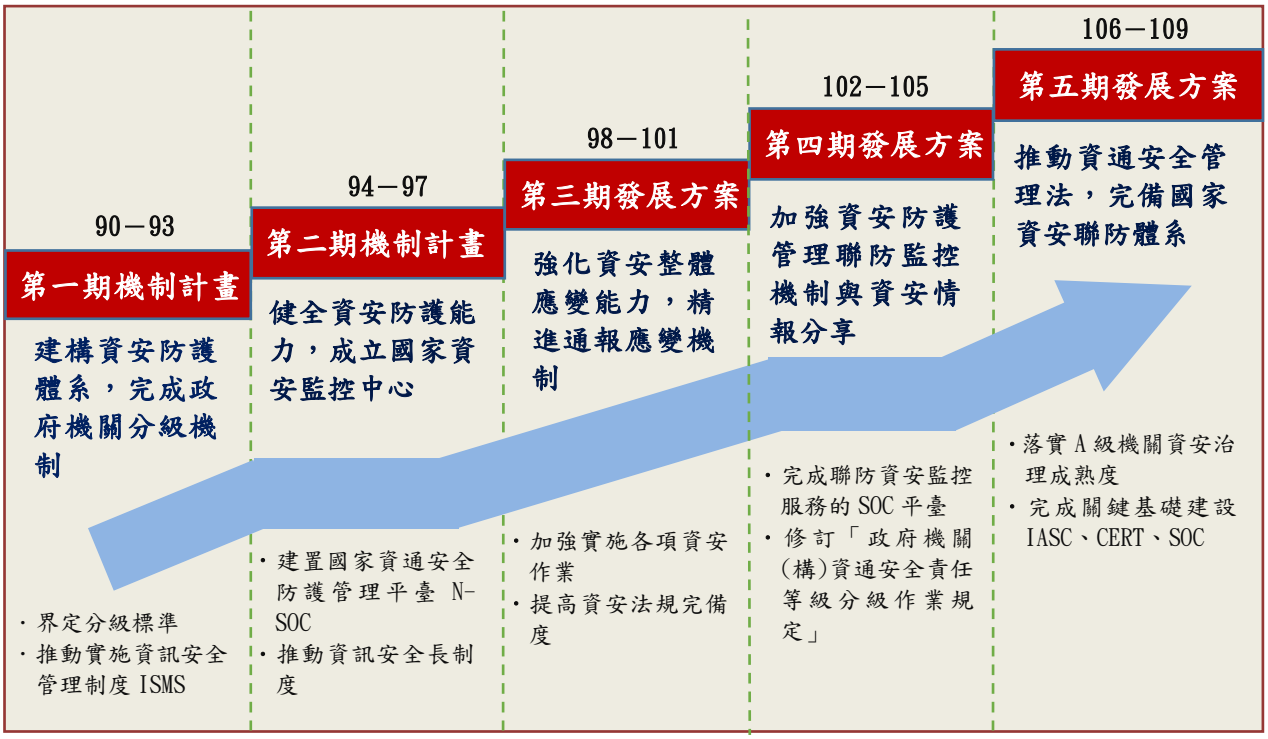
柒、政府推動國家資通安全政策執行情形

行政院為統籌並加速資通訊安全基礎建設，及強化資通訊安全能力，於 90 年 1 月成立國家資通安全會報（下稱資安會報），負責國家資通安全政策及跨部會資通安全事務之協調及督導等；另為研訂資安法規及標準規範，暨督導各機關及相關領域落實資通安全防護等作業，於 105 年 8 月設置資安專責單位－資通安全處（111 年 8 月組改為數位發展部資通安全署，下稱資安署），擔任資安幕僚工作。經查資安會報於 90 至 109 年間陸續推動「建立我國通訊基礎建設安全機制計畫」、「建立我國通資訊基礎設施安全機制計畫（94 年至 97 年）」等 5 項四年期國家資通安全計畫（各期計畫或方案重點如圖 1），在中央各部會、直轄市及縣市政府共同努力之下，已逐步達成「建立安全資安環境，完備資安防護管理，分享多元資安情報，擴大資安人才培育，加強國際資安交流」之階段性目標。鑑於資通訊服務應用廣泛，以及重大科技創新政策，對於國家安全，甚至社會經濟活動各應用層面，資通安全

圖 1　政府資安推動歷程



註：1. 第一、二期機制計畫分別代表「建立我國通訊基礎建設安全機制計畫」、「建立我國通資訊基礎設施安全機制計畫（94 年至 97 年）」；第三、四、五期發展方案分別代表「國家資通訊安全發展方案（98 年至 101 年）」、「國家資通訊安全發展方案（102 年至 105 年）」及「國家資通安全發展方案（106 年至 109 年）」。
2. 資料來源：整理自國家資通安全發展方案（110 年至 113 年）。

皆扮演關鍵角色，為能因應國際趨勢與新型態資安攻擊與威脅，在既有的防禦基礎及面向上延續資安防護能量與優勢，資安會報賡續於 110 年 2 月 23 日提出「國家資通安全發展方案（110 年至 113 年）」（下稱國家資通安全發展方案），作為政府現階段推動資安防護策略與計畫之指引。茲將國家資通安全發展方案推動情形暨審計機關重要審核意見，說明如次：

一、國家資通安全發展政策推動情形

（一） 目標與推動策略

110 至 113 年度推動之國家資通安全發展方案，以「成為亞太資安研訓樞紐」、「建構主動防禦基礎網路」及「公私協力共創網安環境」等 3 項為目標，訂定「吸納全球高階人才，培植自主創研能量」、「推動公私協同治理，提升關鍵設施韌性」、「善用智慧前瞻科技，主動抵禦潛在威脅」及「健全智慧國家資安，提升民間防護能量」等 4 項策略，期在穩健資通安全環境下，促進各項數位經濟脈動，以打造堅韌安全之智慧國家為願景，實現安心社會與智慧生活（圖 2）。

圖 2　110 至 113 年度國家資通安全發展方案架構

資料來源：擷取自數位發展部網站。

（二） 具體措施及執行機關

國家資通安全發展方案共訂定「擴增高教資安師資員額與教學資源」、「挹注資源投入高等資安科研」及「建立各領域公私協同治理運作機制」等 13 項措施（同圖 2），各項措施分別規劃相關細項工作，合計 31 項，由數位發展部（下稱數位部）等 11 個部會分工負責（表 1），主要措施如次：

表 1 國家資通安全發展方案分工情形

單位：項

部會別	主辦工作		
	參與策略	參與措施	負責細項工作
數位部	4	11	18
國家科學及技術委員會	2	5	9
經濟部	4	7	8
國家通訊傳播委員會	2	5	7
衛生福利部	1	3	4
交通部	1	3	4
金融監督管理委員會	1	3	4
教育部	1	2	3
內政部	1	1	3
法務部	1	1	3
國家發展委員會	1	2	2

註：1. 策略、措施與細項工作可由不同機關共同主辦。
2. 資料時點：截至 112 年 5 月底止。
3. 資料來源：整理自國家資通安全發展方案。

1. 規劃成立資安卓越中心，從技術面及人才面為未來資安需求札根，目標成為亞洲地區代表性高階人才及技術創新基地，工作項目包括「專案增加師資員額」、「發展國家依任務導向型及關鍵（核心）」及「跨國人才交流與研究合作」等 7 項。

2. 持續推動及落實各領域之資安防護基準，並輔以攻防演練及稽核檢視其執行成效，同時建構各該領域資安職能學習藍圖，以提升關鍵基礎設施一線人員之資安素質及關鍵基礎設施防護韌性，工作項目包括「賡續推動落實資通安全管理法，並適時檢討以因應國際資安防護趨勢」、「推動落實關鍵基礎設施資安防護基準」及「建構工控領域資安治理成熟度」等 9 項。

3. 以網路攻擊狙殺鏈提出偵查、武裝、遞送、攻擊、安裝、命令與控制、採取行動等 7 個階段，其防禦作為，舉如於偵查階段，透過事先建立資通系統弱點之主動發掘、通報及修補機制，並推動政府大內網及資安防護向上集中，以降低資安風險，工作項目包括「推動政府大內網及資安防護向上集中」、「建立資通系統弱點之主動發掘、通報及修補機制」及「發展主動式防禦前瞻研究及技術應用」等 9 項。

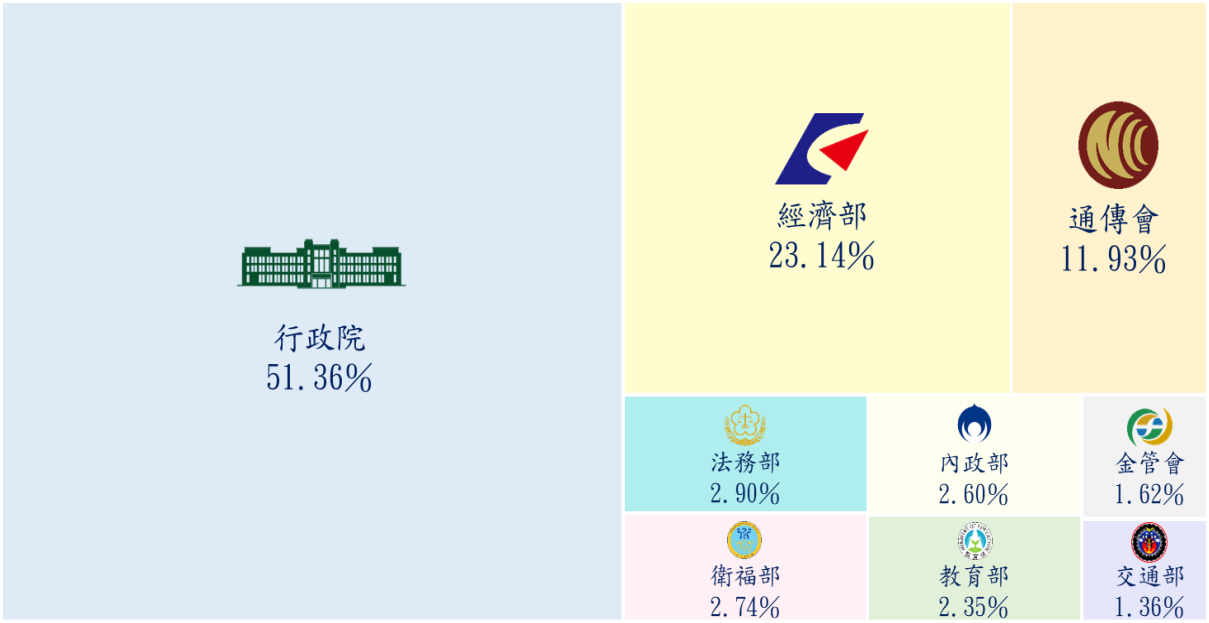
4. 持續強化政府機關資安防護能量及委外供應鏈風險管理、協助電信業者聚焦 5G 資安風險議題，提出對應解決方案，及關注隨著新世代網路發展之各

項物聯網設備及服務，制訂相關合規驗證及場域實證，加速物聯網資安解決方案落地與商用化，並參考國際標準，據以推動具備國際競爭力之資安解決方案，期以輸出國際市場，工作項目包括「結合民間資源，建立公私協同合作機制，協助企業提升資安防護能量」、「提升民眾意識」及「強化委外供應鏈風險管理」等 6 項。

（三） 執行成果

政府推動國家資通安全發展方案，截至 111 年底止，累計編列預算數 25 億 1,847 萬元，累計執行數 21 億 3,693 萬餘元，預算執行率 84.85%，按部會別區分，投入預算資源以行政院編列 12 億 9,351 萬餘元（占 51.36%）最多，經濟部編列 5 億 8,288 萬餘元（占 23.14%）次之，國家通訊傳播委員會編列 3 億 44 萬餘元（占 11.93%）第三（圖 3）。國家資通安全發展方案訂定 31 項工作項目，其中「開放學術區域網路中心、政府網路等場域供實習、實戰用」、「跨國人才交流與研究合作」、「建立資通系統弱點之主動發掘、通報及修補機制」等 3 項，因符合培訓條件人數未如預期、國際資安標準制定涉及多方利害關係人需較長之討論期程、部分機關未積極導入弱點通報機制等因素，執行結果未達預計目標，其餘工作項目均已達標，並獲致多項成果（表 2）。

圖 3　110 至 111 年度國家資通安全發展方案預算編列情形



註：1. 國家發展委員會、國家科學及技術委員會分辦之工作項目，相關預算由行政院統籌編列。
2. 本方案之部分工作項目於 111 年 8 月間移撥至資安署及數位發展部數位產業署執行，惟相關經費仍由行政院及經濟部之原編預算支應，統計圖係按預算編列之部會別繪製。
3. 資料來源：整理自資安署刊登於政府科技計畫資訊網之績效報告書。

表 2　111 年底國家資通安全發展方案 4 項策略執行成果

策　略　面　向	執　行　成　果
吸納全球高階人才，培訓自主創研能量	➢ 已核定 64 名資安師資。 ➢ 已招攬 55 名國內外研究人才建立研究團隊。 ➢ 已完成 13 項前瞻創新資安防護技術與機制設計，及 14 項資安軟體或安全晶片技術與機制研究。 ➢ 已完成 4 門跨域資安課程開發，養成資安實務人才 5,412 人。 ➢ 已培訓政府機關、製造業、資安產業等領域之資安人力 3,600 人。 ➢ 引進國外頂尖資安實戰課程，培訓國內實戰人力 218 人。
推動公私協同治理，提升關鍵設施韌性	➢ 已促成 303 個機關資訊向上集中。 ➢ 關鍵基礎設施之中央目的事業主管機關已完成 78 個關鍵基礎設施提供者之資安稽核作業。 ➢ 已訂定工控領域資安治理成熟度評估機制相關標準文件，並推動完成 12 個 A 級關鍵基礎設施提供者資安治理成熟度達 2 級以上。 ➢ 依國際最新情資交換格式，完成資安事件通報單交換格式。 ➢ 已分享情資達 191 萬餘件，辦理 16 場教育訓練，強化橫向交流。 ➢ 已完成 1 次跨國關鍵基礎設施攻防演練。
善用智慧前瞻科技，主動抵禦潛在威脅	➢ 已完成 16 個政府網際服務網路節點具備網路架構，及設置 87 個資料中心機關。 ➢ 已完成 366 個 A、B 級公務機關及關鍵基礎設施提供者導入資通安全弱點通報機制。 ➢ 已建置攻擊行為情資庫、智能威脅偵防平台、智慧資安威脅偵防服務平台等主動式防禦系統。 ➢ 已完成零信任網路身分鑑別、設備鑑別及信任推斷等 3 大機制之研究、整合協作與概念性驗證，並推動 2 個中央機關完成導入身分鑑別機制。 ➢ 已開辦科技偵查相關培訓課程，培訓 9,585 人。 ➢ 已建立與國外企業調閱相關犯罪資料窗口 13 件。
健全智慧國家資安，提升民間防護能量	➢ 已受理及審核國內企業產品資安漏洞通報 268 個。 ➢ 已完成 20 個機關實地輔導作業，落實委外作業資安管理。 ➢ 已滾動式檢討修訂 5G 資通安全維護計畫落實情形稽核計畫及標準作業程序文件，及已完成 2 件 5G 垂直場域實證。 ➢ 已完成門禁讀取器、智慧門鎖、門禁閘道控制器、門禁管理平台、人臉辨識裝置、智慧聯網地震儀、水位計等 7 項物聯網之資安標準與測試規範。 ➢ 支持國內法人及資通訊廠商參加與資安相關之國際標準制定，已提出 30 件技術貢獻，並納入國際標準。 ➢ 已發布 20 篇資安小知識專欄文章、8 則宣導影片及對民眾進行 28 則資安相關宣導。

資料來源：整理自資安署提供資料。

二、審計機關重要審核意見

茲將本部查核 111 年度國家資通安全發展政策執行情形所提重要審核意見，按政府規劃與機關組織人力、資訊服務類計畫、新興科技類及個人資料(下稱個資)保護等四大面向，歸納摘述如次：

（一） 政府規劃與機關組織人力

1. 政府為加速建構完善之國家資通安全環境,制定公布資通安全管理法並自 108 年 1 月 1 日施行,惟施行以來部分中央公務機關資安專職人力仍欠適足,資安督導業務亦未盡落實等情形,允宜督促相關機關研謀善策,以提升國家整體資安防護量能：政府為強化整體資安防護量能，於 111 年 8 月 27 日成立資安署，負責國家資通安全政策規劃、執行及督導。經查資安署於 112 年 4 月底仍無法提供截至 111 年底之資通安全管理法納管公務機關資安專職(責)人力配置及證照(書)取得情形之相關統計資料，據該署說明將併同 111 年度資通安全維護計畫實施情形調查作業，通函各機關於 112 年 5 月底完成填報，再由該署彙整分析，故僅提供 110 年底資料，不利適時督導各機關資安業務。另據資安署統計，截至 110 年底止，中央政府資通安全責任等級 A 至 C 級公務機關（含行政法人）共 532 個，按資安專職人數、資安專業證照數量及職能評量證書數量等 3 項法遵議題進行查核，未達法規低限者，分別為 124 個（23.31%）、197 個（37.03%）、221 個（41.54%）；人數總缺口及證照、證書總差額，分別為 141 人、225 張、266 張（表 3），與 109 年度相較，中央公務機關資安人力質量整備情形已有改善，惟其中 5 個 A 級、19 個 B 級及 100 個 C 級機關因資安專職人力尚欠適足，致連動影響證照（書）取得

表 3 110 年底中央政府資通安全責任等級 A 至 C 級公務機關（含行政法人）資通安全專職人力配置及證照（書）未達法規低限情形

單位：個、%、人、張

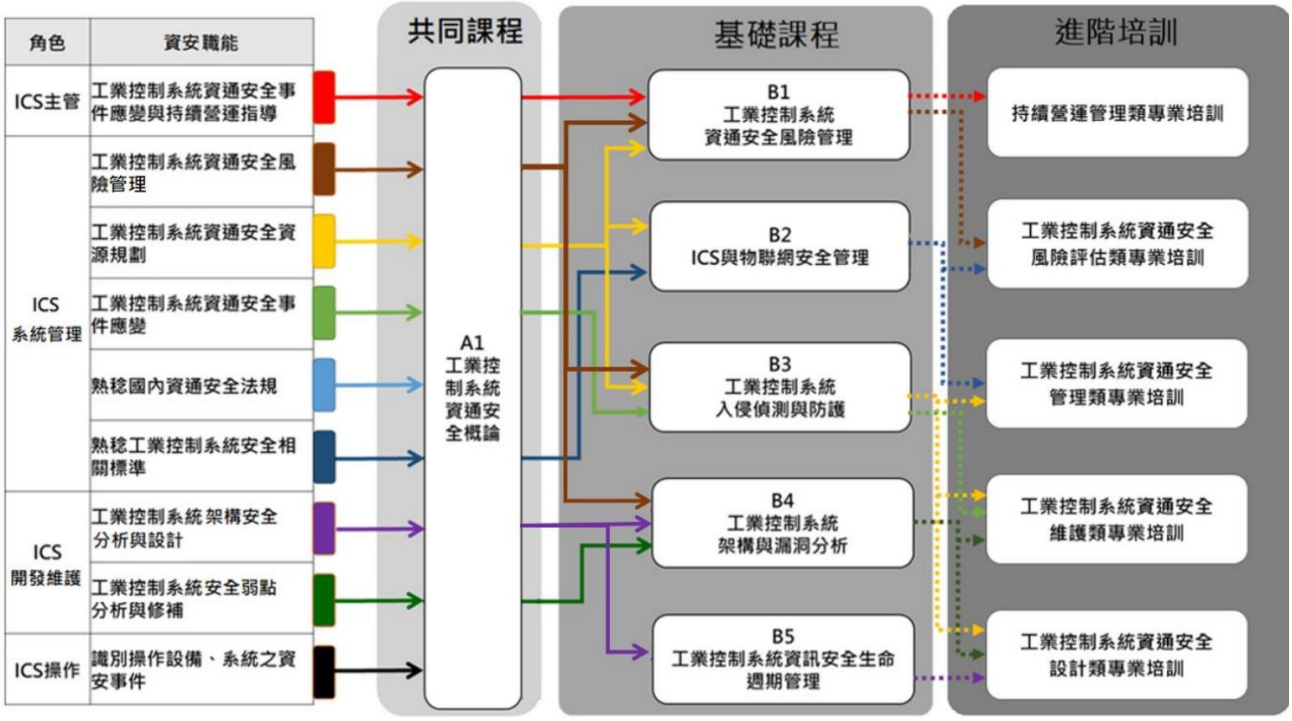
資通安全責任等級	機關（構）數	資安專職人員配置未達			資安人力專業證照數未達			資安人力職能評量證書數未達		
		法規低限	占比	人力缺口	法規低限	占比	證照數差額	法規低限	占比	證書數差額
合計	**532**	**124**	**23.31**	**141**	**197**	**37.03**	**225**	**221**	**41.54**	**266**
A 級	44	5	11.36	11	9	20.45	13	13	29.55	19
B 級	111	19	17.12	30	24	21.62	48	39	35.14	78
C 級	377	100	26.53	100	164	43.50	164	169	44.83	169

資料來源：整理自資安署提供資料。

張數未達法定要求，經函請行政院督促研謀因應改善。【詳總決算審核報告第 2 冊丙、貳、行政院主管項下重要審核意見（十）】

2. 交通部為提升交通領域 CI 核心系統之防護韌性，推動資安整備計畫，已完成交通領域 ICS 資安職能地圖及 CIP 攻防演練，惟相關從業人員未取得適切之資安職能證書，復未將 ICS 資安職能訓練規定納入資通安全維護計畫，亦未持續追蹤資安攻防演練弱點之改善情形，允宜研謀改善，俾利 ICS 從業人員具備適足之資安防護專業能力，降低資安威脅之衝擊：交通部鑑於關鍵基礎設施（Critical Infrastructure, CI）資安風險倍增，為避免交通領域關鍵基礎設施之核心資通系統異常，影響經濟與民心士氣，配合行政院國家資通安全會報於 110 年 2 月提出國家資通安全發展方案，推動資安跨域整合聯防計畫－交通領域關鍵基礎設施資安整備計畫，以提升關鍵基礎設施提供者（Critical Infrastructure Provider, CIP）防護韌性，期程為 110 至 113 年度，總經費 8,241 萬餘元。該部業依據資通安全責任等級分級辦法訂定交通領域資安防護基準，並依據前揭資安防護基準及國家資通安全發展方案所定推動策略，完成交通領域工業控制系統（Industrial Control System, ICS）資安職能地圖（圖 4），對相關人員實施訓

圖 4 交通領域工業控制系統（ICS）資安職能地圖



資料來源：整理自交通部提供資料。

練。經查交通領域關鍵基礎設施資安整備情形，核有：(1)部分交通領域特定非公務機關 ICS 從業人員，未依規定取得交通領域 ICS 資安職能課程證書；(2)110 年度攻防演練對象未將交通領域 ICS 從業人員應取得交通領域 ICS 資安職能課程證書之規定，納入資通安全維護計畫，不利資安防護控制措施之施行；(3)110 至 111 年度已辦理 2 個 CIP 之資安攻防演練，惟未評估低風險等級弱點對系統安全之實質影響，督促攻防演練對象完成資安弱點修補作業；(4)辦理資安攻防演練成果分享會，惟參與者多屬資訊科技人員，不利擴散演練效益等情事，經函請交通部研謀妥處。【詳總決算審核報告第 2 冊丙、拾肆、交通部主管項下重要審核意見（十五）】

3. 金管會已持續增修訂資安規範並導入國際資安管理及驗證標準，惟各業別金融資安缺失仍多，又部分金融機構資安長異動頻繁，允宜督促研謀改善，以強化金融資安韌性並深化資安治理綜效：金融監督管理委員會（下稱金管會）為強化金融業資安防護能力，於 109 年 8 月發布金融資安行動方案，嗣於 111 年 12 月為因應金融科技發展趨勢，滾動檢討研訂金融資安行動方案 2.0 版，訂有 40 項措施（含新增 12 項、擴大 5 項及持續辦理 23 項）引導金融資安持續精進。經查執行情形，核有：(1)金管會已督導金融相關公會持續增修資安規範，並導入國際資安管理標準，惟所屬檢查局擇選南山人壽保險公司等 38 家金融機構辦理資安檢查結果，銀行、保險、電子支付等金融機構存有未落實辦理各主機系統及物聯網設備之弱點掃描作業等 12 項共同性缺失（表 4）；(2)金管會已強制銀行及一定規模之保險、證券業設置資安長，惟華南商業銀行公司等 4 家金融機構資安長異動

表 4　111 年度金融機構共同性資安缺失項目

項次	缺失項目	銀行業	保險業	信用合作社	電子支付機構
1	電子銀行業務安全控管作業有欠妥適	✓	✓(註1)	✓	✓(註1)
2	未落實主機系統弱點掃描作業	✓	✓	✓	✓
3	具客戶個資之電子郵件控管機制有欠妥適	✓	✓	✓	✓
4	個資盤點範圍有欠周延	✓	✓	✓	✓
5	主機帳號授權有欠妥適	✓	✓	✓	✓
6	ATM 及 APP 資安防護作業有欠妥適	✓	✓	✓	✓
7	對外服務網站安全防護作業有欠妥適	✓	✓	✓	✓
8	連線正式營運環境之管控措施有欠妥適	✓	✓	✓	✓
9	系統委外開發管理有欠妥適	✓	✓	✓	
10	新系統或新功能上線前檢測作業有欠妥適	✓	✓	✓	✓
11	辦理弱點掃描或滲透測試作業有欠完善	✓	✓	✓	✓
12	辦理防火牆規則檢視作業有欠確實	✓	✓	✓	✓

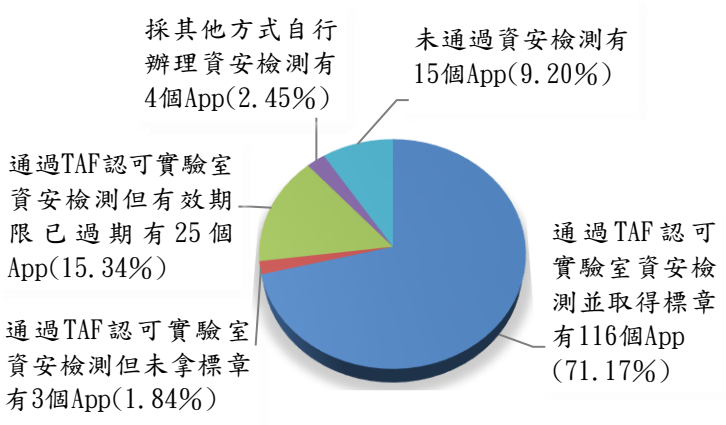
註：1.係指保險業辦理電子商務業務安全控管作業，及電子支付公司辦理電子支付平臺安全控管作業。
2.資料來源：整理自金管會檢查局提供資料。

頻繁，恐不利綜理資訊安全政策之推動及協助董事會對資安情勢之掌握等情事，經函請金管會督促檢討妥處。【詳總決算審核報告第 2 冊丙、貳拾參、金融監督管理委員會主管項下重要審核意見（一）】

（二） 資訊服務類計畫

1. 行政院為建立國人對政府行動化應用軟體使用安全之信賴感，已修正行動化服務作業原則，明定機關開發之 App 應通過資安檢測，始得提供民眾下載使用，惟未明確規範檢測作業方式及頻率、未將機關內部使用之 App 納入作業原則適用對象，及未落實相關管考機制等，易衍生個資外洩及資安風險，相關權責機關允宜研謀妥處，以確保民眾及機關內部使用 App 之安全：行政院為確保各機關行動化服務符合資通安全規範、避免使用者資料外洩或財物損失等風險，建立國人對政府行動化應用軟體（下稱 App）使用之安全信賴感，於 106 年 7 月 28 日修正「行政院及所屬各機關行動化服務發展作業原則」（下稱行動化服務作業原則），明定中央政府各機關開發之行動化服務應通過經濟部工業局訂定行動化應用軟體之檢測項目，始得提供民眾下載使用，以及行政院所屬二級機關應每年彙整其所屬機關（構）之績效及資通安全檢測報告，送國家發展委員會（下稱國發會）進行管考。嗣 111 年 8 月 27 日數位部成立，承接 App 相關規範訂定、管考及資安檢測等相關業務。經查中央政府各機關開發及維護之 App 資訊安全及維護管理情形，核有：（1）行政院修正之行動化服務作業原則，未明確規範 App 檢測作業方式及頻率，致各機關辦理檢測作業方式不一（圖 5），易衍生資安風險；（2）行動化服務作業原則未將機關內部使用之 App 納入適用對象，經參考行動應用資安聯盟資安認證制度認可實驗室安華聯網科技股份有限公司於 110 年揭露臺灣 App 常見之三大風險，包含不安全的資料儲存、不安全的資料傳輸及資料輸入內容未經完整驗證，未因使用對象不同而降

圖 5 中央政府各機關辦理 App 資安檢測作業方式



註：1.資料時點：截至 111 年 7 月 31 日。
2.資料來源：整理自中央政府各機關提供資料。

低資安風險等級，且駭客攻擊層出不窮，公務機關仍有發生民眾個資或機敏資料外洩疑慮；（3）行政院未落實 App 相關管考機制，截至 111 年 7 月底止，中央政府各機關開發提供民眾下載使用之 App 共計 163 個，開發建置成本約 4 億 938 萬餘元，其中 31 個 App 漏未於「我的 E 政府」管理平臺填報、15 個 App 未辦理資安檢測、11 個 App 未依改善期限完成資安檢測等，影響民眾使用 App 之安全等情事，經函請行政院及數位部研謀妥處。【詳總決算審核報告第 2 冊丙、貳、行政院主管項下重要審核意見（十一）】

2. 教育部補助各市縣政府建構綠能雲端資料中心，並推動高中以下學校校務行政系統等資訊資源向上集中，惟部分市縣政府未將存有個資之校務行政系統認定納列為核心資通系統，或未落實校務行政系統資安相關防護，存有學生個資外洩等資安風險，允宜研議因應對策，供市縣政府遵循，以確保學生個資安全：

教育部鑑於多數國中小學校缺乏資安人力及資訊資源，不利資安管理，配合國發會「建構公教體系綠能雲端資料中心計畫」，補助 22 市縣政府推動教育網路中心（下稱教網中心）轉型為綠能雲端資料中心，及轄管縣立高中職、國民中小學資訊資源向上集中至符合資通安全責任等級 B 級之教網中心等重點工作，截至 111 年底止，累計整併逾 3,000 所學校機房，提升服務品質及整體資安，並減低校園機房系統建置及維護費用等，且該部為因應資通安全管理法施行及保護學校教職員生權益，規範中央及地方政府所屬公立高中以下學校存有教職員生個資之校務行政系統等應列入核心資通系統。經抽查新北市等 9 市縣教網中心資安管理機制及高中以下學校校務行政系統資安防護情形，核有：（1）苗栗縣、彰化縣（教網中心）等 2 縣政府認定校務行政系統非屬核心資通系統；（2）嘉義市、苗栗縣等 6 市縣政府提供廠商介接所管學校校務行政系統之 App 未通過資安檢測，或未明確界定行動應用 App 介接資料範圍、欄位格式及資料存取權限（表 5）；（3）未將校務行政系統或學習歷程檔案系統盤點納入

表 5　111 年底市縣政府未落實校務行政系統資安防護情形

市縣政府	未界定使用資料範圍及存取權限之校務行政系統名稱	未通過資安檢測之 App 名稱
高雄市	國中校務行政電腦化系統	高雄高中職點名家長即時通
基隆市	國民中小學校務行政系統	School+家長
新竹縣	國中小校務行政系統	School+家長
苗栗縣	國中小電子化校園校務系統	
嘉義市	國中小校務行政系統	School+家長
宜蘭縣	國民中小學校務行政系統	School+家長

資料來源：整理自高雄市等 6 市縣政府提供資料。

資通安全維護計畫辦理相關資安應辦事項，暨未妥適執行核心資通系統弱點掃描、滲透測試等多項通案性缺失等情事，經函請教育部研謀妥處。【詳總決算審核報告第2冊丙、拾壹、教育部主管項下重要審核意見（十一）】

3. 僑務委員會推動智能僑務服務發行i僑卡，建置與整合多元系統，惟系統存管跨國海外臺灣僑胞個資，允宜審慎評估機關資通安全責任等級及核心資通系統，研謀強化資安防護及管控措施，以確保資通安全：僑務委員會為發展智能僑務服務，推動僑務資料智能分析及運用規劃計畫，以提供更精準化之全球僑胞服務，計畫期程為111至114年度，總經費2,535萬元，111年度編列預算435萬元。經查執行情形，已建置i僑卡管理系統，並於111年9月正式發行i僑卡，後續並將整合相關僑務服務系統，該等系統包含跨國之海外臺灣僑胞等個資，且整合系統為跨僑務委員會及外交部駐外館處共用性資通系統，其資安防護及管控措施更顯重要，惟現行僑務委員會仍列為資通安全責任等級B級機關，又i僑卡管理系統係推動智能僑務服務後續發展之基石，卻未列入資通安全維護計畫之核心資通系統，經函請僑務委員會研謀強化資安防護及管控措施。【詳總決算審核報告第2冊丙、拾陸、僑務委員會主管項下重要審核意見（一）1.】

4. 臺鐵局為確保新MMIS運作環境安全，已將系統列為核心資通系統，惟未依規定檢討納入年度資通安全維護計畫據以辦理相關資安防護措施，如發生資安事件，恐影響車輛維修工作，衍生營運風險，允宜妥為研謀因應，以確保系統應用上線運作期間保持可控之安全狀態：交通部臺灣鐵路管理局（下稱臺鐵局）於108年6月19日資通安全責任等級初次受核定為A級，依資通安全責任等級分級辦法附表二規定須於 3 年內完成公正第三方資訊安全管理制度（Information Security Management System, ISMS）驗證，並持續維護其驗證有效性（表6）。經查該局為掌握車輛維修成本，提高維修保養品質，於109年12月規劃建置全新「車輛維修管理資訊系統」（下稱新MMIS），110年2月決標，決標金額3億2,392萬餘元，期以完備車輛檢修計畫管理為目標。按上開採購案已於契約明定新MMIS為核心資通系統，並於111年2月正式上線，截至111年9月底止，已提供12款車型上線服務，惟該局未按資通安全管理法第10條規定，妥適檢討將該系統納入111年度資通安全維護計畫之核心資通系統，據以辦理相關資安防護措施，且於111

年 3 月 14 日資訊安全管理審查會議，決議俟系統完成建置且全面上線後 2 年內(118 年 2 月)再完成導入 ISMS，期間該系統倘若發生資安事件，恐影響已上線車輛維修工作，衍生營運風險，為確保系統應用上線運作期間維持安全狀態，經函請臺鐵局研謀改善。【詳審核報告營業部分乙、肆、二、交通部主管臺灣鐵路管理局項下重要審核意見 5.（2）】

表 6　資通安全責任等級 A 級之特定非公務機關管理面應辦事項

辦　理　項　目	內　　容
資通系統分級及防護基準	初次受核定或等級變更後之 1 年內，針對自行或委外開發之資通系統，依資通系統防護需求分級原則完成資通系統分級，並完成資通系統防護基準之控制措施；其後應每年至少檢視 1 次資通系統分級妥適性。
ISMS 之導入及通過公正第三方之驗證	初次受核定或等級變更後之 2 年內，全部核心資通系統導入 CNS 27001 或 ISO 27001 等 ISMS 標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於 3 年內完成公正第三方驗證，並持續維持其驗證有效性。
資通安全專責人員	初次受核定或等級變更後之 1 年內，配置 4 人。
內部資通安全稽核	每年辦理 2 次。
業務持續運作演練	全部核心資通系統每年辦理 1 次。

資料來源：整理自 110 年 8 月 23 日資通安全責任等級分級辦法附件二。

5.　國教署因應資通安全管理法之施行，訂定公立高級中等以下學校資通安全防護計畫，推動學校核心資通系統向上集中，惟國立高級中等學校逾 9 成校務行政系統及逾 6 成學習歷程檔案系統未能向上集中，學校資安稽核並存有多項缺失，允宜研謀改善，建構校園資通安全環境：資通安全管理法（下稱資安法）於 108 年 1 月 1 日施行，教育部國民及學前教育署（下稱國教署）鑑於各國立高級中等學校資安防護水準不一，主機及資料庫存有資安風險，經依據教育部資訊資源向上集中，全部核心資通系統由上級或監督機關維運之原則，訂定「公立高級中等以下學校資通安全防護計畫」（下稱資安防護計畫），推動學校核心資通系統向上集中，並建置專業資訊機房，提供委外建置與所屬學校資通系統向上集中之用，以符合資通安全責任等級分級辦法之規定。經查執行情形，核有：（1）國教署所轄 131 所國立高級中等學校（不含 14 所特殊教育學校，下同），計有 122 校（占 93.13%）之校務行政系統及 79 校（占 60.31%）之學習歷程檔案系統，因選用系統版本之架構非屬雲端版系統，未能依資安防護計畫規定完成向上集中；（2）131 所國立高級中等學校，計有 81 校經核定資通安全責任等級為 C

級，惟多數學校（70 校）囿於人力及物力，未能配置資通安全專責人員，不利落實資安應辦事項；(3)國教署為落實資安法之規定，分年就所轄學校辦理資安稽核，部分學校稽核不符項數比率逾 3 成（表 7）或資安事件頻傳等情事，經函請國教署研謀改善。【詳審核報告非營業部分乙、壹、四、（六）國立高級中等學校校務基金項下重要審核意見（1）】

表 7　資安實地稽核不符項數比率逾 3 成之學校

單位：項、%

年度	學校名稱	不符合項數	不符合比率
109	國立蘇澳海事高級水產職業學校	24	33.3
110	國立新竹高級工業職業學校	33	45.8
	國立嘉義女子高級中學	28	38.9
	國立彰化高級商業職業學校	23	31.9
	國立彰化師範大學附屬高級工業職業學校	23	31.9
111	國立花蓮女子高級中學	28	38.9
	國立花蓮高級工業職業學校	24	33.3

資料來源：整理自國教署提供資料。

（三）　新興科技類

1.　政府原定 111 年底開放 5G 專頻專網執照申請，惟截至 112 年 4 月底止，仍未完成 5G 專頻專網相關法規之訂定，延宕發展期程，允宜研謀改善，以健全 5G 專頻專網管理制度及創新應用服務發展與安全：行政院為推動 5G 專網發展，於 108 年 12 月 5 日院會決議指配 4.8-4.9GHz 頻段以「專網專頻」方式獨立運作，並定於 111 年底前開放 5G 專頻專網執照申請。業者可申請在特定場域範圍，設置供本身業務使用之專屬網路，無須擔心頻率干擾衍生影響設備或更換機器等問題，確保聯網之通訊品質與資訊安全。經查國家通訊傳播委員會（下稱通傳會）於 110 年間完成「行動寬頻專用電信網路設置使用管理辦法」草案，並於 111 年 7 月預告該草案內容，嗣因應數位部 111 年 8 月成立，數位部另擬具該部版之「行動寬頻專用電信網路設置使用管理辦法」草案，並於通傳會 111 年 11 月 15 日召開之「5G 專頻專網管理業務討論會議」提出 5G 專頻專網之法規制（訂）定、修正及網路管理，宜由數位部主政之建議。因數位部及通傳會對於 5G 專頻專網之法規制（訂）定、修正及網路管理之主政機關未達成共識，經通傳會於 111 年 11 月 24 日函請行政院秘書長協調，行政院於 112 年 3 月 6 日召開會議決議由數位部主政，惟已逾原定 111 年底開放 5G 專頻專網執照申請政策目標，經函請數位部研謀改善。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建

設項下重要審核意見（五）1.】。

2. 5G 自主垂直應用專網系統未辦理資安驗測，且部分計畫應用示範場域使用之 5G 設備亦未辦理資安驗測，影響資安防護完整性，允宜研謀改善，以確保 5G 專網系統及設備資安與防護能力：經濟部為協助產業掌握 5G 網路通訊發展契機，打造跨部會、跨產業領域 5G 創新應用發展環境，辦理「5G+系統暨應用淬鍊計畫」（下稱 5G+淬鍊計畫），嗣於 110 年度經濟部將該計畫有關打造全方位資安防護系統項目，另案移至前瞻計畫數位建設項下「5G 資安防護系統開發計畫」辦理。數位部所屬數位產業署（下稱產業署）於 111 年 8 月 27 日成立，承接 5G+淬鍊計畫及 5G 資安防護系統開發計畫。經查執行情形，核有：（1）5G 資安防護系統開發計畫已對 5G 核心網路元件之存取與移動管理功能、連結管理功能、用戶平面功能制訂完整測試項目，並於 110 年完成開發存取與移動管理功能及用戶平面功能自動化檢測工具，惟 5G+淬鍊計畫內之 5G 自主垂直應用專網系統，僅將存取與移動管理功能 1 項提交 5G 資安防護系統開發計畫團隊進行資安驗證與測試（下稱驗測），其餘 5G 核心網路元件並未進行資安驗測；（2）5G+淬鍊計畫於 109 至 111 年間，辦理 5G 物聯網無人機應用等應用示範，所使用之基地台與終端等設備未辦理資安驗測等情事，經函請數位部督促研謀改善。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建設項下重要審核意見（五）2.】

3. 5G 資安防護系統開發計畫執行成果，已完成多項 5G 合規檢測技術及自動化檢測工具，惟尚未就新興之開放式無線接取網路（O-RAN）完成資安相關規範與檢測工具，允宜研謀改善，以利帶動國內相關產業發展，提升產業競爭力：經濟部為確保業者設置 5G 系統安全、可靠及可信賴，並與國內 5G 專網業主合作進行服務驗證，建立在地 5G 專網資安解決方案實際案例，協助開拓國際市場，辦理「5G 資安防護系統開發計畫」，又數位部所屬產業署於 111 年 8 月 27 日成立，承接執行 5G 資安防護系統開發計畫，截至 111 年底止，已研發多項 5G 合規檢測技術與自動化檢測工具，及發布「5G 基地臺資安測試規範」。經查全球網路虛擬化技術日漸成熟，具有開放式無線接取網路（Open Radio Access Network, O-RAN）的新架構，除能提升成本效益，更將加速 5G 網路佈建，惟「5G 資安防護系

統開發計畫」未將 5G O-RAN 基站資安測試規範訂定與檢測工具開發等列入計畫預期關鍵成果；另該計畫雖將邊際運算資安防護納入研發範圍，惟尚無開發邊際運算資安檢測工具與規範，經函請數位部督促研謀改善。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建設項下重要審核意見（五）3.】

4. 數位部為確保 5G 網路安全及協助第三方創新服務提供者增強其資安能量與能力，成立國家通訊軟體領域安全與 5G 網路資安實驗室，惟相關計畫將於 112 年底結束，允宜預為檢討後續營運規劃策略，以提升 5G 資安產業防護能量：通傳會為協助 5G 業者及第三方創新服務提供者增強其資安能量與能力，於健全電信資安防護設備建置計畫內，規劃建置「國家通訊軟體領域安全實驗室」，建置經費 6,888 萬餘元；另為加速 5G 網路建設，確保 5G 網路安全可信賴，於推動 5G 垂直應用場域實證、法規調適與網路資安之防護研析計畫內，規劃建置「5G 網路資安實驗室」，建置經費 8,164 萬餘元。嗣數位部於 111 年 8 月 27 日成立，承接上開 2 實驗室相關業務。該部考量 5G 法規逐漸成熟，且 5G 網路資安實驗室之原計畫相關經費縮減，於 112 年度將該實驗室併入健全電信資安防護設備建置計畫內執行，惟該計畫亦將於 112 年度結束，為有效利用實驗室相關軟硬體實驗設備，經函請數位部預為檢討妥處。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建設項下重要審核意見（五）4.】

5. 數位部為確保 5G 網路安全，已研訂 5G 資通安全技術稽核項目，惟辦理通訊傳播業者資通安全維護計畫稽核作業時，尚未將技術稽核納入，允宜研謀改善，以掌握 5G 業者資安防護情形，確保國家關鍵基礎設施安全：通傳會為確保 5G 網路安全，配合電信管理法及資通安全管理法要求，研訂 5G 資通安全維護計畫之稽核項目及稽核計畫。嗣數位部於 111 年 8 月 27 日成立，相關業務移由數位部辦理。上開 5G 資通安全維護計畫之稽核項目涵括 16 項技術稽核項目，規劃以測試場域執行檢測或由業者提出實際操作畫面佐證資料等方式進行稽核，檢視業者資安防護機制之完整性及有效性。惟該部於 111 年 9 至 12 月辦理通訊傳播業者資通安全維護計畫實施情形之稽核作業時，仍採現場實地查閱作業紀錄及管理文件為主，尚未包括技術稽核，致未能確認業者資通安全維護措施之落實程度，經函請

數位部研謀改善。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建設項下重要審核意見（五）5.】

6. 政府為強化物聯網設備資安防護機制，訂有 16 項物聯網設備資安標準與測試規範，惟僅 4 項發布成為國家標準，且尚未就智慧醫療物聯網設備訂定相關資安標準，允宜研謀妥處，以建立可信賴之物聯網應用環境：行政院為因應科技技術與未來產業發展需求，陸續核定「建構民生公共物聯網計畫（106 至 109 年）」與「民生公共物聯網數據應用及產業開展計畫（110 至 114 年）」，並由科技部（於 111 年 7 月 27 日改制為國家科學及技術委員會）等中央部會主責辦理，截至 111 年底止，累計編列預算數 69 億 629 萬餘元，執行數 68 億 9,316 萬餘元，執行率 99.81%。經查物聯網設備資安防護機制，核有：經濟部工業局為提供業者產品設計導入資安規格時有所依循，協同產業界共同發布 16 項「物聯網資安產業標準與測試規範」，惟尚有 12 項未發布為國家標準；又按資料竊取資源中心（Identity Theft Resource Center, ITRC）統計，2022 年上半年醫療服務業為資料洩漏次數最高產業，惟該局尚未訂定智慧醫療物聯網資安產業標準等情事，經函請行政院督促檢討妥處。【詳中央政府前瞻基礎建設計畫第 3 期特別決算審核報告甲、參、五、數位建設項下重要審核意見（七）1.】

（四） 個資保護

1. 經濟部所訂個資安維辦法，其適用範圍僅包含資本額 1 千萬元以上之網際網路零售業及網際網路服務平台業者，且部分案件未及時函請業者改善個資安維作業缺失，允宜研謀改善，以確保國人個資安全：經濟部為監管數位經濟相關產業類非公務機關個資檔案安全維護管理情形，於 104 年 9 月訂定網際網路零售業及網際網路零售服務平台業個人資料檔案安全維護計畫及業務終止後個人資料處理作業辦法（下稱個資安維辦法），以強化業者個資保護措施，上開監管業務已於 111 年 8 月 27 日移由數位部所屬產業署辦理。經查執行情形，核有：（1）產業署轄管個資安維辦法未納管登記資本額未達 1 千萬元，或非股份有限公司者，恐不利有效監管高風險業者；（2）產業署辦理網際網路零售業及平台業個資安全維護業務，僅就警政署通報案件啟動行政調查程序，尚乏主動檢查或實地查核機

制；（3）產業署處理疑似個資外洩通報案件，平均需 13 天始函請業者說明改善情形，又行政檢查會議決議後經 22 至 36 天始函請業者改正等情事，經函請數位部督促研謀妥處。【詳總決算審核報告第 2 冊丙、貳、行政院主管項下重要審核意見（九）3.】

2. 經濟部委外建置及維護之法人科專系統遭駭客攻擊，致資料庫部分資料遭刪除，嚴重影響系統運作，允宜督促研謀改善，以保障國家安全：按經濟部為推動ｅ化管理，自 97 年度起建置整合性ｅ化社群平臺之「法人科專計畫管理系統」（下稱法人科專系統），該部及各計畫執行之相關法人單位，可透過該系統帳號及權限之管制，運用系統提供即時性資料查詢及彙整性統計報表，管控科專計畫整體執行情形。經查法人科專系統之「法人科技專案管考暨成果計畫」功能項目管理維護事宜，係每年委託財團法人中衛發展中心辦理，其中資通安全為主要工作項目之一，惟該系統於 111 年 3 月 22 日遭駭客攻擊，致資料庫 477 筆委員個資紀錄被刪除。且該部後續委請第三方單位歷時 5 個月餘完成資安檢測，111 年 9 月 2 日始重新啟用，並於同年月 7 日通報各法人單位於該系統補登錄 111 年 3 月至 9 月間資料，致近半年期間採紙本化方式辦理計畫管考作業，未能發揮系統提供彙整性統計報表、即時性資料查詢，及整體管控法人科專計畫等建置效能，經函請經濟部研謀改善。【詳總決算審核報告第 2 冊丙、拾參、經濟部主管項下重要審核意見（九）2.】

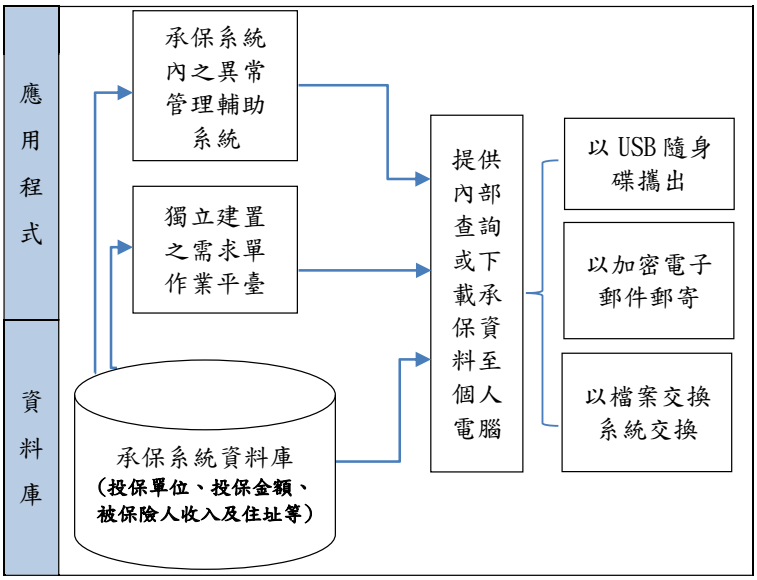
3. 行政院已規範中央目的事業主管機關對非公務機關個資保護加以監管，惟交通部及所屬公路總局與民用航空局辦理行政檢查作業，存有未於規定期限內辦理或後續行政措施及處理時間過長等情事，允宜研謀改善，以落實非公務機關個資檔案之安全維護：依據行政院及所屬各機關落實個人資料保護聯繫作業要點（110 年 8 月 11 日訂定，下稱聯繫要點）第 2 點第 2 項第 2 款規定，重大矚目之個資外洩案件範圍，包括經平面媒體全國性版面報導、電子媒體專題討論。又聯繫要點第 8 點規定，對個資外洩案件之行政檢查流程，除重大矚目之個資外洩案件外，其餘行政檢查程序，依收受通知（報）機關認有管轄疑義者，應於 10 日內

確認權責範圍；對於重大社會矚目案件，應於 30 日內辦理行政檢查。另依聯繫要點第 6 點第 2 項規定，就個資外洩案件之後續行政措施及處理情形，按季通報國發會。經查交通部及所屬公路總局與民用航空局（下稱民航局）辦理非公務機關個資外洩案件通報及行政檢查作業情形，核有：（1）交通部接獲其他公務機關函送汽車運輸業者個資外洩案件通報紀錄，惟自該部收受通報（111 年 4 月 18 日）起至函轉公路總局查處（111 年 5 月 24 日）止，已歷時 36 日，致未能依規定於 30 日內辦理行政檢查作業；（2）民航局接獲已遭媒體報導揭露之航空運輸業者個資外洩案件，卻判斷為一般案件，與聯繫要點規定為重大矚目之個資外洩案件範圍未合；（3）民航局收受航空運輸業者通報部分個資外洩案件，惟未依規定於 30 日內辦理行政檢查作業，逾規定期限 16 至 138 日不等，或多次要求業者補充相關教育訓練及改善情形等資料，惟已逾 252 日尚未結案，其後續行政措施及處理時間過長等情事，經函請交通部督促研謀改善。【詳總決算審核報告第 2 冊丙、拾肆、交通部主管項下重要審核意見（十八）】

4. 健保署為提升署內及各區業務組辦理承保相關業務服務效能，建置承保系統存放加退保及保費紀錄，惟未依規定辦理承保子系統及資料庫相關資通安全事項，暨建立 USB 隨身碟資料攜出及使用完畢刪除等管控機制，允宜研謀妥處，以完善個資保護制度及提升整體資安防護：中央健康保險署（下稱健保署）為提升署內及各區業務組辦理承保相關業務服務效能，於 92 年建置承保財務資訊系統（下稱承保系統），存放加退保及保費紀錄，系統開發費用約 2,000 萬元，每年維護費用約 1,000 萬元，截至 111 年底止，承保人數計 2,378 萬餘人。復為保護民眾個資及隱私，辦理全部資通系統導入 ISO 27001 ISMS 標準等資通安全應辦事項，並設置資通安全暨個資保護策進會負責監督與處理該署資通安全暨個資保護事宜。經查醫療健保個資管理及監督執行情形，核有：（1）承保系統內之異常管理輔助系統及自行開發之資訊需求單作業平臺子系統可供存取大量承保系統資料並下載儲存運用（圖 6），惟尚未落實辦理系統盤點、帳號與權限清查、安全性檢測等安全防護措施；（2）每年辦理承保系統資料庫使用帳號清查作業，惟漏未清查應用系統介接查詢承保系統資料使用之帳號，暨未依業務不同設定對應存取權

限；（3）相關人員自承保系統下載資料情形及 USB 隨身碟存取電腦資料過程（同圖 6），缺乏資料下載範圍合理性及最小化原則審查機制，與 USB 隨身碟資料攜出及使用完畢刪除等管控機制；（4）未依規定擬訂個資檔案接觸人員安全管理規範與建立個資事件之預防、通報及應變機制；（5）ISMS 第三方驗證範圍僅以資訊組織為主，未包含因業務運作需要，需頻繁接觸或查詢轉錄全民健保個資檔案之署內其他單位等情事，經函請健保署研謀妥處。【詳總決算審核報告第 2 冊丙、拾玖、衛生福利部主管項下重要審核意見（十二）】

圖 6　承保資料存取示意



資料來源：整理自健保署提供資料。

5.　退輔會為因應長照人力資源不足，於所屬榮家導入智慧照護產品輔助，惟使用者個資安全保護措施不足，允應檢討研謀妥處，以維相關資訊安全：國軍退除役官兵輔導委員會（下稱退輔會）為因應長照人力資源不足狀況，以資通訊科技輔助建構智慧醫療照護，自 108 年起陸續開放所屬 16 所榮家長照場域導入智慧照護產品。截至 112 年 4 月 14 日止，各榮家已導入或試辦智慧產品計 17 項，其中 3 項由退輔會與業者簽定契約或備忘錄，並視榮家需求統一導入；其餘 14 項則由榮家自行與合作單位洽商後導入。經查各榮家自行接洽導入之智慧照護產品，部分涉有將住民使用產品之個人生理健康紀錄（如生命體徵、睡眠狀況及活動路線）等屬個人資料保護法第 2 條第 1 項第 1 款所定義之個資，提供合作單位分析運用，其中除臺北榮家於開始試辦時即與合作單位簽訂契約，約定應遵守個人資料保護法及資料僅供計畫使用內容等事項外，其餘各該榮家僅於正式付費導入產品時，始與合作單位簽訂契約，且契約內容未包含個人資料保護法等資訊安全保護措施，存有資安風險，經函請退輔會研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾伍、國軍退除役官兵輔導委員會主管項下重要審核意見（一）1.(3)】