僅供委員問政所需參考
不代表本院意見或立場

編號：3167

議題研析

一、題目：美國《強化國家因應先進密碼攻擊能力》行政命令簡介

二、議題所涉法規

資通安全管理法、政府採購法

三、背景說明（緣起）

量子技術發展攸關國家安全、產業洗牌與數位信任秩序，美國政府與國際科技巨擘已投入數十億美元搶佔量子晶片主導權，我國電子代工大廠與金融機構亦積極投入相關領域。然而，量子運算雖對產業帶來新機會，亦帶來強大的資安震撼彈，具破密能力的量子電腦將在 10 年內問世，象徵現行加密體系隨時面臨瓦解，「Q-Day[1]」威脅恐將使現行金融與通訊加密機制於數分鐘內被破解，因此，建構以後量子密碼（Post-Quantum Cryptography, PQC）為基礎之資安架構，為因應量子技術發展之重點[2]。

四、問題爭點

美國於 2026 年 6 月 22 日發布第 14412 號《強化國家因應先進密碼攻擊能力》行政命令（Securing the Nation Against Advanced Cryptographic Attacks[3]，下稱第 14412 號行政命令），著重於聯邦政

[1] Q-Day 為一個假設的時間點，指量子電腦得以破解現有加密演算法之時刻。

[2] 吳雅如，第 11 屆《WHATs NEXT》量子科技高峰會登場 聚焦商轉與後量子防禦，2026 年 7 月 29 日，工商時報，網址：https://www.ctee.com.tw/news/20260729701582-431202，最後瀏覽日期：2026 年 8 月 12 日。

[3] White House, Executive Order 14412, available at：https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/, last visited on Aug. 18, 2026.

府資訊系統與關鍵基礎設施之後量子密碼遷移[4]，茲簡介該行政命令重點，以供我國法制參考。

五、探討研析

（一）明確相關事務監督協調機關

依第 14412 號行政命令第 3 點（section 3），該命令所規定之國家後量子密碼遷移（migration）政策與策略，由預算管理局（Office of Management and Budget, OMB）局長與國家網路總監（National Cyber Director）共同領導、協調及監督；至於各機構導入後量子密碼之最佳實踐與風險管理策略等技術指引，則由商務部長（Secretary of Commerce）與國土安全部長（Secretary of Homeland Security）分別透過國家標準暨技術研究院（National Institute of Standards and Technology, NIST）及網路安全暨基礎設施安全局（Cybersecurity and Infrastructure Security Agency, CISA）負責提供。

（二）明定各機構[5]應辦理事項及時程

為促使各機構落實辦理後量子密碼遷移工作，第 14412 號行政命令第 4 點（section 4）明定相關應辦事項之時程，包括：

1、自命令下達之日起 30 天，各機構應指派並提報主責後量子密碼遷移之人員；

2、自命令下達之日起 90 天，預算管理局應發布技術指引，內容包

[4] 呂沛柔，美國白宮發布兩則行政命令，旨為強化美國於量子資訊科學與技術之技術優勢，並推動關鍵技術部署與商業化，以因應相關威脅，資策會科技法律研究所，2026 年 7 月，網址：https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&d=9514，最後瀏覽日期：2026 年 8 月 12 日。

[5] 依第 14412 號行政命令第 2 點（a），各機構（agency）之名詞定義係參照美國法典第 44 篇第 3502 條（44 U.S. Code § 3502(1)），係指任何行政部門、軍事部門、政府公司、政府控制之公司，或其他屬於政府行政分部（包括總統行政辦公室）之機構，或任何獨立監理機關，但不包括：政府問責辦公室；聯邦選舉委員會；華盛頓哥倫比亞特區政府、美國領地與屬地政府，及其各自之派駐/下屬單位；或政府所有且由承包商營運之設施，包括從事國防研究與生產活動之實驗室。

括引導各機構盤點高價值資產[6]與高影響系統[7]清冊、於 2030 年 12 月 31 日前將該資產及系統過渡至使用後量子密碼建立金鑰、於 2031 年 12 月 31 日前過渡至使用後量子密碼進行數位簽章，及擬定辦理上開事項之計畫等事宜；

3、自命令下達之日起 180 天，應針對國家標準暨技術研究院擁有或營運之資訊系統之適當子集（subset），啟動後量子密碼遷移試辦專案，該專案至遲應於 2027 年 12 月 31 日前完成。

（三）積極協助外界因應後量子密碼

為引領各界因應後量子密碼之衝擊，第 14412 號行政命令第 5 點（section 5）明定，依 2024 年 4 月 30 日第 22 號國家安全備忘錄《關鍵基礎設施安全與韌性》（Critical Infrastructure Security and Resilience）或其後續文件所定義，擔任部門風險管理機構（Sector Risk Management Agencies, SRMAs）之各機構，應協助關鍵基礎設施所有者及營運者擬定後量子密碼遷移計畫；命令下達後 180 天起，每年應向總統報告擁有或營運國家安全系統之機構的後量子密碼遷移進度；命令下達後 270 天應發布指引，說明加密資料清單[8]（Cryptographic Bill of Materials，簡稱 CBOM）應包含之要素。

（四）修正政府採購法納入後量子密碼相關要求

第 14412 號行政命令第 6 點（section 6）明定，聯邦採購法規委員會（Federal Acquisition Regulatory Council, FAR Council）應於命令下達之日起 180 天內，提出《聯邦採購法》（Federal Acquisition Regulation, FAR）修正草案，要求廠商於 2030 年 12 月 31 日前，須

[6] 依第 14412 號行政命令第 2 點（d），高價值資產係指依預算管理局（OMB）M-19-03《透過強化高價值資產計畫以加強聯邦機構之網路安全》（Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program）備忘錄或其後續文件，指定為高價值資產之聯邦資訊或聯邦資訊系統。

[7] 依第 14412 號行政命令第 2 點（c），高影響系統係指在該資訊系統中，至少有一個安全目標（即機密性、完整性或可用性），依聯邦資訊處理標準第 199 號（FIPS 199）評定為具有高潛在影響。

[8] 該清單係指完整盤點系統軟硬體所使用之加密技術，例如加密演算法、金鑰、憑證等。

遵守國家標準暨技術研究院發布之聯邦資訊處理標準（Federal Information Processing Standards, FIPS），並包含所有適用且納入後量子密碼演算法之聯邦資訊處理標準規範；270 天內提出《聯邦採購法》修正草案，調整《聯邦採購法》規範要件及契約條款，納入廠商弱點揭露計畫，確保相關廠商依國家標準暨技術研究院發布之指引落實弱點揭露政策（vulnerability disclosure policies, VDPs）。

（五）比較法之借鏡與建議

數位發展部於 2025 年 4 月發布由後量子資安產業聯盟與財團法人資訊工業策進會共同發行之「後量子密碼遷移指引」，協助資安產業因應後量子密碼[9]；2026 年 6 月金融監督管理委員會亦針對金融業發布「金融業後量子密碼遷移參考指引」[10]。協助產業因應相關衝擊固然重要，惟政府機關內部掌握龐大機密、敏感資料，關鍵基礎設施之相關資料庫亦包含大量機敏資訊，一旦遭竊取、破解，恐對國家安全造成重大影響，爰建議主管機關參考國際作法，研議後量子密碼遷移時程及政府採購契約範本或法規之修正，以降低後量子密碼衝擊。

撰稿人：陳育靖

[9] 數位發展部數位產業署，數產署攜手後量子資安產業聯盟發布「後量子密碼遷移指引」，協助產業提升資安保障、建構更安全的資安環境！2025 年 4 月 16 日，網址：https://moda.gov.tw/ADI/news/latest-news/16090，最後瀏覽日期：2026 年 8 月 18 日。

[10] 金融監督管理委員會，金管會發布「金融業後量子密碼遷移參考指引」 引導金融機構強化量子風險整備，2026 年 6 月 18 日，網址：https://www.fsc.gov.tw/ch/home.jsp?id=2&parentpath=0&mcustomize=news_view.jsp&dataserno=202606180001&dtable=News，最後瀏覽日期：2026 年 8 月 18 日。