強化全國網路安全：延續關鍵行動並修正第13694號與第14144號行政命令

根據美利堅合眾國憲法及法律，包含《國際緊急經濟權力法》（50 U.S.C. 1701 及其後條文）、《國家緊急狀態法》（50 U.S.C. 1601 及其後條文）、《1952年移民與國籍法》第212(f)條（8 U.S.C. 1182(f)）以及《美國法典》第3編第301條所賦予我作為總統的權力，茲命令如下：

第一節：對第14144號行政命令之修正

2025年1月16日發布之第14144號行政命令（「加強並促進國家網路安全創新」）經如下修正：

(a) 刪除第2條第(a)-(b)項，並將第(c)、(d)、(e)項重新標示為第(a)、(b)、(c)項；

(b) 刪除第2條第(e)項的第一句；

(c) 刪除第3條第(a)-(b)項，並將第(c)、(d)、(e)項重新標示為第(a)、(b)、(c)項；

(d) 自第3條第(c)項中刪除下述語句：「在第14028號行政命令中，我指示國防部長及國土安全部長建立程序，立即分享威脅資訊，以加強國防部與民間網路的集體防禦」；

(e) 自第3條第(c)(i)(A)項刪除「新型（novel）」一詞；

(f) 刪除第4條第(b)(iv)項；

(g) 刪除第4條第(d)(ii)-(iii)項；

(h) 刪除第5條，並將第6、7、8、9、10與11條分別重新標示為第5、6、7、8、9與10條；

(i) 自第8條第(c)項刪除下述語句：「涵蓋入侵偵測、安全啟動所使用的硬體信任根，以及安全修補程式的開發與部署領域」。

第二節：對第14144號行政命令之進一步修正

第14144號行政命令進一步修正如下：

(a) 刪除第1條，並改列如下內容：

「**第一條：政策。** 外國勢力與犯罪分子持續對美國及其公民發動網路攻擊行動。中華人民共和國對美國政府、私人部門與關鍵基礎設施網路構成最活躍且持續的網路威脅，其他如俄羅斯、伊朗、北韓及其他對手亦帶來重大風險，持續破壞美國的網路安全。此類行動破壞全國關鍵服務之提供，造成數十億美元損失，並危及美國人民的安全與隱私。為應對上述威脅，國家必須加強網路安全。我現下命令採取額外行動，加強國家網路防禦，重點包括保護我國數位基礎設施、強化關鍵數位領域之服務與能力，以及提升我們對主要威脅的應對能力。」

(b) 刪除第2條第(c)項，並改列如下：

「(c) 有關之行政部門與機構（以下簡稱『機構』）應採取以下行動：

(i) 商務部長應透過國家標準與技術研究院（NIST）院長，於2025年8月1日前，在國家網路安全卓越中心（NCCoE）與產業建立合作聯盟，制定依據NIST特刊800-218《安全軟體開發框架（SSDF）》之安全軟體開發、維護與運營指引，並納入產業意見作為參考。

(ii) 商務部長應透過NIST院長，於2025年9月2日前更新NIST特刊800-53《資訊系統與組織之安全與隱私控管》，提供修補與更新之安全部署指引。

(iii) 商務部長應透過NIST院長，並與相關機構首長協商，於2025年12月1日前發布SSDF之初步更新版本，內容應涵蓋安全與可靠之軟體開發與部署之實務、程序、控制機制與範例。該初步更新發布後120日內，應完成最終版本之發布。」

(c) 刪除第4條第(b)項原文，並改列為：

「有關機構應採取以下行動：」

(d) 刪除第4條第(f)項，並改列如下：

「(f) 具足夠規模與複雜度之量子電腦（即具密碼分析效力之量子電腦，CRQC）將可破解目前在美國與全球數位系統上所使用的大多數公開金鑰加密技術。2022年5月4日第10號國家安全備忘錄《促進美國在量子運算之領導地位並降低對脆弱密碼系統之風險》指示聯邦政府應為轉向不受CRQC威脅之加密演算法做準備。

(i) 國土安全部長應透過網路安全暨基礎設施安全局（CISA）局長，並與國安局局長協商，於2025年12月1日前公布並定期更新支援後量子密碼學（PQC）之產品類別清單。

(ii) 為推動PQC轉型，國安局局長（針對國家安全系統）與行政管理與預算局（OMB）局長（針對非國安系統）應於2025年12月1日前分別發布規定，要求各機構最遲於2030年1月2日前支援TLS 1.3或後續版本。」

(e) 刪除原第6條（現為第5條），並改列如下：

「**第五條：促進人工智慧之網路安全應用。** 人工智慧（AI）具有轉變網路防禦能力之潛力，可快速識別弱點、擴大威脅偵測規模並自動化防禦行動。

(a) 商務部長（透過NIST院長）、能源部長、國土安全部長（透過科學與技術次長）及國家科學基金會主任應於2025年11月1日前，盡可能讓網路防禦研究資料集對學術界可取得，並兼顧商業機密與國安。

(b) 國防部長、國土安全部長與國家情報總監應於2025年11月1日前，與白宮內部機構合作，包括科技政策辦公室、國家網路總監辦公室與OMB，將AI漏洞管理納入各自機構之作業程序及跨機構協調機制，包括事件追蹤、應變與通報，並分享AI系統的攻擊跡象。」

(f) 刪除第7條，並改列如下：

「**第七條：政策與實務之對齊。** 各機構之政策應調整資源與優先事項，以提升網路可視性與安全控制，降低網路風險。各機構應諮詢國家網路總監並採取以下行動：

(a) 自本命令發布起三年內，OMB局長應發布指引（如有需要，修正OMB通告A-130）以因應重大風險，並推動現代資訊架構與實務於聯邦資訊系統中應用。

(b) 自本命令發布起一年內，商務部長（透過NIST院長）、國土安全部長（透過CISA局長）及OMB局長應共同建立一項試點計畫，以機器可讀格式推動規則即代碼之政策與指引。

(c) 自本命令發布起一年內，FAR理事會中之各機構成員應根據適用法律，採取行動修訂FAR，要求自2027年1月4日起，向聯邦政府提供消費型物聯網產品（依47 CFR 8.203(b)定義）之廠商，必須為其產品貼上「美國網路信任標章」。」

(g) 刪除第8條第(a)項，並改列如下：

「(a) 除第4條第(f)項另有規定外，本命令第1至第7條不適用於國家安全系統（NSS）資訊系統，或由國防部或情報界界定為具有重大破壞性影響之系統。」

第三節：對第13694號行政命令之修正

2015年4月1日發布之第13694號行政命令（「封鎖參與重大惡意網路行為人之財產」），經2016年12月28日之第13757號行政命令、2021年1月19日之第13984號行政命令，以及第14144號行政命令修訂後，再行修正如下：

(a) 刪除第1條第(a)(ii)項之「任何人（any person）」並改為「任何外國人（any foreign person）」；

(b) 刪除第1條第(a)(iii)項之「任何人（any person）」並改為「任何外國人（any foreign person）」。

第四節：一般條款

(a) 本命令不得解釋為限制或影響：

(i) 依法賦予任何行政部門、機構或其首長之權限；或
(ii) 行政管理與預算局局長對於預算、行政或立法提案之職責。

(b) 本命令之實施應符合現行法律，並依預算可用性執行。

(c) 本命令不擬創設，亦不應解釋為創設任何實體或程序上之權利或利益，任何人不得依此命令對美國、其部門、機構或人員主張可依法執行之權利。

(d) 本命令之公布費用由國土安全部承擔。

唐納．約翰．川普
白宮
2025年6月6日