人（占 29.80%），存有資安專業能力不足之風險，經函請行政院督促研擬配套措施，俾補足公務機關資安專職人力需求並強化資安人員專業訓練及取得專業證照。據復：數位發展部資通安全署（下稱資安署）已推動公務人員高考三級增設資通安全類科、政府資安人力職能轉換訓練計畫等攬才精進措施，並透過公務機關績效評核等政策工具，鼓勵政府機關減少運用非正式人員擔任資安專職人員情形；持續協助各機關資安專職人員取得職能訓練證書，並定期審查資安專業證照清單，提供資安專職人員考取證照選擇。

3. 規範公務機關禁用危害國家資通安全產品，惟僅就個案審查結果進行情資分享，未就已審查發現之危害國家資通安全產品建立清單：依據 114 年 12 月 1 日修正施行之資安法第 11 條規定，公務機關不得下載安裝或使用危害國家資通安全產品；另依數位發展部訂定之危害國家資通安全產品審查辦法第 4 條第 1 項有關危害國家資通安全產品審查程序，第 1 款後段規定，同一資通系統、服務或產品業經主管機關審查，且無其他新事實或新證據者，得逕為結案；第 2 款規定，提報之資通系統、服務或產品為大陸廠牌者，主管機關得逕依規定進行情資分享；第 5 款規定，審查結果認定為危害國家資通安全產品者，主管機關應依規定進行情資分享。鑑於上述危害國家資通安全產品審查結果，係就個案進行情資分享，未將已審查發現之危害國家資通安全產品建立清單。為免各機關誤用相關資通系統、服務或產品，並肇生資安漏洞，或重複提報審查徒耗行政成本，經函請資安署研議將已審查發現之危害國家資通安全產品建立清單，並滾動檢討修訂，以利各機關參辦。據復：將研議透過其他適當管道提供已審認為危害國家資通安全之產品，請各機關確認相關產品使用情形，並作為機關未來採購之參考依據。

4. 部分地方政府未將資通系統防護需求等級及其防護基準納入資訊服務採購契約規範，或使用大陸品牌與已終止支援之資通訊產品，存有資料安全與業務運作風險：依行政院公共工程委員會（下稱工程會）發布之資訊服務採購作業指引第 3 點規定，機關應依資安責任等級分級辦法擇定資通系統防護需求，及涉及資安之履約項目，並應每年至少檢視 1 次資通系統分級及其防護基準之妥適性。本部抽查各地方政府辦理之 211 件系統建置、增設功能或維運採購案，計有 25 件未依規定每年重新評估資通系統分級之妥適性，並於契約納入資通系統防護需求等級及其防護基準，核與前開規定未合，且可能導致廠商未能依資通系統防護需求等級及其防護基準，合理估列資安相關成本費用，增加履約爭議或履約成果未符資通系統防護基準之風險。又行政院於 112 年 6 月 20 日及 114 年 3 月 31 日分別以院授數資安字第 1121000202 號及第

1141000253 號函，重申各公務機關之公務用資通訊產品（含軟體、硬體及服務）不得使用大陸廠牌，且不得安裝非公務用軟體，以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。本部抽查高雄市、苗栗縣、彰化縣等 3 個市縣資安責任等級 B 級及 C 級機關，於 114 年 10 月提交於資安署推動建置之資安弱點通報系統之資訊資產清冊，經分析其資產名稱、資產廠商欄位，分別計有 512 項、34 項及 528 項資訊資產為大陸廠牌；另分別有 24,311 項、10,855 項及 16,113 項資訊資產已終止支援，其中屬於資通系統伺服器之作業系統及資料庫分別有 16 項、27 項及 28 項。該等資訊資產及資訊系統因缺乏安全更新，恐無法應對新型態攻擊威脅，存有資料安全、系統穩定與業務運作風險，經函請資安署督促檢討改善。據復：業已協助工程會檢閱資訊服務採購契約範本並提供修正意見在案；資安署將於 115 年 5 月 1 日至 6 月 30 日辦理各機關危害國家資通安全產品盤點作業並向各中央及地方機關宣導，不得下載、安裝或使用危害國家資通安全產品；另將於辦理國家資通安全會報、資安長共識營或資訊（安）主管資安治理研習等活動，適時宣導已終止支援之資訊資產，應爭取經費優先汰換或採取適當風險緩解措施，以降低資安風險。

（十）數位發展部為降低企業發生資安危害風險，規劃透過臺灣電腦網路危機處理暨協調中心實現公私聯防，惟參與家數僅2千餘家，未達預計目標，又尚有7百餘家上市上櫃企業未加入資安情資聯防體系，允宜督促研謀改善。

依據金融監督管理委員會（下稱金管會）113 年 4 月 22 日修正發布之公開發行公司建立內部控制制度處理準則第 9-1 條第 1 項前段規定，公開發行公司應配置適當人力資源及設備，進行資訊安全制度之規劃、監控及執行資訊安全管理作業。復依金管會 113 年 9 月 10 日修正發布之上市上櫃公司資通安全管控指引第 35 條規定，加入資安情資分享組織，取得資安預警情資、資安威脅與弱點資訊，如：所屬產業資安資訊分享與分析中心（ISAC）、臺灣電腦網路危機處理暨協調中心（TWCERT/CC）。數位發展部為降低企業發生資安危害風險，於 114 年 5 月 27 日協同所屬資通安全署（下稱資安署）與國家資通安全研究院（下稱資安院）召開記者會，揭示臺灣在資安領域「公私聯防策略」，規劃透過資安院維運之 TWCERT/CC，強化企業資安情資共享、技術支援及人才培育。企業可免費加入 TWCERT/CC，接收資安電子報、暗網監控通報，掌握高風險或已被利用漏洞等情資，提前應變，並預計 114 年底平臺會員數將從 2 千家成長至 4 千家。截至 115 年 2 月底止，資安院雖已透過各類資安相關會議場合（如資安大會等活動）加強宣導 TWCERT/CC 聯盟相關資訊，惟 TWCERT/CC 會員數計 2,176 家，僅占全國中小企業家數 171 萬餘家之 0.13%，未達數位發展部所揭示 114 年底達 4 千家之目標；又國內上市上櫃公司總數計 1,957 家，經分析尚有 735 家未加入 TWCERT/CC 或所屬產業之 ISAC，未加入比率 37.56%，顯示企業參與資安情資分享意願仍顯不足，未能充分發揮平臺情資共享之優勢。鑑於近年國內陸續有多起上市上櫃公司發生資安事件，並遭相關主管機關裁罰，經函請行政院督導數位發展部協同相關主管機關優先鼓勵上市上櫃公司評估加入 TWCERT/CC 或所屬產業 ISAC 等情資共享平臺，以提

升國內企業資安韌性。據復：金管會持續推動上市上櫃公司加入 TWCERT/CC，截至 115 年 3 月底止，第 1 級及第 2 級上市上櫃公司加入 TWCERT/CC 已增加 24 家，後續將持續督導辦理，以完善上市上櫃公司資通安全強化措施；另為鼓勵企業踴躍加入，資安署於臺灣證券交易所「強化上市櫃公司資安措施任務小組」會議宣導上市上櫃公司加入會員。

(十一) 數位發展部為強化跨機關資料傳輸安全機制，持續輔導資安A級機關導入T-Road資料傳輸服務，惟部分新增資安A級機關、於MyData平臺提供個人資料服務及建置一站式系統介接機敏性資料之機關尚未導入T-Road傳輸，允宜研謀改善，以提升資料傳輸安全。

數位發展部為強化跨機關資料傳輸安全機制，辦理「政府骨幹網路服務計畫」，110 至 114 年度計畫經費共計 9 億 9,472 萬餘元，依「政府骨幹網路服務計畫」內容載述，數位發展部將優先輔導 111 年度所屬資通安全署（下稱資安署）核定之 47 個資通安全責任 A 級公務機關（下稱資安 A 級機關）導入 T-Road 及零信任架構。截至 114 年底止，除行政院、立法院及教育部國家教育研究院等 3 個資安 A 級機關因業務無跨機關資料傳輸需求而未導入 T-Road 外，其餘 44 個資安 A 級機關均已完成導入。惟據資安署提供資料，計畫執行期間（111 至 114 年度）部分機關資通安全責任等級已有調整，截至 114 年底止資安 A 級機關數量已增加至 50 個，尚待適時盤整各機關資安等級變更情形及資料傳輸需求，輔導導入 T-Road 傳輸；又國家發展委員會為讓民眾個人資料得以自主運用，建置個人化資料自主運用（MyData）平臺（下稱 MyData 平臺），據數位發展部提供資料，截至 114 年底止，已有 23 個機關於 MyData 平臺提供 143 項個人資料服務，供資料需求機關介接。經比對其中 14 個機關為「政府骨幹網路服務計畫」核定優先導入 T-Road 之資安 A 級機關，渠等於 MyData 平臺提供 76 項個人資料服務，其中交通部公路局等 10 個機關於該平臺提供之 55 項個人資料已導入 T-Road 傳輸，尚有內政部等 6 個機關之 21 項個人資料未導

表 6 截至 114 年底政府骨幹網路服務計畫核定之資安 A 級機關其 MyData 平臺個人資料導入 T-Road 情形

單位：項

項次	機關單位	MyData 平臺個人資料項數		
			已導入 T-Road 項數	未導入 T-Road 項數
合 計		76	55	21
1	內政部	12	7	5
2	內政部移民署	1	1	—
3	內政部警政署	2	2	—
4	財政部財政資訊中心	26	25	1
5	交通部公路局	3	3	—
6	勞動部勞工保險局	10	10	—
7	外交部領事事務局	1	1	—
8	教育部	2	—	2
9	行政院人事行政總處	1	—	1
10	行政院公共工程委員會	3	3	—
11	國家通訊傳播委員會	3	—	3
12	考試院	1	1	—
13	衛生福利部	9	—	9
14	衛生福利部中央健康保險署	2	2	—

資料來源：整理自數位發展部提供資料。

入 T-Road 傳輸（表 6）；另本部抽查內政部等 17 個機關辦理 20 個一站式整合為民服務系統執行情形，其中 13 個系統均有介接其他單位之公務或個人資料，惟除國營臺灣鐵路股份有限公司票務系統介接內政部戶役政資訊系統資料、財政部關務署關港貿單一窗口介接財政部財政資訊中

心資料係採用 T-Road 傳輸，其餘系統資料多數仍採用傳統網際網路之應用程式介面（Application Programming Interface, API）、安全檔案傳輸協定（SSH File Transfer Protocol, SFTP）等方式傳輸，安全性相對較低。經函請數位發展部適時盤整相關機關資料傳輸需求，輔導導入 T-Road 傳輸，以強化跨機關資料傳輸安全。據復：將滾動更新資安 A 級機關導入 T-Road 傳輸服務範圍，並持續輔導資安 A 級機關於 MyData 平臺及一站式整合為民服務系統將資料集改以 T-Road 方式傳輸，以提升跨機關資料傳輸安全。

（十二） 數產署承接維運企業得來速（Smepass）網站，未積極查證確認瀏覽人次之合理性，間有大量單一 IP 位址密集瀏覽及於凌晨瀏覽等異常情事；又未因應網站瀏覽人次陡降之經營困境，研採具體因應作為，即逕自終止網站服務，未能發揮網站建置效益，允宜研謀改善。

前經濟部中小企業處（112 年 9 月 26 日改制為中小及新創企業署，下稱中企署）為透過優化政府雲服務方式，加速中小微型企業數位轉型，辦理「以企業視角優化政府雲服務介面計畫」，110 至 113 年度計畫經費共計 2 億 3,341 萬元。嗣 111 年 8 月 27 日數位發展部數位產業署（下稱數產署）成立，承接計畫相關業務，並於 112 至 113 年度延續辦理，維運並推廣企業得來速（Smepass）網站，提供以中小微型企業視角，呈現個人化專屬服務之政府服務平臺，包含公司籌辦、創業、經營各階段之政府資訊與服務指引，2 年度決標金額分別為 5,300 萬元及 4,485 萬元。為達成企業得來速（Smepass）網站推廣及擴散目標，中企署及數產署於「以企業視角優化政府雲服務介面計畫」111 至 113 年度計畫書訂有網站瀏覽量之關鍵績效指標，其中 111 年度網頁瀏覽數應達 20 萬人次；112 及 113 年度網頁新增瀏覽數應達 10 萬人次及 24 萬人次等。據數產署提供資料，該網站 111 至 113 年度瀏覽人次分別為 24 萬餘人次、30 萬餘人次及 27 萬餘人次，已達計畫預期目標，惟查 114 年度截至 8 月底止網站瀏覽數僅剩 6 千餘人次，與前 3 年度瀏覽數差異甚鉅，經本部抽查該網站 113 年度瀏覽人次之日誌檔案（log 檔）發現，瀏覽次數前 20 名 IP 位址占總瀏覽次數之 55.74%，多數 IP 位址全年瀏覽量集中於連續短期 2 至 5 日間，日均瀏覽次數最高達 3 千餘次，且間有單一 IP 位址瀏覽間隔小於 1 秒情形達 5 千餘次，及凌晨 12 點至 6 點之間瀏覽次數達 4 千餘次等異常情事，顯示該等瀏覽量多數恐為機器人流量，相關關鍵績效指標統計結果無法反映實際服務使用成效；又數產署於該計畫執行將屆時，未積極研討企業得來速（Smepass）網站之永續經營方向，研採具體作為或相關配套措施，即逕以該年度已無經費支應維運、網站瀏覽人次低落，於 114 年 8 月 1 日起關閉網站服務，肇致 4 年計畫執行經費 2 億 3,341 萬元所建置之網站未能持續吸引使用客群，發揮預期效益。經函請數位發展部督促數產署研謀具體改善措施。據復：將妥適設定合適績效指標及積極查證推動成效，並滾動檢討指標之合理性，納入主動過濾異常 IP 與機器人流量之機制，另後續將配合國家科學及技術委員會建置跨部會之企業履歷資料庫系統，該系統可銜接、涵蓋及優化原企業得來速（Smepass）網站，預計於 115 年底前完成建置及上線。

四、113年度重要審核意見追蹤查核情形

本部於 113 年度審核報告內列普通公務相關重要審核意見 9 項，經賡續追蹤查核實際辦理結果，均已研謀改善或依改善措施持續辦理（表 7）。

表 7 113 年度審核報告所列數位發展部主管普通公務相關重要審核意見覆核辦理情形

重要審核意見標題	說明
已研謀改善或依改善措施持續辦理	
（一）推行網路廣告實名制與下架網路詐騙訊息等防詐措施，有助從源頭防範網路詐騙，惟網路防詐措施之深度及廣度仍須持續提升，相關業者之監督管理作業，尚待檢討加強。	
（二）規劃建置「網路詐騙通報查詢網」，有助提供民眾即時查詢與通報可疑網路詐騙廣告，惟部分功能與警政署「165 全民防騙網」相同或類似，且不具備報案功能；未明確訂定委託建置系統之功能需求，影響原定 113 年底上線期程；未規範通報涉詐案件機關處理時限且缺乏下架案件追蹤檢核機制；AI 自動掃描詐騙廣告範圍與內容不足，允宜研謀改善，以提升防制詐騙廣告政策成效。	
（三）推動智慧政府服務相關計畫已獲初步成果，惟我國公共服務數位化之國際評比排名持續下滑，政府單一入口服務網可提供線上申辦服務項目比率未及 5 成，又網站管理未盡周妥，致有重要服務漏未連結、錯誤或失效等情事；我的 E 政府及政府資料開放平臺網站資料搜尋功能友善程度不足或欠精準，影響民眾使用便利性，均待研謀改善，以提升政府數位服務效能。	
（四）政府為強化關鍵基礎設施資安防護能力，建立國家資安聯防運作機制，惟各領域之資通安全通報途徑不同，有待整合、部分 A 級關鍵基礎設施提供者工控領域資安治理成熟度未達目標、部分領域資安防護基準尚未訂定或其適用範圍未臻周延，允宜研謀改善。	
（五）政府為建構國家資通安全環境，推動各機關配置適足資通安全專職人力，惟部分機關未按資通系統維運現況，提交資安責任等級，影響資安人力配置之適切性；另資安職能訓練相關規範及執行作業未盡周妥，非資訊處理職系人員參加資安人力職能轉換訓練後，輔導轉任、留才等配套措施未盡完善，允宜研謀改善。	
（六）數位發展部推動設立國內 AI 評測中心並制定 AI 評測制度，有助降低 AI 產品與系統應用風險，允宜研議公部門導入 AI 產品與系統送測機制，以確保 AI 應用技術安全及可信賴；另數產署規劃建構 AI 應用技術與工具平臺，提供中小企業取用資源導入 AI 應用，惟計畫目標值訂定不具挑戰性，亦宜檢討改善。	
（七）數產署為解決中小微型企業數位人才缺口問題，辦理青年 T 大使計畫，惟計畫完訓青年就業率目標僅設定 2 成，遠低於勞動部職訓計畫訓後就業率目標為 7 成以上；另辦理 AI 相關人才培育計畫，培訓課程內容較少涵蓋資訊服務業關鍵人才所需演算法開發等技術能力，允宜研謀改善。	
（八）數位發展部補助地方政府辦理地政、財政及社福等業務免檢具申辦數位服務，提升服務品質，由於補助項目係由各地地方政府自提，致產生數位服務項目不一情事；依據產業創新條例規定補助之公司或企業，涉違反環境保護、勞工相關法律且情節重大，允宜研謀改善。	
（九）數位發展部推動戶政、醫療及勞保等 18 個民生關鍵系統雲端備份及回復機制，確保系統具備數位韌性，惟尚有部分民生關鍵系統未納入推動辦理，允宜檢討改善，以確保災害或緊急狀態發生期間維持政府與社會持續運作。	