數位發展部主管113年度單位決算評估報告

二、部分公務機關資安作業仍待改善，允宜督導並協助機關完備相關防範措施，俾有效降低資安風險

資通安全署113年度「資通安全業務」預算數4億9,195萬3千元，決算數4億7,561萬3千元，決算數占預算數比率96.68%，係辦理國家資通安全政策之規劃、資通安全事件應變處理、輔導及培訓機關資安能量、各級政府資安稽核、攻防演練及推動相關資安計畫等。經查：

(一)113年度公務機關資安通報，以非法入侵事件占比最高

依資通安全管理法第6條第1項規定[1]略以，主管機關應定期公布國家資通安全情勢報告及資通安全維護計畫實施情形稽核概況報告等。就113年度國家資通安全情勢報告觀之，113年全球資安威脅情勢可歸納6大面向，包含駭客利用AI技術發展新型態入侵與惡意詐騙、個人資料與憑證外洩致防護機制失效、社交工程泛濫致APT攻擊與勒索軟體風險增加、資安(訊)供應商遭駭致破壞供應鏈安全、資通系統弱點頻遭揭露利用及雲端應用服務衍生多元威脅等；另就113年1至12月之監控情資觀之，資安威脅類型中資訊蒐集占43.2%、入侵攻擊占18.8%、入侵嘗試占17.9%，合計高達79.9%[2]；復參113年公務機關資安通報統計，以非法入侵事件占62.52%為最高，顯示惡意攻擊行

[1]依資通安全管理法第6條第1項規定：「主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應每年公布國家資通安全情勢報告、資通安全維護計畫實施情形稽核概況報告及國家資通安全發展方案。」

[2]資訊蒐集主要係針對透過掃描、探測及社交工程等攻擊手法取得資訊情資之資訊蒐集行為；入侵攻擊主要為針對系統與服務成功破壞之行為，造成未經授權存取或取得系統服務資源與權限，包含成為殭屍網路之受害者；入侵嘗試係針對嘗試入侵未經授權主機之情資，包含試圖透過暴力破解或利用已知與未知漏洞等攻擊手法，嘗試破壞與干擾系統服務。

為占比高且集中。

(二)113 年度部分公務機關資安作業仍待改善，允宜追蹤受稽核機關後續改善情形，適時給予輔導

觀 113 年度公務機關資安稽核結果，待改善事項包括：部分機關業務持續運作演練未切合實際，且未妥適規劃備份資料之復原程序；資通安全政策及目標未臻妥適，或目標、指標設定過低；持續精進及績效管理機制未確實執行；未落實監督及管理委外廠商工作；未完整盤點資通系統及資訊資產、未妥適界定核心系統及系統分級；內部稽核辦理範圍、頻率及稽核項目規劃未臻妥適；未完成全部高風險弱點之修補，或完成修補前未加強管控或採行緩解措施；資安事件通報作業仍有未符規定情形；資安防護控制措施之執行未完備等。為強化資安防護量能，允宜追蹤受稽核機關後續改善情形，並促請該等機關落實強化資安防護工作。

綜上，113 年度全球與國內資安威脅態勢更趨多樣化，非法入侵及相關惡意攻擊行為已成公務機關資安事件之主要來源，且非法入侵占比高達六成；然部分公務機關於資安治理與作業面仍有缺失，資安管理制度落實容有精進空間，允宜督導並協助機關完備相關防範措施，以有效降低資安風險，俾能強化整體資安韌性及提升公務體系之防護能量