政府因應先進AI資安風險政策

壹、先進AI帶來的資安新挑戰

人工智慧技術快速進展，正逐步改變網路攻防的速度、規模與成本。具備高度程式分析、漏洞辨識及工具運用能力的先進AI模型，使威脅行為者可更快速發現漏洞、產生攻擊程式，並串接複雜的攻擊步驟，使漏洞從發現、揭露到遭濫用的時間持續縮短。面對此一變化，政府資安防護不能僅以既有作業速度因應，而必須做到更早掌握曝險、更快辨識威脅、更快完成處置，並在攻擊發生時確保政府及關鍵基礎設施核心功能持續運作。

我國已建立涵蓋資通安全管理、資安事件通報應變及跨機關聯防的整體防護體系，是因應先進AI資安風險的重要基礎。然而，面對快速變化的威脅情勢，仍有三項挑戰必須優先因應：第一，漏洞發現到濫用漏洞發動攻擊的速度持續加快，使既有漏洞研判、排序、修補及應變機制必須進一步提升風險判斷與處置效率；第二，政府及重要產業高度仰賴資通訊產品、委外服務及第三方元件，供應鏈共通弱點一旦遭利用，影響可能迅速擴及多個機關與產業；第三，先進AI能力與重要資安情資多掌握於國外業者，其取得可能受技術、商業條件及國際情勢影響，因此我國必須兼顧國際合作與自主能力建構。

因此，政府將以「加速防禦、提升資通訊產品安全、強化國家資安韌性」為政策主軸，在既有資安治理及聯防體系基礎上，依風險急迫程度、制度整備及技術發展情形，分短期、中期及長期推動因應策略，並隨先進AI能力及威脅情勢持續滾動調整。

貳、建立跨部會、公私協力的推動機制

為整合相關部會專業與資源，並及時因應先進AI帶來的新興資安風險，數位發展部成立「先進AI資安風險因應小組」，結合相關部會及關鍵基礎設施領域主管機關，持續掌握新興AI技術與資安威脅發展，研議防護策略，協調政策方向及資源投入。政府將深化與關鍵基礎設施提供者、資通訊及資安產業、研究機構之合作，透過公私協力及產官學研合作，提升我國整體防禦能力。

參、建立階段性戰略防護對策

一、短期策略：加速防禦，降低當前曝險

面對AI加速漏洞發現及發動攻擊的風險，短期將以提升防禦速度為重點，優先調整既有機制並導入可即時運用的防禦工具，縮短漏洞發現、影響研判至完成處置的時間。

（一）建立風險導向的漏洞管理機制

由於漏洞數量與修補壓力同時增加，為使機關能在有限時間內優先降低主要風險，政府將發布漏洞管理指引，建立依漏洞風險、系統重要性及實際曝險程度，決定漏洞處置優先順序與期限的管理機制。

（二）運用 AI 加速資安防禦

運用 AI 模型開發弱點掃描工具，協助重要機關及關鍵基礎設施提供者檢測重要系統資安漏洞，續由受測單位儘早評估漏洞修補時限或採行補償防護措施。同時，強化情資分享及漏洞通報機制，導入 AI 輔助情資分析與特徵比對，加速掌握漏洞影響範圍，以及縮短通報及修補時間。

（三）強化網路曝險管理

防禦除加速漏洞修補外，也須主動減少可能遭受攻擊的入口。政府將強化網路曝險管理，並依機關風險及系統環境，協助機關強化防護措施，降低攻擊者入侵及橫向移動風險。

二、中期策略：提升資通訊產品與供應鏈安全

隨著先進AI降低發現及濫用漏洞的門檻，政府資安治理不僅著眼於機關內部系統。中期應將治理範圍延伸至產品與供應鏈，從政府採購、產品安全及供應商管理等面向，逐步落實安全設計理念。

（一）強化政府採購與產品安全

共同供應契約產品係整合政府機關共通需求品項，單一產品漏洞可能形成跨機關共同風險。政府將落實安全設計原則，檢討產品上架及資安管理機制，優先針對軟體產品進行自動化漏洞掃描，並要求廠商於一定期限內完成修補，降低漏洞擴散至多個機關之風險。

（二）提升供應鏈資安防護

政府持續推動企業加入台灣電腦網路危機處理暨協調中心（TWCERT/CC），協助其即時掌握資安警訊。為確保委外廠商及第三方元件，將推動建立軟體物料清單（SBOM），辦理委外廠商聯合稽核，並輔導廠商建立產品資安事件應變小組（PSIRT）機制，以強化產品漏洞與資安事件的應變及處理能力。

三、長期策略：深化國際合作，建立自主 AI 資安防禦能力

先進 AI 模型與漏洞研究需要高度技術、算力、資料及人才投入。面對快速演進的全球 AI 技術，我國必須同時「深化國際合作」與「建立自主能力」。國際合作讓臺灣持續接軌全球最先進的模型、技術與威脅情資；自主能力則確保在外部供應條件改變時，我國仍具有維持關鍵資安防禦的能力。

（一）深化國際資安合作與情資交流

政府將持續深化與國際夥伴的資安合作，結合政府、研究機構與民間業者之力量，建立多元交流管道，爭取使用國際先進 AI 模型，並強化重大漏洞與新興威脅情資分享機制。政府將持續接軌全球頂尖先進 AI 生態，即時掌握威脅情資，及結合國際夥伴之先進資安技術，以協助進行弱點掃描與漏洞分析，藉由精準部署防衛，全面提升國家資安防護能力。

（二）發展臺灣自主 AI 驅動的資安防禦能力

持續發展自主能力，是鞏固國家核心安全之重要基礎。政府將透過產官學研跨界協作，積極打造具備「主權 AI」精神的資安防護體系，發展自主資安 AI 所需的模型、資料、工具、驗證環境及專業人才，建構符合我國政府機關、關鍵基礎設施及重要產業實際需求的 AI 驅動資安防禦技術與系統，落實資安主權，確保國家關鍵防禦能力具備高度的自主性、可控性與韌性。

肆、結語：以更快的防禦、更強的韌性，因應先進 AI 時代

先進 AI 的能力與應用仍將持續演進，其對網路攻防的實際影響也可能隨模型、工具及使用方式而改變。面對快速變動且具有不確定性的風險，政策重點在於建立能夠持續掌握風險、調整防護並迅速應處的制度與能力。

本政策係政府因應現階段風險情勢與能力需求所建立之框架。政府將透過「先進 AI 資安風險因應小組」，持續結合各部會、關鍵基礎設施提供者、產業及研究能量，掌握技術能力、威脅情勢及國際政策發展，協調相關工作與資源投入，並依風險變化、技術成熟度及執行成效，滾動調整各項推動措施，以利及早辨識風險、加速應處，提升我國面對先進 AI 資安風險的整體韌性。