（十三） 資通安全管理法各納管機關（構）於落實應辦事項及資訊作業委外安全管理等方面，間有實施範圍不足或未盡落實等共通性待改進事項；另該法授權行政院實施公務機關資安外部稽核之對象，未涵蓋總統府、行政院以外四院及地方政府，允宜研議擴大稽核對象，並訂頒相關文件範本及參考指引，俾優化各機關第二方資安稽核品質。

政府自 90 年起漸進推動資安基礎建設，以風險導向陸續建構資安責任等級分級、資安事件通報應變、資訊系統分級及資安防護基準、資安治理成熟度評估等機制，嗣於 107 年 6 月 6 日完成資通安全管理法之立法，連同 6 項配套子法於 108 年 1 月 1 日起施行，將相關風險評估、管理、應變措施提升至法律位階。上開資通安全管理法及各配套子法截至 109 年底止已實施 2 年，經查各納管機關（構）依相關法規整備資安環境及落實各應辦事項情形，核有下列事項，已函請行政院研謀妥處，本部業列管注意後續辦理情形：

1. **中央政府各機關（構）依資通安全管理法及相關配套子法規定推動各項資安防護工作，核有尚未依規定提報資通安全等級等共通性待改進事項，亟待引導及督促各機關（構）依法落實辦理：**中央政府各資通安全責任等級 A 級機關，及各上級（監督）機關暨中央目的事業主管機關依資通安全管理法及相關配套子法規定落實情形，核有：(1) 財團法人原住民族語言研究發展基金會已於 109 年 2 月 22 日成立，惟截至 110 年 3 月 8 日止，尚未經該管上級機關依規定提報資通安全責任等級。另國立臺灣大學附設醫院新竹生醫園區分院於 109 年 1 月 1 日成立，並於 110 年 1 月 1 日與新竹分院、竹東分院合併為新竹臺大分院，教育部於 110 年 3 月 10 日始提報資通安全責任等級，且截至同年 5 月 10 日尚未經行政院核定，恐未能及時接軌相關資安規制；(2) 行政院國家發展基金及其管理會推動國家創新轉型發展相關政策，宜由資通安全管理法完整納管，惟其管理機關國家發展委員會之資通安全維護計畫實施範圍未涵蓋該管理會，該管理會亦未依分級辦法相關規定經行政院個別核予資通安全責任等級；(3) 行政院已於 109 年度中央及地方政府資通安全長及資訊主管會議宣導勿以資安事件數作為資安業務績效衡量指標，並鼓勵機關確實依限通報資安事件等，惟仍有部分機關以資安事件數量作為資安業務績效衡量指標，恐產生資通安全事件通報意願降低或逾期通報等不利影響；(4) 部分機關業依規定辦理資安內部稽核作業，惟其稽核計畫擬定、稽核實施、報告研提、改善追蹤等事項皆由資訊單位辦理，未依行政院國家資通安全會報「資通安全維護計畫範本」之建議適當劃分權責；另部分機關委託資安輔導顧問公司辦理內部稽核作業，雖有機關內部資安稽核人力或專業不足等實務考量，惟仍與上開範本建議意旨不符，恐損害稽核獨立性；(5) 部分機關辦理資安內部稽核範圍僅限資訊單位、核心資通訊系統，或資訊安全管理系統標準（下稱 ISMS）導入範圍等，並未涵蓋全組織，核與行政院國家資通安全會報「資通安全管理法常見問題」之相關回應未合；

（6）部分機關之資通系統，尚未全數完成資通安全責任等級分級辦法附表十所訂各項資通系統防護基準控制措施，且未依上開分級辦法第 11 條第 3 項規定報請該管上級機關同意及主管機關備查後免予執行；(7) 部分機關依資通安全責任等級分級辦法附表一（資通安全責任等級 A 級之公務機關應辦事項）辦理資通安全健診，惟囿於經費不足或操作限制等原因，健診項目之使用者端電腦惡意活動檢視範圍未涵蓋全數使用者電腦，甚至檢測覆蓋率低於 10%，核與行政院國家資通安全會報「資通安全管理法常見問題」之相關回應未合；(8) 依資通安全責任等級分級辦法附表一（資通安全責任等級 A 級之公務機關應辦事項）規定略以，A 級機關全部核心資通訊系統應於初次受核定或等級變更後之 2 年內，導入 CNS 27001 或 ISO 27001 等 ISMS，並於 3 年內完成第三方驗證。部分機關依據上開規定辦理 ISMS 委外輔導及第三方驗證，核有以同一標案合併辦理，並以通過第三方驗證為計價或驗收條件之情事，恐影響驗證作業之獨立客觀等共通性待檢討改善事項。經函請行政院加強法規宣導及輔以資安稽核，賡續督促、輔導各納管機關（構）落實遵法義務，並評估就機關導入及取得 ISMS 驗證訂定標準作業流程或相關行政指引之可行性，俾引導機關依循較適作法以降低相關風險。

2. 中央政府各機關（構）於推動資訊作業委外安全管理方面，間有納管範圍不足或法遵事項未盡落實等情事，允宜督促檢討辦理，俾降低資訊作業委外之資安風險：依資通安全管理法第 9 條、同法施行細則第 4 條及第 6 條第 1 項等規定，公務機關或特定非公務機關，委外辦理資通系統之建置、維運或資通服務之提供，應依相關注意事項選任適當之受託者，並監督其資通安全維護情形；公務機關或特定非公務機關之資通安全維護計畫，應包括資通系統或服務委外辦理之管理措施。行政院復為完備各納管機關資通安全維護計畫之委外管理措施相關規範，於「資通安全維護計畫範本」建議各納管機關分節訂定「選任受託者應注意事項」及「監督受託者資通安全維護情形應注意事項」，並提供「委外廠商查核項目表」範本供各納管機關辦理對委外廠商稽核作業之參考。經抽核 108、109 年度行政院資安稽核報告，及部分納管機關(構)依上開規定辦理資訊作業委外管理情形，核有：(1) 部分機關僅針對核心資通系統訂定委外管理程序，未涵蓋非核心資通系統之建置、維運或資通服務提供等事項，委外管理範圍尚有不足；(2) 部分機關（構）未依自訂之資訊作業委外管理相關規範落實辦理委外廠商稽核作業；(3) 部分機關參考行政院「委外廠商查核項目表」範本辦理委外廠商稽核，惟稽核紀錄僅勾選「符合」、「不符合」或「不適用」，未具體描述實際查核發現，不利覆核及追蹤後續改善情形；(4) 部分機關委外開發或維運之資通系統，未按資通安全責任等級分級辦法第 11 條第 2 項規定，依防護需求分級原則完成資通系統分級，或未於委外契約中明確定義防護基準需求；(5) 部分機關以補助案形式委辦核心資通系統開發維護，惟未依資通安全管理法施行細則第 4 條規定自行

辦理或委託第三方進行安全檢測等情事。按近年政府機關資安事件之根因之一，係資訊（安）供應商之資安管理完備度未盡嚴謹，且政府機關疏於監督管理，致產生資安破口所致；又據本部調查，中央政府各機關普通公務預算之資訊委外預算占總資訊預算比率，業自 108 年度之 59.72%逐年遞增至 110 年度之 62.51%（表 18），顯示各機關資訊作業委外辦理情形有增加趨勢，委外安全管理措施之完備及落實，益顯重要。經函請行政院督促各納管機關（構）賡續檢討及強化對委外廠商之資安要求及有效監督管理，確保委外開發或維運之資通系統皆有效落實法定應辦事項及防護基準，俾降低委外資安風險，提升政府機關資安防護水準。

表 18　中央政府各機關普通公務資訊委外預算編列情形

單位：新臺幣千元、%

年度／項目	108	109	110
資訊預算	15,940,872	16,664,599	16,931,599
資訊委外預算	9,519,232	10,037,349	10,583,409
委外占比	59.72	60.23	62.51

資料來源：整理自各中央政府機關提供資料。

3.　資通安全管理法授權行政院實施公務機關資安外部稽核之對象，未涵蓋總統府、行政院以外四院及地方政府，允宜研議賦予法規主管機關必要時得稽核所有納管機關權限之可行作法，俾適度透過外部稽核機制強化政府機關資安防護整備：行政院為協助各機關強化資通安全防護工作之完整性及有效性，於行政院國家資通安全會報之網際防護體系下設「資通安全防護組」，自 90 年起每年選定重要機關辦理資安外部稽核，透過稽核作為持續改善以提升政府資安防護水準。資通安全管理法自 108 年起正式施行後，行政院及各納管機關賡續依該法第 7 條第 2 項、第 13 條第 1 項、第 16 條第 4 項，及第 17 條第 3 項等規定辦理對所屬（監督）公務機關及所管特定非公務機關資安稽核作業（下稱第二方資安稽核），據行政院 109 年 8 月於中央及地方政府資通安全長及資訊主管會議所作報告內容略以，資通安全管理法第 13 條第 1 項授權行政院實施公務機關第二方資安稽核作業之對象，僅限行政院所屬中央二級機關，至於行政院體系以外公務機關，該院依法尚無稽核權限。據本部抽查總統府、立法院、監察院、司法院、考試院（下稱四院一府）及其所屬，暨地方政府落實資通安全管理法及相關配套子法情形，部分機關核有：(1) 資通訊系統尚未全數依資通系統防護基準完成相關控制措施；(2) 資安內部稽核範圍，僅限核心資通訊系統或資訊單位，尚未涵蓋全組織；(3) 尚未落實依資通安全管理法第 13 條第 1 項稽核所屬機關資通安全維護計畫實施情形；(4) A 級公務機關 109 年度資安治理成熟度評估結果，尚未達國家資通安全發展方案（106 年至 109 年）所訂成熟度達第 3 級以上之績效目標；(5) 未將物聯網設備納入資訊資產盤點範疇，及未依規定頻率辦理核心資通系統弱點檢測等情事；又近年銓敘部、總統府、臺北市政府衛生局陸續發生公務人員個資外洩、系統遭受滲透攻擊、市民資料被駭客竊取等重大資安事件，顯示四院一府及其所屬，暨地方政府

於資通安全管理法遵法情形及整體資安防護整備等面向，仍有尚待落實及改進空間。惟現行資通安全管理法並未授予法規主管機關，於必要時得主動對所有納管公務機關實施資安稽核之權限，恐不利資安法規主管機關發揮其督導權責。經函請行政院研議賦予法規主管機關對於所有納管機關主動稽核權限之可行作法，俾適度透過外部稽核手段強化政府機關資安防護整備。

4. 據行政院辦理第二方資安稽核輔導作業之共通性建議意見，核有受輔導機關稽核文件內容未臻完備、稽核人員對資通安全管理法規認知不足等共通性缺失，允宜研議訂頒相關文件範本及稽核參考指引，俾協助優化各機關第二方稽核文件品質、提升資安稽核人員專業知能：行政院為督促各機關落實資通安全管理法分層管理監督精神，提升各上級（監督）機關及中央目的事業主管機關對所屬（監督）公務機關及所管特定非公務機關之資安稽核品質，每年度規劃辦理第二方資安稽核輔導作業，復為培育政府機關資安稽核人力，確保政府機關自辦資通安全稽核作業成效，自 107 年起辦理政府機關（構）資通安全稽核員培訓及遴選作業計畫，由行政院及所屬中央二級機關、地方政府推薦觀察員人選參與培訓。經查，行政院 108 及 109 年度辦理第二方資安稽核輔導作業，對受輔導機關提出之共通性建議意見，包括：部分稽核委員僅對自身熟悉之領域深度訪談，致查核事項受限，又部分稽核委員對於資通安全管理法及其子法法規要求瞭解深度不足，建議於稽核前安排稽核訓練，以強化稽核委員對於法規瞭解程度，並適度擴大查核範圍；建議受輔導機關於稽核計畫增列作業時程與重點工作，以利受稽機關瞭解稽核作業時程與要求；建議於稽核計畫增列稽核團隊成員保密義務與利益迴避之規定；建議於稽核報告增列抽樣聲明；稽核報告項目宜明確列入稽核目標、稽核範圍、稽核機關、稽核團隊、受稽核機關介紹、稽核日期與地點、稽核準則之聲明、稽核結論等事項。鑑於行政院期藉由辦理第二方資安稽核輔導及資安稽核員培訓計畫以促進各機關資安稽核作業品質，暨提升稽核人員專業素養與實務經驗，惟該院之稽核輔導及人員培訓量能有限，尚難全面實施至所有適用機關。經函請行政院研議彙整各機關辦理第二方資安稽核常見缺失及應注意事項，據以研訂第二方稽核作業相關文件範本，供各納管機關參考運用之可行性，俾透過知識分享提升稽核人員專業知能，進而強化政府整體資安稽核量能。

（十四） 政府推動智慧政府行動方案，規劃全面換發數位身分識別證及建立資料交換機制基礎架構，提供民眾數位服務及優化決策品質，有助數位轉型，惟部分工作項目執行未如預期或尚待持續辦理，亟待研謀改善。

我國自 87 年開始推動電子化政府，完成多項里程碑，包括網路報稅、電子發票、電子公文、雲端病歷、開放資料等項目，行政院為引導各級機關以民眾需求為訴求，優先以數位化方式發展政府服務等目標，於 105 年 11 月 24 日核定「數位國家・創新經濟推動方案」。嗣行政院院長