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。據行政法人國家資通安全研究院（下稱資安院）112 年 6 月 16 日公布「政府零信任架構」說明及美國國家標準技術研究院建議，導入零信任架構是一段逐步成熟之過程，非一次大規模替換基礎架構與存取流程，導入範圍須由機關考量其系統重要性、人力及預算逐步推動。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。據復：將持續與資安署及資安院緊密合作，由該部推展政府機關導入零信任機制，資安署研擬全國資安發展策略，資安院就零信任機制軟體執行技術驗證工作，並持續滾動修正，協助推動地方政府導入零信任機制，以完備政府資安防護深廣度等。

（五） 資安署為提升資安防護能量，補助市縣政府辦理資通安全弱點通報機制及培育資安人才等事項，惟補助計畫前置作業尚待精進、整體計畫目標訂定未臻周妥、資通安全弱點通報管理措施未臻完善，及紅藍軍攻防演練方式未盡周延等情事，允宜研謀改善，以落實政府資安防護。

前行政院資通安全處及承接業務之數位發展部資通安全署（下稱資安署）為提升市縣政府資安防護能量，及落實第六期國家資通安全發展方案（110 至 113 年度）之「善用智慧前瞻科技，主動抵禦潛在威脅」推動策略，陸續推動「強化政府基層機關資安防護計畫」，期程為 110 年 7 月至 111 年 6 月，計畫經費 2 億 1,500 萬元，及「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，並集中資源導入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）等資通安全管理法所定應辦事項，以強化資安防護機制，提升整體資安防護能量，達到主動發現潛在威脅及降低資安風險之目標。經本部及所屬各地方審計處室抽查相關計畫執行情形，核有下列事項：

1. 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：資安署為提升市縣政府資安防護能量，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，影響整體計畫推動成效；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之合作模式辦理(表 8)，據各直轄市及相關市縣政府反映，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，作業時間有所不足，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，影響提報計畫內容完整性等情事，經函請資安署檢討改善。據復：後續補助計畫提報作業，將於相關說明會宣導說明，以各市縣政府現有基礎推動資安防護作業，及可提出個別性資安防護作業需求之彈性，俾利市縣政府預為規劃準備，另俟補助計畫核定後，通知各市縣政府於合理之作業時間內依最新需要修正分項計畫，使整體計畫更為周延。

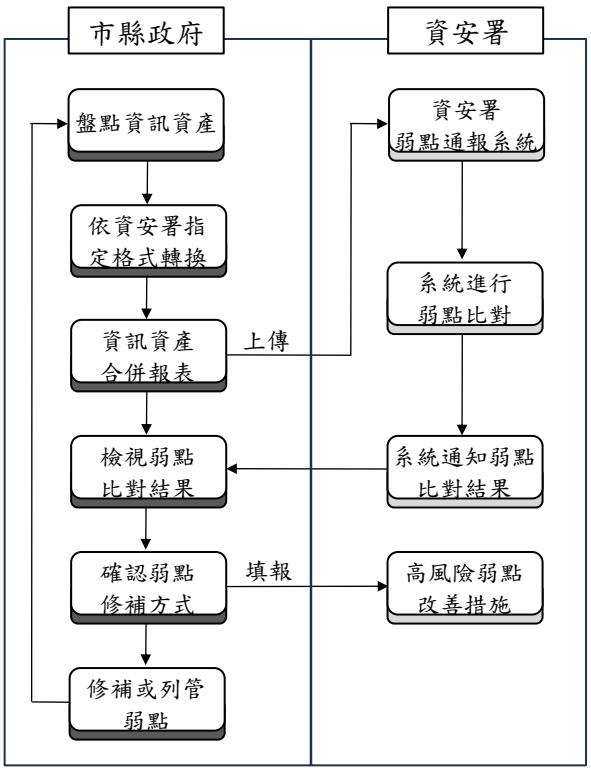
表 8　市縣政府共同提報分項計畫及接受督導訪視之區域劃分

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.　補助市縣政府導入資通安全弱點通報機制，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：資安署協助市縣政府導入 VANS 機制（圖 1），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)，依資安署指定格式轉換，併同資產名稱、資產版本等資訊合併成報表，定期上傳至資安署建置之弱點通報系統，該系統可自動進行比對，羅列出資訊資產弱點並通知機關，機關應定期至該系統填報高風險弱點（CVSS 7 分以上）改善措施並進行弱點修補，落實導入 VANS 之效益；另資安署可透過弱點通報系統掌握機關之資安風險，以強化資訊資產之資安管理。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，以避免機敏公務資訊外洩或造成國家資通安全危害風險，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

圖 1　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。

937 項及 783 項資訊資產，與上述函示未合，存有資安疑慮；（2）機關應依資安署指定格式轉換資訊資產，上傳弱點通報系統進行自動化弱點比對，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，影響後續資安弱點比對；（3）機關上傳資訊資產於弱點通報系統比對後，由資安署以電子郵件通知機關至該系統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，影響機關導入 VANS 之預期效益；（4）弱點通報系統可自動將機關資訊資產與國際權威弱點資料庫（NVD）比對，羅列出資訊資產所對應之弱點資訊，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，方能確認處置方式，查找過程繁瑣且費時等情事，經函請資安署研謀妥處。據復：（1）已於資訊主管聯席會及資通安全防護巡迴研討會重申，公務機關不得使用具資安疑慮或非公務用之資通訊系統政策，並將持續關注及督導市縣政府資訊資產盤點情形；（2）將彙整機關資訊資產格式轉換失敗樣態，供開發廠商據以檢視調修程式邏輯，預定於 113 年公布通過轉換測試廠商名單；另持續研析提升中文軟體弱點比對完整度之作法及可行性，以降低相關軟體發生之資安風險；（3）已於新版弱點通報系統提供相關管理功能，將定期檢視機關導入、上傳資訊資產數量等情形，暨適時予以輔導；（4）新版弱點管理系統除將提供原廠修補資訊連結，供機關參考使用，另規劃於弱點通報系統標示常被利用之高風險弱點，以利機關優先處置。

3. 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：依資安責任等級分級辦法附表 1 至 6 規定，資安責任等級 A 級、B 級、C 級之公務機關及關鍵基礎設施提供者（特定非公務機關）應導入 VANS；資安責任等級 A 級及 B 級公務機關應導入 EDR。另據資安署網站公告之資安法常見問題 4.14 及 4.16 所示，有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入 VANS 及 EDR。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 者計 218 個（約 15.52%）、B 級機關之核心資通系統未導入 EDR 者計 38 個（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，透過模擬駭客入侵攻擊手法，進行機關系統資安檢測，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，影響市縣政府人才培育成效及防護能量等情事，經函請資安署研謀妥處。據復：將督促相關市縣政府核心資通系統導入 VANS 及 EDR，並瞭解各市縣政府補助計畫結束後之持續營運規劃，爭取經費補助建置資安法各應辦事項；另將請 113 年辦理紅藍軍攻防演練之市縣政府妥善規劃，並透過實地訪視檢視辦理成效，以符計畫實質效益。