近年強化國家數位韌性預算執行及相關問題探討-以數位發展部主導計畫為例

一、我國對強化國家數位韌性之政策目標及執行成效

數發部以強化國家數位韌性、驅動數位經濟發展及積極推動打詐工作等三大方向為 114 年度之施政主軸，其中為強化我國面對災害與資安威脅之應變能力，數發部與相關部會推動建構多元異質應變通訊網路、強化資通安全韌性，深化資安防護量能；推動資安法制調適，厚植資安職能培力、強化政府民生關鍵系統運作韌性等數位韌性政策目標(詳表 2-1)，茲就各項目標執行成果說明如下：

(一)建構多元異質應變通訊網路：為強化我國在災害或突發事件下之通訊應變能力，數發部推動多元異質通訊網路之建構，打造海、陸、空三維備援體系，以確保緊急情況下政府指揮與救災單位基本通訊不中斷。具體措施包括補助電信業者於偏遠與離島地區建設微波鏈路與海底電纜、導入非同步軌道衛星通訊技術、推動災難漫遊與公共安全通訊系統，並整合衛星與 5G 行動網路提供多元傳輸管道。另透過公私協力與資安要求，持續督導通訊基礎設施業者強化資安防護與緊急應變機制。此外，並加速推動偏鄉寬頻與 5G 建設，縮短數位落差，提升網路覆蓋與韌性等。然面臨低軌衛星代理商調漲費率，且未來須與電信業者協調商轉機制等之挑戰。

(二)強化資通安全韌性，深化資安防護量能；推動資安法制調適，厚植資安職能培力：數發部從法規調整、技術強化、人才培育與國際合作等面向推動資安工作，明確機關責任並強化資安管理與人力配置，並透過說明會廣泛蒐集意見，確保制度落實；另規劃第七期「國家資通安全發展方案(114 年至 117 年)」草

案，結合政府、產業與人才 3 大要素，打造健全之資安防護體系，推動 AI 與新興科技應用。數發部並積極參與國際資安交流，與多國建立合作關係，推動情資共享與聯防；建構資安聯防機制，自動化分享威脅情資與黑名單，協助機關即時應對攻擊；並推廣零信任網路架構與關鍵基礎設施資安標準，提升整體防護能力。

(三)強化政府民生關鍵系統運作韌性：為強化政府關鍵民生系統在災害或突發事件下之持續運作能力，數發部推動雲端備份與回復計畫，協助各機關建立跨境公有雲之加密與分持備份程序，完成實地演練與系統備份功能設計，提升應變能力。透過檢討會議，彙整執行經驗並提出改善建議，以擴大成效，並培訓具備國際標準能力之營運管理專業人員，進一步強化系統韌性與備援能力。

表 2-1　數發部 114 年度「強化國家數位韌性」之政策目標說明表

數位韌性政策目標	現況說明	執行難度說明	需配合機關	預計達成日
建構多元異質應變通訊網路	數發部已積極建構「多元異質」之通訊系統，包含固定通訊網路、行動通訊網路、海纜、微波、衛星等，透過備援再備援方式，確保臺灣遇到重大災難時，即使部分通訊系統無法提供服務，仍有其他通訊管道可提供指揮體系基本通訊需求。	1. 目前非同步衛星驗證網路所採用之低軌衛星系統之獨家代理商，調漲通訊資費，致預算不敷支應。 2. 完成多元異質通訊網路概念性驗證後，需與電信業者研議、協調轉換為商用服務，俾需求單位長時間使用。	政府指揮體系關鍵部會	114.12.31
強化資通安全韌性，深化資安防護量能；推動資安法制調適，厚植資安職能培力	資安署已積極推動調適資安法規，強化資安聯防機制及關鍵基礎設施治理作為，透過國家資安聯防監控通報機制，分享國內外資安訊息，並推動關鍵基礎設施(CI)領域之資安防護基準及深化政府	114 年國際資通安全事務合作策略之規劃及推動。(本項計畫經立法院預算刪減，無法派員參加國際交流會議、技術研討會議、國際(法規)會議等)	各相關機關	114.12.31

數位韌性政策目標	現況說明	執行難度說明	需配合機關	預計達成日
	資安防護。另已增設公務人員高考資安類科及「政府資安人力職能轉換訓練計畫」，協助非資訊處理職系現職公務人員取得資安專長及職能，強化智慧國家數位安全韌性。			
強化政府民生關鍵系統運作韌性	每年擇定民生關鍵資訊系統及機關主要業務系統進行數位韌性健檢作業。	政府資訊系統可能會因使用者過多而當機，或是可能因系統、網路架構設計不良而回應緩慢。從機制面與技術面進行巡航健檢，協助機關人員檢視系統架構並給予專業建議，並透過實地輔導協助機關落實數位韌性。	受數位巡航健檢之資訊系統涉及民生關鍵資訊系統之主管機關	114.12.31

資料來源：數發部提供。