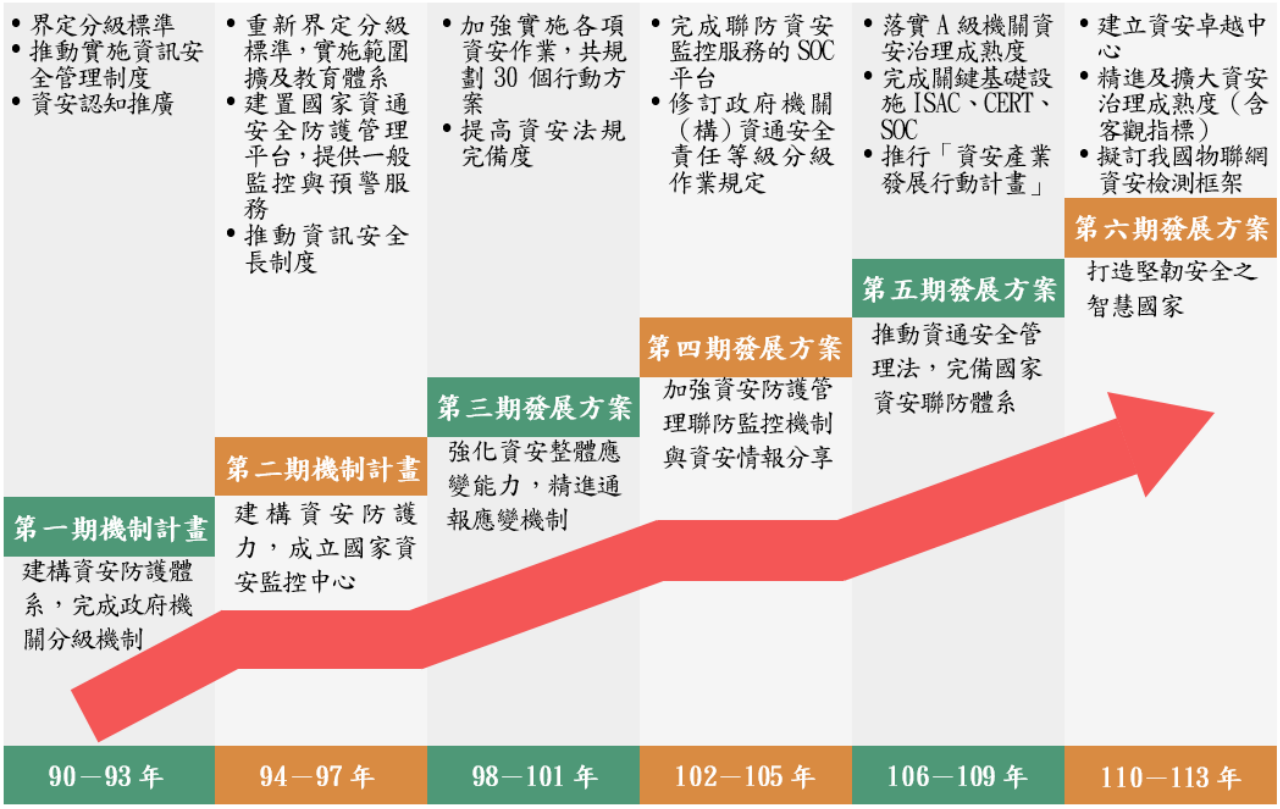
玖、政府推動資通安全防護執行情形

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安防護等作業，於 105 年 8 月設置資安專責單位－資通安全處。嗣數位發展部於 111 年 8 月 27 日成立，除接續擔任資安會報的幕僚單位，並研擬國家資安基本方針、政策及重大計畫，以及制定相關法規及規範。經查資安會報於 90 至 109 年間陸續推動「建立我國通資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 項四年期國家資安計畫（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

圖 1　政府資安推動歷程



註：1. 第一、二期機制計畫分別代表「建立我國通資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、六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）」、「國家資通安全發展方案（106 年至 109 年）」及「國家資通安全發展方案（110 年至 113 年）」。

2. 資料來源：整理自「國家資通安全發展方案（110 年至 113 年）」。

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）」（下稱第六期國家資安發展方案），作為政府現階段推動資安防護策略與計畫之指引。另聯合國永續發展目標（SDGs）核心目標 9 亦列有發展可靠、可持續及具有韌性之基礎設施，並推動創新等具體目標。茲將政府推動資通安全防護執行情形及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 年度推動之第六期國家資安發展方案，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（圖 2），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　第六期國家資安發展方案架構

資料來源：擷取自數位發展部資通安全署網站。

（二） 具體措施及執行機關

第六期國家資安發展方案共訂定「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，由數位發展部等 9 個部會分工負責（表 1），主要措施如次：

表 1 第六期國家資安發展方案分工情形

單位：項

部會別	主辦工作		
	參與策略	參與措施	負責細項工作
數位發展部	4	12	26
國家科學及技術委員會	2	4	6
經濟部	2	4	5
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

註：1. 策略、措施與細項工作可由不同機關共同主辦。
2. 資料來源：整理自第六期國家資安發展方案(112 年 5 月修正)。

1. 吸納全球高階人才，培植自主創研能量：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扎根，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」、「發展國家任務導向型及關鍵（核心）資安型前瞻研究」及「跨國人才交流與研究合作」等 7 項。

2. 推動公私協同治理，提升關鍵設施韌性：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. 善用智慧前瞻科技，主動抵禦潛在威脅：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。

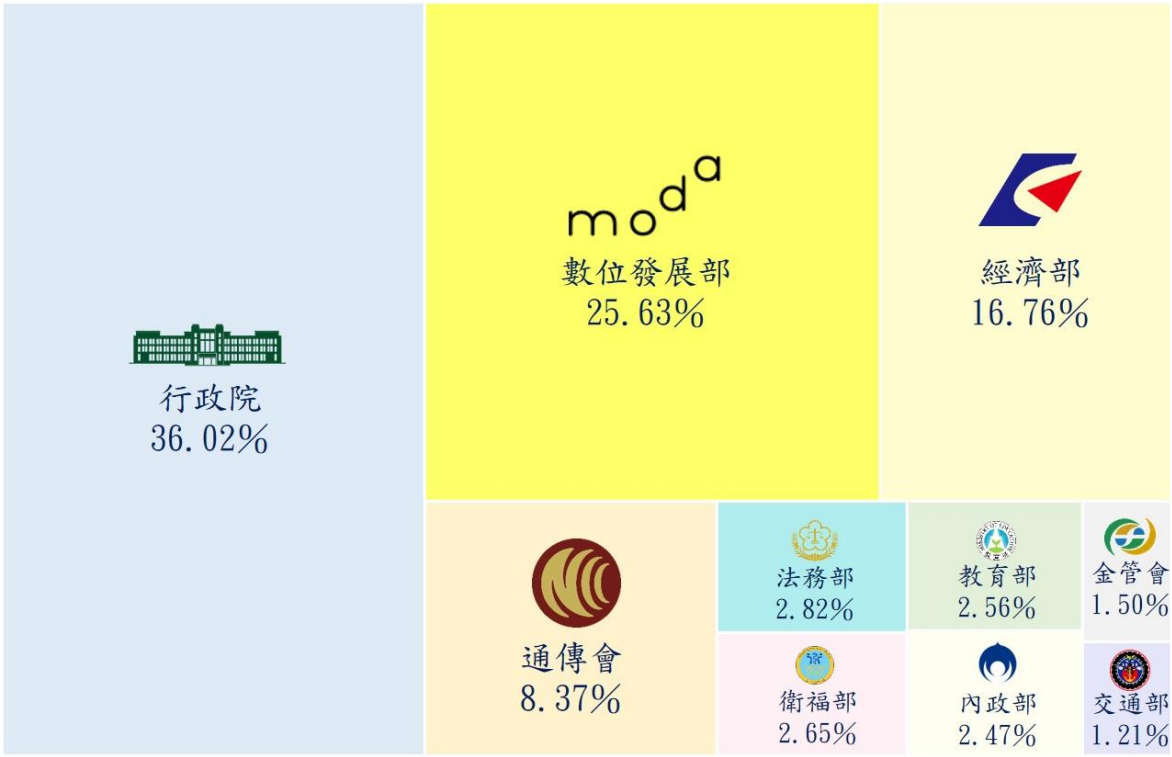
4. 健全智慧國家資安，提升民間防護能量：持續強化政府機關資安防護能量及委外供應鏈風險管理、協助電信業者聚焦 5G 資安風險議題，提出對應解

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」、「提升民眾資安意識」及「強化委外供應鏈風險管理」等 6 項。

（三） 執行成果

政府推動第六期國家資安發展方案，截至 112 年底止，累計編列預算數 35 億 9,112 萬餘元，累計執行數 32 億 6,691 萬餘元，預算執行率 90.97%，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 36.02%）最多，數位發展部編列 9 億 2,041 萬餘元（占 25.63%）次之，經濟部編列 6 億 192 萬餘元（占 16.76%）第三（圖 3）；其中 112 年度相關部會編列預算數計 10 億 7,265 萬餘元，以數位發展部編列預算 9 億 2,041 萬餘元（占 85.81%）最多。依數位發展

圖 3　第六期國家資安發展方案各機關預算編列占比



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 月間移撥至數位發展部資通安全署及數位產業署執行，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：整理自數位發展部資通安全署刊登於政府科技計畫資訊網之績效報告書。

部資通安全署（下稱資安署）提供第六期國家資安發展方案工作項目執行情形，區分為4大策略面向，茲就13項具體措施之工作項目執行成果擇要摘列如表2。

表2　110至112年度第六期國家資安發展方案具體措施執行成果

策略面向	執　行　成　果
吸納全球高階人才，培訓自主創研能量	1.**擴增高教資安師資員額與教學資源**：核定80名資安師資員額；建置2所區域網路中心實習場域並提供訓練；建置政府開放場域基礎環境暨實驗室，並訂定政府開放場域營運規章。 2.**挹注資源投入高等資安科研**：累計完成43項資安技術與機制研究；112年度參與2次會議與國際組織進行資安合作交流，及辦理1場大型國際資安政策研討會。 3.**培育頂尖資安實戰及跨域人才**：累計開發5門跨域資安實務課程，養成資安實務人才7,756人；每年完成2個以上資安職能訓練構面課程開發，累計培訓政府機關專職人力5,015人；引進國外頂尖資安實戰課程，及辦理資安菁英人才培訓課程，共培訓國內資安實戰人才382人。
推動公私協同治理，提升關鍵設施韌性	1.**建立各領域公私協同治理運作機制**：完成政府機關資安治理成熟度客觀指標3個及檢核項目1個；各關鍵基礎設施（Critical Infrastructure, CI）主管機關已訂定並推動CI提供者導入CI領域資安防護基準；CI主管機關於110、111及112年度分別稽核35個、43個及39個CI提供者；已訂定國家層級資安風險評估機制相關標準文件，並綜整CI領域國家層級資安風險評估結果，共計完成283個評估報告。 2.**增強人員資安意識與能力建構**：各CI提供者已完成資安長設置，建置領域資安專家資料庫；逐年開發相關課程，累計培訓逾2萬人；已建置3個CI模擬場域，分別為能源（油）、水資源及醫療領域之CI模擬場域，累計培訓逾90人次實戰人才。 3.**公私合作深化平時情資交流與應變演練**：依國際最新情資交換格式，完成國內資安事件通報單交換格式；各CI主管機關於110、111及112年度分別遴選8個、14個及10個CI提供者辦理攻防演練。
善用智慧前瞻科技，主動抵禦潛在威脅	1.**賡續推動政府資訊（安）集中共享**：已完成93.48%網路集中出口及6個機關導入內網威脅誘捕與惡意電郵偵測機制；A、B、C級公務機關與A、B級CI提供者導入資安弱點通報機制，導入完成率均已達100%。 2.**擴大國際參與及深化跨國情資分享**：110及111年度分別完成攻擊行為情資庫與智能威脅偵防平台及智慧資安威脅偵防服務平台；112年度導入8家場域實證建立示範應用。 3.**制敵機先阻絕攻擊於邊境**：110年度完成零信任網路身分鑑別、設備鑑別及信任推斷3大機制之研究，並協助2個機關試行零信任網路身分鑑別，完成部署驗證；111年度完成2個機關零信任網路身分鑑別機制導入；112年度完成2個機關設備鑑別導入。 4.**提升科技偵查能量防制新型網路犯罪**：完成高雄南部延伸鑑識實驗室；建立與國外企業調閱相關犯罪資料窗口16件；建置人工智慧（AI）犯罪偵查溯源分析系統及主動式全球資訊網路威脅行為溯源分析系統。
健全智慧國家資安，提升民間防護能量	1.**輔導企業強化數位轉型之資安防護能量**：受理並審核國內企業產品資安漏洞通報計357個；輔導40家高風險網路零售業者導入資安防護措施，及舉辦8場電商資安推廣活動。 2.**強化供應鏈安全管理**：完成85場機關資安稽核作業；完成晶片惡意邏輯威脅檢測工具1套；研發晶片旁通道攻擊檢測自動化工具1套；協助2家國內晶片業者之晶片產品通過晶片安全測試相關標準，並完成測試報告。 3.**建構安全智慧聯網**：已滾動檢討修訂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；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；112年度完成「監控平台資安評估規範」。

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 112 年度本部對政府推動資通安全防護執行情形所提重要審核意見，按制度規章、政策推動、計畫執行、資訊系統服務等四大面向，歸納摘述如次：

（一） 制度規章面

1. 資通安全管理法修正草案規定資安署得逕予調度各機關資安人員支援重大資安事件，惟有關人力調度、支援方式及保密措施，尚待研議相關配套措施等，允宜審慎研議配套措施，以完備國家資安環境：數位發展部為使資通安全管理法（下稱資安法）規範事項更符合實務運作，於 112 年 9 至 11 月間預告資安法修正草案，列有 4 項修法目標及相對應之 14 項修法重點。經查資安法修正草案第 18 條第 2 項規定，遇有重大資安事件，資安署得逕予調度各級機關資安人員支援。據資安署提供資料，110 年 9 月至 112 年 8 月底止，重大資安事件共計 112 件，平均每月發生 5 件，又該署統計，截至 111 年底止，中央政府資通安全責任等級（下稱資安責任等級）A 至 C 級公務機關（含行政法人）共 625 個（A 級 47 個、B 級 112 個、C 級 466 個），資安專職人數分別為 265 人、238 人及 424 人，以資通安全責任等級分級辦法規定資安責任等級 A 至 C 級機關須分別配置專職人員 4 人、2 人、1 人之標準檢視，人數缺口達 42 人。資安署調度各級機關資安人員支援重大資安事件前，允宜評估各機關資安人員之服務量能，避免影響機關資安防護作業；又對於重大資安事件調查、處理及改善資料均屬密件，其他機關資安人員對所支援之重大資安事件，其相關保密措施及支援方式亦待該署審慎研議，經函請數位發展部研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（三）1.】

2. 數位發展部為提高無人機資訊安全，已促成相關業者成立無人機資安實驗室，惟尚未會銜交通部發布無人機資安檢測指引，易引發外界對資安檢測標準適用疑慮，允宜儘速研議會銜交通部發布無人機資安檢測相關作業指引，俾無人機資安驗測機制有所依循：行政院為應無人機應用發展快速，責由數位發展部建立無人載具資安聯合驗測實驗室，經該部評估檢測量能，委由財團法人電信技術中心（Telecom Technology Center, TTC）與相關資安業者共同成立無人機資安聯合驗測實驗室（下稱無人機資安實驗室）、研訂無人機資安保障規範，提供無人機製造商資安檢測服務，該實驗室自 112 年 3 月 1 日起正式提供檢測服務。據行政院

第 5 次研商無人機相關議題專案會議決定，無人機資安檢測規範涉及資安專業，由數位發展部研訂無人機資安檢測指引，與交通部討論後會銜發布事宜等。經查無人機資安實驗室於 111 年 12 月 30 日出版「無人機資安保障規範」，並於 TTC 網站正式公告，其後又於 112 年 6 月進行第 1 次改版。據 TTC 統計，該實驗室自正式提供服務迄至 112 年 10 月底止，受理申請檢測件數 27 件，已完成檢測 19 件，累計收取檢驗相關費用 474 萬元，惟上開規範為民間實驗室自行發布，並非數位發展部會銜交通部發布，因尚乏法律明確授權，恐引發外界對無人機資安實驗室所作資安檢測項目基準及適用之疑慮，經函請數位發展部研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（三）3.】

3. 數位發展部數位產業署辦理電腦軟體共同供應契約採購，提供弱點通報機制（VANS）、端點偵測及應變機制（EDR）電腦軟體，以因應公務機關遵循資通安全責任等級分級辦法之應辦事項，惟 VANS 軟體品質不一，EDR 軟體尚乏雲端服務資安規範，且未通過資安院連通測試，允宜研謀改善，以提升政府採購電腦軟體服務品質：數位發展部數位產業署（下稱數產署）為節省機關與廠商逐案招（投）標所耗費人（物）力，辦理電腦軟體共同供應契約採購，品項包含具備資通安全弱點通報機制（下稱 VANS）與端點偵測及應變機制（下稱 EDR）功能之資安軟體，以因應公務機關遵循資安法規應辦事項。經分析臺北市等 16 個市縣政府資安責任等級 B 級機關 113 年 3 月份資訊資產，發現不同機關間，同一資產名稱與版本，部分未成功依資安署指定格式轉換，主要係市縣政府採購之 VANS 軟體存在中英文語系轉換問題，或比對資訊資產名稱之程序不完整所致；另共同供應契約提供之 EDR 軟體，部分未列於行政法人國家資通安全研究院（下稱資安院）EDR 連通測試廠商名單，恐造成機關無法回傳 EDR 偵測資料；又 EDR 軟體廠商持有機關資料並於雲端分析運算，似屬雲端服務，惟相關契約未參考資安院訂定之政府機關雲端服務應用資安參考指引，納列資訊雲端服務相關規範或機制，存有資安風險，經函請數位發展部督促研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（三）4.】

（二） 政策推動面

1. 政府為提升公務機關資安治理成熟度，於第六期國家資安發展方案明定 113 年度目標值，惟評核結果與預期目標仍有差距，允宜積極輔導協助，提升

資安治理能力，強化整體政府資安防護：政府為賡續推動落實資安法應辦事項，第六期國家資安發展方案之分年重要進程訂定 113 年度政府機關資安治理成熟度目標為所有 A 級政府機關成熟度達第 3 級以上，80%之 B 級政府機關成熟度達第 3 級以上。經查資安署辦理資安治理成熟度評核機制之輔導及推動業務情形，據該署統計 109 至 111 年度 A、B 級公務機關資安治理成熟度評核結果，111 年度 A 級機關成熟度達第 3 級以上之數量與比率較 109 年度減少原因，為每年滾動修正評核問項及新增客觀指標所致，惟其中 111 年度資安治理成熟度等級仍為第 0 級、第 1 級者，分別為 2 個、7 個（表 3），合計 9 個，占 A 級機關總數達 19.15%，仍待積極輔導各該機關提升資安防護能力；又 B 級機關 109 至 111 年度整體資安治理成熟度達第 3 級之比率逐年提升，惟與第六期國家資安發展方案所訂 113 年度 B 級機關成熟度第 3 級以上達 80%之目標值相較，仍存有差距等，經函請資安署研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（四）2.】

表 3　A 級與 B 級公務機關資安治理成熟度評核情形

單位：個、%

年度/分級 / 成熟度等級	109				110				111			
	A 級		B 級		A 級		B 級		A 級		B 級	
	機關數	占比	機關數	占比	機關數	占比	機關數	占比	機關數	占比	機關數	占比
合 計	**44**	**100.00**	**247**	**100.00**	**44**	**100.00**	**208**	**100.00**	**47**	**100.00**	**214**	**100.00**
已達第 3 級	**32**	**72.73**	**31**	**12.55**	**35**	**79.55**	**44**	**21.15**	**30**	**63.83**	**50**	**23.36**
Level 5	—	—	—	—	—	—	—	—	—	—	—	—
Level 4	2	4.55	5	2.02	1	2.27	—	—	2	4.26	2	0.93
Level 3	30	68.18	26	10.53	34	77.27	44	21.15	28	59.57	48	22.43
未達第 3 級	**12**	**27.27**	**216**	**87.45**	**9**	**20.45**	**164**	**78.85**	**17**	**36.17**	**164**	**76.64**
Level 2	5	11.36	64	25.91	4	9.09	83	39.90	8	17.02	102	47.66
Level 1	6	13.64	118	47.77	5	11.36	71	34.13	7	14.89	54	25.23
Level 0	1	2.27	34	13.77	—	—	10	4.81	2	4.26	8	3.74

註：1.資安治理成熟度等級分為 6 級，為「Level 0 未執行流程（Incomplete Process）」、「Level 1 已執行流程（Performed Process）」、「Level 2 已管理流程（Managed Process）」、「Level 3 標準化流程（Established Process）」、「Level 4 可預測流程(Predictable Process)」及「Level 5 最佳化流程(Optimizing Process)」。
2.資料來源：整理自資安署提供資料。

2.　數位發展部修正調降第六期國家資安發展方案之資料中心網路集中出口目標值，惟部分未完成網路出口向上集中之機關，未報經同意另設資料中心，允宜研謀改善，以落實資安防護：政府為強化基礎通訊韌性及安全，自第五期國家資安發展方案起，推動資訊資源向上集中策略，建置以部會為集中之資料中心，提升安全防護能量，並於第六期國家資安發展方案將範圍擴大至所有中央二、

三級機關，惟數位發展部報經行政院核定之第六期國家資安發展方案第2次修正，將原規劃「112 年以得設置資料中心之機關為單位，完成所有網路集中出口」目標，調降為維持90%網路集中出口，與行政院推動資訊資源向上集中政策未盡相合，恐影響原核定之預期效益；又依行政院及所屬各機關資料中心設置作業要點規定，行政院所屬三級或四級機關掌理特殊業務者，應報請上級機關核轉數位發展部同意後，始得設置資料中心，惟查部分未完成網路出口向上集中之機關，未報經數位發展部同意另設資料中心，恐未有相對應資料中心等級之強化資訊安全管制措施，使資安風險驟增，經函請數位發展部研謀妥處。【詳總決算審核報告第2冊丙、貳拾貳、數位發展部主管項下重要審核意見（四）1.】

3. 政府為因應國際趨勢與新型態資安攻擊及威脅，推動機關試行導入零信任網路，惟導入期程及作法，尚乏整體推動策略，允宜研謀妥處，以提升政府網路資安防護之成效：政府為因應新型態資安攻擊與威脅，於第六期國家資安發展方案之「善用智慧前瞻科技、主動抵禦潛在威脅」推動策略，規劃發展零信任架構資安防護環境，推動政府機關導入零信任網路，包含身分鑑別、設備鑑別及信任推斷3大核心機制，自111 年度起遴選文化部及國軍退除役官兵輔導委員會為試行機關，逐年導入零信任網路核心機制，後續並規劃優先推動資安責任等級A級公務機關導入。嗣數位發展部為加速A級公務機關於113 年前完成導入零信任身分鑑別制度，112 年度透過共同供應契約方式，由該部採購單一機關導入零信任身分鑑別制度之基礎環境所需軟硬體（總經費2,808 萬餘元），協助22個介接跨機關資料傳輸專屬通道（T-Road）之A級公務機關試行導入身分鑑別制度。按現行數位發展部及資安署已引導試行機關及22個A級公務機關擇選1個資通系統導入零信任身分鑑別制度，惟其他核心資通系統尚無導入規劃；另據資安署統計，截至111年底止，中央政府資安責任等級B至C級公務機關（含行政法人）共578個（B級112個、C級466個），C級以上機關均有自行或委外開發之資通系統，惟就導入零信任網路之期程及作法，亦乏整體推動策略，於各機關普遍面對資訊技術人力及現有預算資源不足困境下，後續擴大推動有其難度。又查各該機關導入零信任身分鑑別制度，其作法係由機關自行擇選1個具個資或高度敏感資料之資通系統試行，對象以該資通系統之維運人員（廠商）為主，未含括公務機關組織內部所有使用該資通系統之成員，且採現有網路存取機制與零信任網路併行方式運作，亦影響機關

導入零信任網路資安防護之成效。經函請數位發展部督同資安署結合相關資安政策，進一步研議各機關導入零信任網路之整體推動策略作法，以提升政府網路資安防護之成效。【詳總決算審核報告第2冊丙、貳拾貳、數位發展部主管項下重要審核意見（四）3.】

4. 金融業者及上市櫃公司均已依規定配置資安人力，惟部分公司之資安長未具資訊領域經歷，又逾5成之上市櫃公司仍未加入資安情資分享平台，允宜檢討精進輔導或監理措施，以厚植資安防禦量能：金融監督管理委員會（下稱金管會）為強化公司之資訊安全管理機制，要求符合條件之金融業及上市櫃公司應依規定指派副總經理以上或職責相當之人員兼任資安長。據金管會統計，截至112年底止，金融業及上市櫃公司均已完成資安人力配置，惟其中67家金融業及118家應於111年底設置資安長之上市櫃公司中，分別計有15家金融業及11家上市櫃公司之資安長未具資訊領域經歷，占比分別為22.39%及9.32%，另截至112年底止，須設置資安長及資安專責主管之上市櫃公司計有1,567家，惟仍有847家上市櫃公司尚未加入相關資安情資分享平台，約占54.05%；又近期上市櫃公司因發生重大資安事件發布重大訊息者，由112年度平均每月1.92件，攀升至113年1至3月之平均每月2.67件，並自112年下半年起迭因資訊系統遭駭客網路攻擊發生資安事件，顯示資安情資之重要性與日俱增，經函請金管會研謀改善。【詳總決算審核報告第2冊丙、貳拾肆、金融監督管理委員會主管項下重要審核意見（六）】

（三） 計畫執行面

1. 資安署補助市縣政府提升整體資安防護能量，惟補助計畫前置作業尚待精進，且未妥適訂定計畫目標，允宜檢討研謀善策，以提升計畫推動成效：資安署為提升市縣政府資安防護能量，辦理「政府基層機關資安主動防禦計畫」，期程為112至113年度，計畫經費9億2,000萬元，補助市縣政府推動資訊資源向上集中等項目，並依數位發展部補助地方政府強化資通安全防護作業要點規定，辦理市縣政府補助計畫之受理申請、審核及考核等作業。經查資安署補助市縣政府辦理「推動地方政府資訊資源向上集中」作業，112及113年度「計畫執行機關完成所屬機關資料中心減量」目標值為應減數量占總數各達5%及10%，惟訂定目標前，未先行與22個市縣政府研商訂定各年度預計達成資料中心減量目標，僅以有意願參與之市縣政府計算資料中心減量目標；另查市縣政府申請補助計畫，由較具

備資源優勢之直轄市政府負責彙整鄰近市縣計畫書，以共同提報分項計畫及接受督導訪視（表4），因相關作業時間僅1至6日，且尚須協調鄰近市縣彙整提報計畫，市縣政府尚無法全面盤點所屬機關需求，並據以規劃計畫執行進度等情事，經函請資安署檢討改善。【詳總決算審核報告第2冊丙、貳拾貳、數位發展部主管項下重要審核意見（五）1.】

表4　市縣政府共同提報分項計畫及接受督導訪視之區域劃分

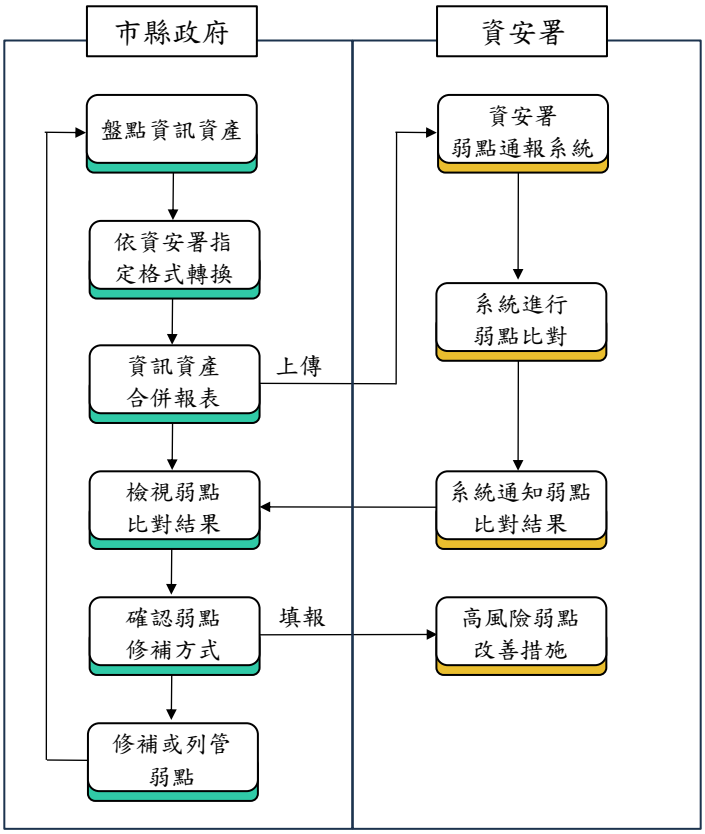
項次	直轄市（區域）	涵蓋市縣
1	臺北市	臺北市、花蓮縣、金門縣、連江縣
2	新北市	新北市、基隆市、宜蘭縣
3	桃園市	桃園市、新竹縣、新竹市、苗栗縣
4	臺中市	臺中市、彰化縣、南投縣
5	臺南市	臺南市、雲林縣、嘉義縣、嘉義市
6	高雄市	高雄市、屏東縣、臺東縣、澎湖縣

資料來源：整理自資安署提供資料。

2.　資安署補助市縣政府導入VANS機制，惟部分機關仍使用具資安疑慮或非公務軟體、部分資訊資產格式未成功轉換，及弱點修補作業配套措施未臻完善，允宜研謀妥處，俾利機關落實資安弱點風險評估，強化資訊資產之資安管理：

資安署協助市縣政府導入VANS機制（圖4），受補助之市縣政府每月應盤點伺服器主機與使用者電腦之作業系統及應用程式等軟體資訊（下稱資訊資產），並上傳至資安署建置之弱點通報系統進行比對後，至該系統填報高風險弱點改善措施及進行弱點修補，以利資安署掌握機關之資安風險。經查執行情形，核有：（1）行政院秘書長多次函示提醒各公務機關不應使用具資安疑慮或不得安裝非公務用軟體，經抽查16個市縣政府資安責任等級B級機關113年3月資訊資產，部分機關仍使用具資安疑慮或非公務用軟體，各為937項及783項資訊資產；（2）機關應依資安署指定格式轉換資訊資產，並上傳至弱點通報系統，經抽查16個市縣政府資安責任等級B級機關113年3月資

圖4　資通安全弱點通報機制管理流程



資料來源：整理自資安署提供資料。

訊資產，部分機關資訊資產未成功轉換為資安署指定之格式，其中 1 萬餘筆存有中英文語系轉換問題；（3）機關上傳資訊資產後，由資安署以電子郵件通知機關填報弱點修補改善措施，惟查 3 個縣政府部分資安責任等級 B 級或 C 級機關，仍有 112 年 11 月至 113 年 3 月間資訊資產漏未上傳或未依限填報弱點處置措施，資安署未於系統設計相關提醒機制，未能適時督導機關落實辦理；（4）弱點通報系統可將機關資訊資產與國際權威弱點資料庫（NVD）比對出弱點資訊，經分析 16 個市縣政府資安責任等級 B 級機關 113 年 2 月資訊資產，部分機關高風險弱點修補資訊僅提供 NVD 網站連結，機關須逐筆至 NVD 網站查找弱點修補建議，其查找過程繁瑣且費時等情事，經函請資安署研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（五）2.】

3. 資安署補助市縣政府落實法令遵循事項並培育資安人才，惟部分市縣政府 VANS 及 EDR 導入範圍未全面涵蓋核心系統，且紅藍軍攻防演練方式未盡周延，允宜研謀改善，以確保符合資安法遵要求及提升資安人才培育成效：據資通安全責任等級分級辦法及資安署網站公告之資安法常見問題 4.14 及 4.16 所示，資安責任等級 A 級、B 級、C 級機關應於規定時限內完成導入 VANS；A 級、B 級公務機關應於規定時限內完成導入 EDR，其導入範圍包含支持核心業務之資通系統主機與電腦。經查截至 112 年底止，市縣政府資安責任等級 B 級及 C 級機關之核心資通系統未導入 VANS 者約 15.52%、B 級機關之核心資通系統未導入 EDR 者約 5.92%，顯示資安防護範圍未全面涵蓋支持核心業務持續運作之主機與電腦，存有潛在資安風險；另查資安防護係持續性監控作業，市縣政府導入初期仰賴中央補助，計畫期程結束後由各市縣政府自籌經費持續辦理，布建範圍恐受市縣政府預算影響；又查資安署補助市縣政府辦理紅藍軍攻防演練，以培訓資安人才及強化市縣政府資安基礎環境，惟 2 個市縣政府僅參加演練結束後之教育訓練或以採購軟體測試環境辦理演練等情事，經函請資安署研謀妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（五）3.】

4. 數產署辦理智慧城鄉計畫，運用補助機制，形成民眾所需智慧應用服務，惟未落實查證廠商資安防護與個資保護情形，恐有資安風險，允宜檢討妥處，以降低資安風險：按第 2、3 期智慧城鄉生活應用發展計畫補助申請須知規定，廠商提供相關產品或服務須通過資安驗證；以及補助案件蒐集個資之特定目的消

失或於計畫結束前，應抹除儲存裝置之個人資料、機密資料及其備份資料，並留下紀錄。經查第 2、3 期智慧城鄉生活應用發展計畫補助案，其中 2 件補助案運用物聯網設備蒐集環境資訊，數產署未查證廠商提供之物聯網設備是否通過資安驗證；另有 6 件補助案涉及蒐集與儲存個資或機密資料，且置於公有雲端平台提供智慧城鄉服務，該署亦未要求廠商依規定提供刪除個資之佐證資料；又第 3 期中小企業行動智慧應用計畫補助申請須知規定，補助機關得隨時查核受補助廠商是否遵循個人資料保護法規定，惟數產署未將 8 件補助案之廠商資安執行情形納入查證範圍等情（表 5），經函請數產署檢討妥處。【詳總決算審核報告第 2 冊丙、貳拾貳、數位發展部主管項下重要審核意見（七）2.】

表 5　數產署未落實查證廠商執行資安防護情形

細部計畫名稱	期別	缺失態樣
智慧城鄉生活應用發展計畫	2	6 件補助案未要求廠商依規定提供刪除個資之佐證資料
	3	2 件補助案未檢視廠商提供之物聯網設備是否通過資安驗證
中小企業行動智慧應用計畫	3	8 件補助案未檢視廠商辦理資安及個資保護措施情形

註：1.資料截止日期：113 年 3 月底止。
2.資料來源：整理自數產署提供資料。

（四）　資訊系統服務面

1.　內政部開發戶役政資訊系統，並派送作業系統及相關軟體至全國各戶役政工作站，有助維護資料之機密性、可用性及完整性，惟面臨工作站作業系統版本不再支援更新，潛藏資安風險，允宜適時規劃導入作業系統更新機制，以強化戶役政資訊系統整體資通安全防護能力：內政部為辦理全國人民戶役政作業，開發戶役政資訊系統，管理全國民眾戶籍、兵籍之隱私資料，並依資安責任等級 A 級之標準，導入資訊安全管理制度，對於資料存取均有紀錄，並嚴密管控，各戶役政工作站之作業系統及相關軟體皆由內政部統一派送始能安裝。經查全國各戶役政工作站合計 6,945 臺，據微軟官方網站公告，其中 6,687 臺安裝作業系統版本（約占總臺數之 96.29%），已陸續自 109 年 12 月 8 日至 112 年 6 月 13 日終止服務，除安全性更新外，亦不再提供技術支援服務；另依資安院 113 年 3 月 13 日發布之「漏洞警訊公告」指出，微軟公司 Windows 10 專業版 1809、21H2、22H2 等作業系統存有高風險安全漏洞，已遭駭客利用，建議儘速確認並進行修復更新等，顯示作業系統版本於終止技術支援服務後，易被駭客發現及利用安全漏洞入侵電腦，潛藏資安風險較高。經函請內政部檢討改善，以強化戶役政資訊系

統整體資通安全防護能力。【詳總決算審核報告第2冊丙、柒、內政部主管項下重要審核意見（三）】

2. 故宮因應數位時代趨勢，推動數位轉型，惟未依資訊安全管理規範，落實辦理資通系統變更管理及作業環境控制措施等情事，允宜研謀改善，以避免機敏資料外洩：國立故宮博物院（下稱故宮）為典藏國家文物資源、維護文物安全，辦理文物數位圖檔等資訊檔案之輸出入保存及加值運用，並依資安法、資通安全事件通報及應變辦法等規定，建立故宮資訊安全政策、資通安全維護計畫及資訊安全管理制度（Information Security Management System, ISMS），進行資訊網路資安架構調整，嚴控對外服務設備存放區域權限，管制各區域網路連通等作業，以建立安全資訊作業環境。經查執行情形，核有：（1）開發文物高階圖檔影像降階程式進行圖檔降階處理及開放於數位典藏系統供外界讀取，惟未依故宮ISMS規範，落實辦理資通系統變更管理、區隔測試及正式作業環境等控制措施；(2)持續進行網路資安架構調整，惟對下載交付使用之文物高階圖檔未實施保存與使用情形之追蹤查察，未於使用單位使用目的完成後要求刪除及銷毀，核與故宮 ISMS 規範未合；(3)依ISMS規範盤點建立資訊資產清冊，惟以系統伺服器為標的建立之資訊資產清冊未包含員工端之電腦及周邊設備，未能涵括全院電腦機房、控制中心與相關辦公區域等實體資訊設備之資安防護；（4）建置票務系統提供雲端購票服務，系統存有個人資料及線上交易資訊，惟未參照政府機關雲端服務應用資安參考指引（表6），將雲端服務資安控制措施納入既有資通安全維護計畫等情事，經函請故宮研謀改善。【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（二十四）】

表6 雲端服務資安管理應納入資通安全維護計畫項目及內容

序號	資通安全維護計畫項目	內容
1	資通安全政策及目標	有獨立篇幅說明雲端服務資安政策。
2	資通安全推動組織 專職（責）人力及經費配置	說明機關對雲端服務資安管理人力配置。
3	資通安全風險評估	加入對雲端服務資安風險評鑑過程，並調整相關附件。
4	資通安全防護及控制措施	增修因雲端服務資安風險處理計畫而產生之額外相關控制措施。
5	資通安全系統或服務委外辦理之管理	增補因雲端服務所產生之額外通報與應變流程。
6	資通系統或服務委外辦理之管理	增補對雲端服務提供者之選商與管理監督程序，並調整相關附件。
7	資通安全維護計畫、實施情形之持續精進及績效管理機制	增補對雲端服務提供者之稽核過程，並調整相關附件。

資料來源：整理自政府機關雲端服務應用資安參考指引（V1.2）。