國家關鍵基礎設施軟體供應鏈安全初探

◆ 國防大學兼任助理教授 — 張喻閔

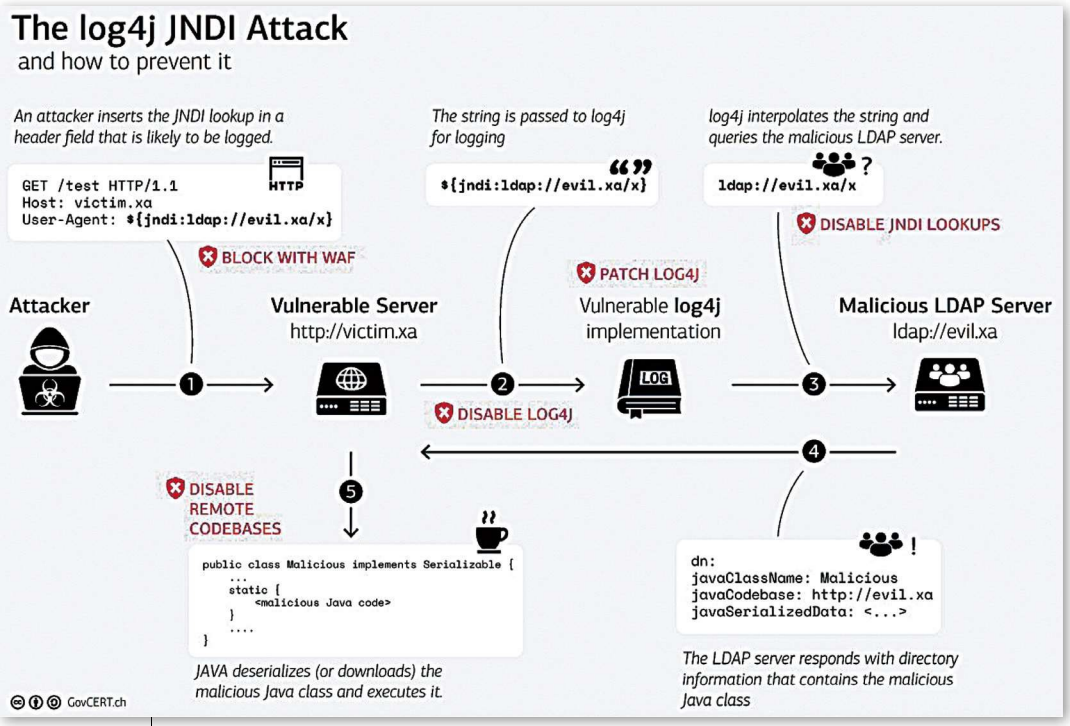
美國頒布 EO-14028 行政命令與推廣軟體物料清單（Software Bill of Materials, SBOM），藉此提高自身軟體供應鏈安全，進而協助國家關鍵基礎設施提升資安管理機制，其相關法制及政策值得我國借鏡與推廣。

關鍵設施軟體供應鏈安全日益重要

2020 年 SolarWinds 事件，駭客通過對雲端服務業者實施供應鏈攻擊，造成美國政府和工業部門機密資料重大外洩，2021 年 11 月 Log4j 漏洞（CVE-2021-44228）事件，造成美國金融業者至少 400 多萬客戶之重要金融資料被竊。[1] 2021 年 5 月，美國最大油管公司 Colonial Pipeline 遭勒索軟體攻擊，緊急關閉部分管道與 IT 系統，造成營運嚴重停擺。[2] 相關案例使各界重視軟體供應鏈安全，由於現今開源軟體大量應用，資訊專案軟體組成高度複雜，國家關鍵基礎設施之軟體安全，便格外受到矚目。

[1] 2021 年 12 月，廣泛出現於各應用程式的 Apache Log4j Java 有重大遠端執行漏洞，造成攻擊者能完全控制受影響系統。影響包括微軟 Minecraft、蘋果 iCloud、Steam 等大型網站，Tenable 稱其為 10 年來最嚴重之漏洞。

[2] 周峻佑，〈資安一周第 145 期：燃油供應商 Colonial Pipeline 遭勒索軟體攻擊，美國宣布進入緊急狀態〉，《iThome》，2021 年 5 月 11 日，https://www.ithome.com.tw/news/144342。



2021 年 11 月 Log4j 漏洞事件，造成美國金融業者至少 400 多萬客戶之重要金融資料被竊。（Photo Credit: GovCERT.CH, https://www.ncsc.gov.ie/emailsfrom/Reports/Log4j）

2021 年 5 月，美國最大油管公司 Colonial Pipeline 遭勒索軟體攻擊，造成營運嚴重停擺。（Photo Credit: Famartin, https://w.wiki/4qej）

美國政府重要政策

2021 年 5 月 12 日，美國總統拜登公布「改善國家網路安全的行政命令」（Executive Order on Improving the Nation's Cybersecurity, EO-14028），[3] 其中針對商業軟體開發因缺乏透明度、難以防止惡意行為者篡改等問題，實施更嚴格的安全維護機制。該命令要求美國網路安全及關鍵基礎設施安全署（Cybersecurity and Infrastructure Security Agency, CISA）等主管機關，應定期發布安全指引，增強軟體供應鏈之安全性。[4]

EO-14028 行政命令要求之重點 [5]

一、EO-14028 要求確保 IT 服務提供者能夠與聯邦政府分享資訊，尤其針對重大違規的資訊。

二、要求實施更嚴格網路安全標準，強化雲端服務保護和推展零信任架構，在特定時間內部署多因子驗證和加密措施。

三、要求銷售予政府軟體開發者應建立基本的軟體安全標準，包含開發人員應對其開發之軟體內容，保有更高的可見性（visibility），以及持續確保外界得以公開取得與其相關之軟體資訊。

[3] The White House, "Executive Order on Improving the Nation's Cybersecurity", May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.

[4] EO-14028 適用範圍為 FCEB 之聯邦部門（Federal Civilian Executive Branch），不包含國安、國防與情治單位。

[5] CISA, "Executive Order on Improving the Nation's Cybersecurity", https://www.cisa.gov/topics/cybersecurity-best-practices/executive-order-improving-nations-cybersecurity.

四、設立網路安全審查委員會，由政府和私部門負責人共同主持。委員會有權在重大網路事件發生後召開會議，分析原因並提出改善建議。

五、建立標準化手冊，確保所有聯邦機構符合一定的技術門檻，並採取一致性步驟來識別和減緩資安威脅。另強化聯邦政府內之端點偵測和回應（Endpoint Detection and Response, EDR）系統，並改善資訊分享機制以提升網路安全能力。

六、要求聯邦制訂網路安全事件日誌之規範，以提高有關入侵偵測、緩解駭侵行為以及認定資安事件程度的能力。

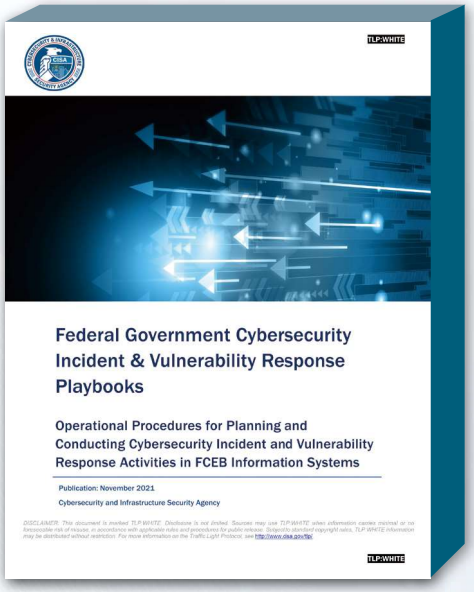
另為確保聯邦政府軟體供應鏈安全，EO-14028 要求採取下列措施：[6]

一、聯邦政府應推廣採用自動化工具或類似流程，來維護可信任之原始碼供應鏈，進而確保其完整性。

二、採用自動化工具或類似之流程來檢查已知與潛在漏洞並進行修復，該工具或流程應定期運作，或至少在產品、版本或更新發布前運作。

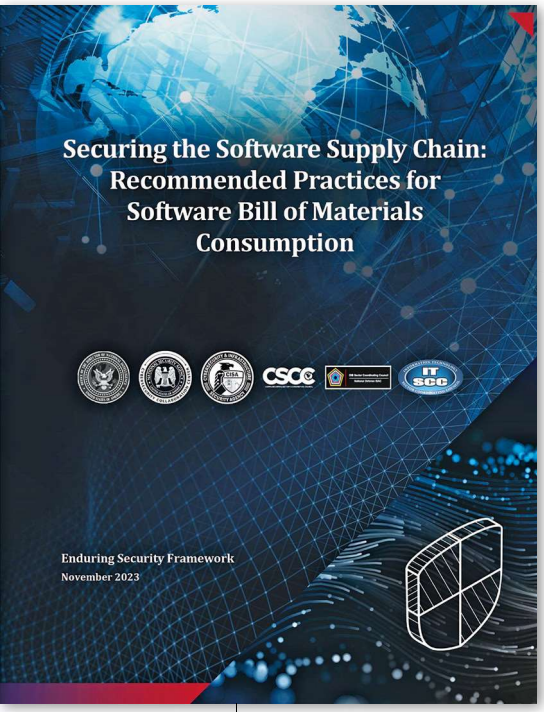
三、為促進開發商和供應商提供更安全的供應鏈，應採行於網站上發布等公開等方式，向購買者提供產品或資訊專案之「軟體物料清單」。

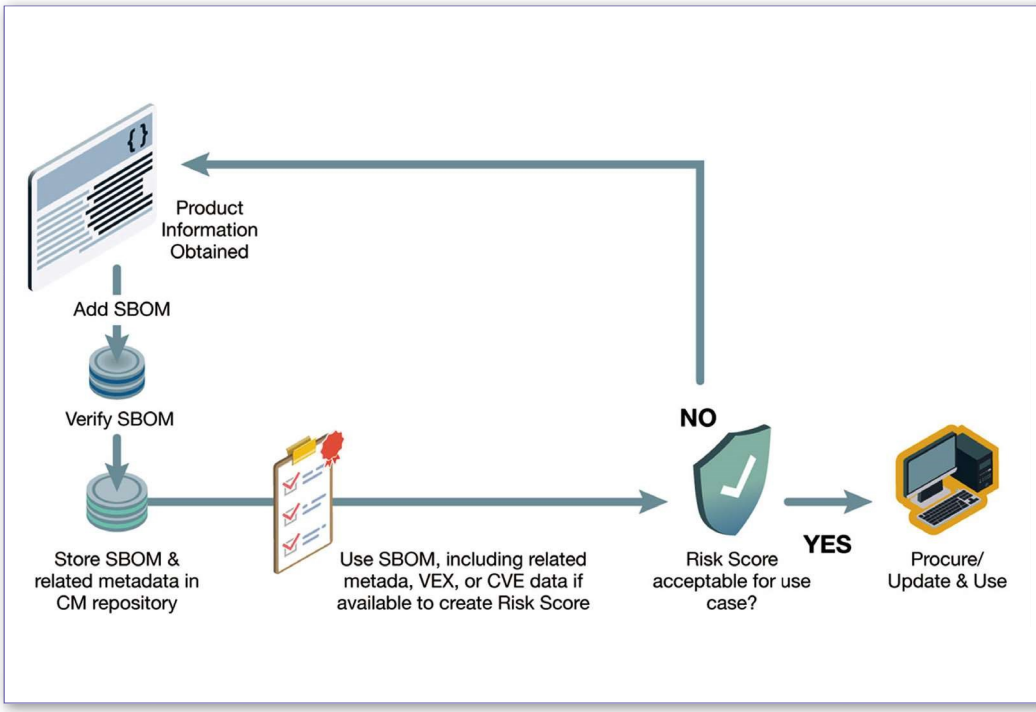
EO-14028 行政命令設立網路安全審查委員會，由政府和私部門負責人共同主持。（Photo Credit: Homeland Security twitter, https://twitter.com/DHSgov/status/1489254258897666055）



EO-14028 行政命令建立標準化手冊，確保聯邦機構符合一定的技術門檻，並採取一致性步驟來識別和減緩資安威脅。（Source: CISA, https://cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf）

[6] 參見EO-14028, Sec. 4. Enhancing Software Supply Chain Security, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity.





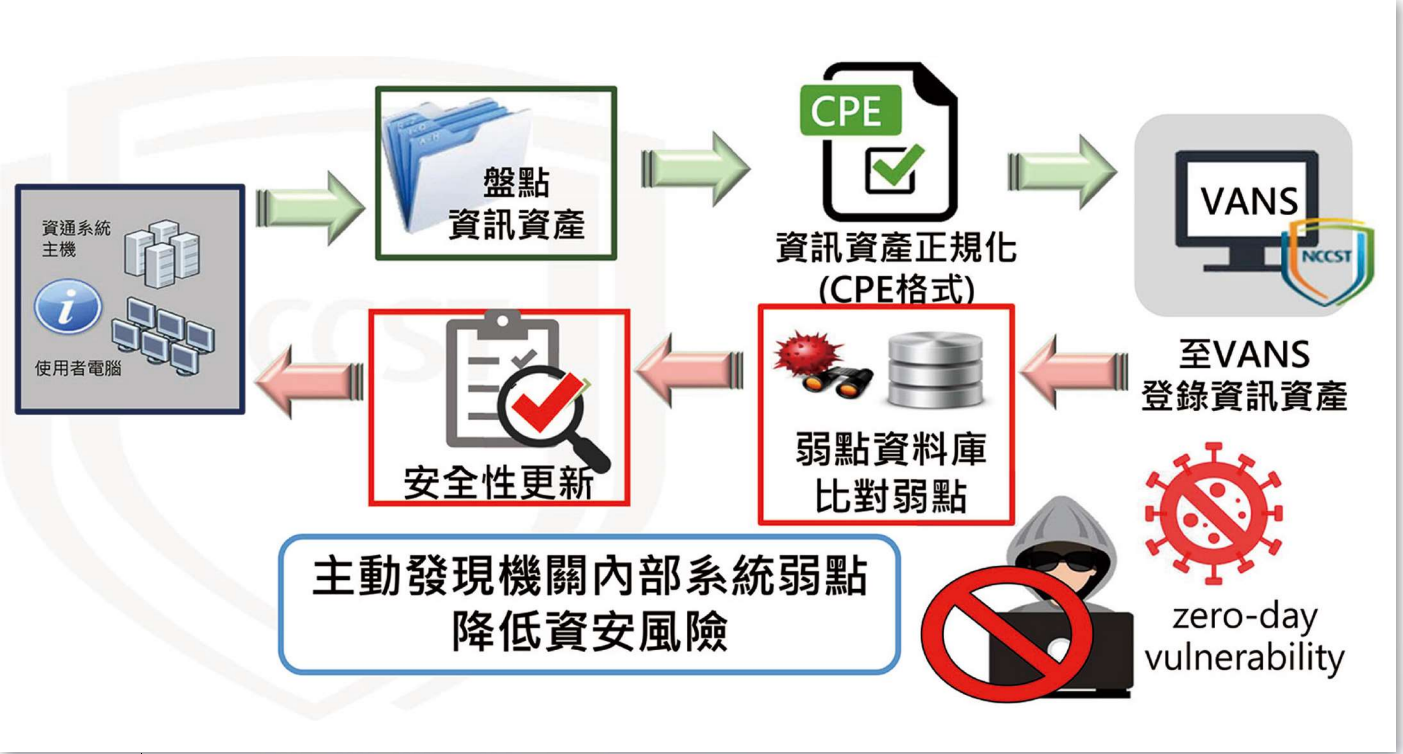
美國政府於 2023 年 11 月公布「保護軟體供應鏈：軟體物料清單的實踐建議」，協助使用者完成軟體之採購、測試、資安部署和軟體修補的建議流程，SBOM 具有即時更新組件內容與呈現完整資訊的效果，對降低攻擊風險有益。（Source: U.S. D.O.D, https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF）

軟體物料清單（SBOM）

軟體物料清單類似於軟體的「成分清單」，包含該軟體所有的基礎組件（component），都必須遵循既定的、機器可讀取的模式記錄，以標準化形式呈現其資訊。CISA、國家安全局（National Security Agency, NSA）和國家情報總監辦公室（Office of the Director of National Intelligence, ODNI）組成一個跨部門、公私合作的安全框架工作小組，並在 2023 年 11 月 9 日公布「保護軟體供應鏈：軟體物料清單的實踐建議」，以因應 EO-14028 對聯邦政府應提高軟體供應鏈安全性之要求，協助使用者完成軟體之採購、測試、資安部署和軟體修補的建議流程，並開發 SBOM 內容，以促進軟體資訊公開與漏洞即時修補。[7]

美國政府藉由 EO-14028 法案，對聯邦政府與企業界提高資安水準要求，並透過 SBOM 機制協助管理，讓使用者可對新出現的資安威脅快速反應，無須被動等待軟體商通知。另因 SBOM 具有即時更新軟體組件內容與呈現完整資訊的效果，對於降低零日漏洞攻擊風險，以及確保軟體符合智慧財產權規範等皆有助益，因此成為現今軟體安全和供應鏈風險管理的關鍵因素。

[7] CISA, "CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain", November, 9, 2023, https://www.cisa.gov/news-events/alerts/2023/11/09/cisa-nsa-and-partners-release-new-guidance-securing-software-supply-chain.



由國家資通安全研究院管理之「資通安全弱點通報系統」可供機關登錄資訊資產、自動比對弱點資料庫，以協助機關確認其資訊資產是否存在公開漏洞。（資料來源：國家資通安全研究院，https://download.nics.nat.gov.tw/UploadFile/vans/ 資通安全弱點通報機制推廣說明 v1.0_1100609.pdf）

我國相關法制措施

我國近年依《資通安全管理法》及施行細則，要求政府與企業依循「事前規劃」、「事中維運」及「事後改善」等階段，落實安全維護計畫、改善資安缺失，並制度化鼓勵情資分享與公私合作；另公告「各機關對危害國家資通安全產品限制使用原則」、「政府資訊服務委外管理規定」、「政府資訊服務採購作業指引」等規定，試圖從法規面降低軟體供應鏈可能之資安風險。此外，由「國家資通安全研究院」管理之「資通安全弱點通報系統」（Vulnerability Analysis and Notice Service, VANS），可供機關登錄資訊資產、自動比對弱點資料庫，以協助機關確認其資訊資產是否存在公開漏洞。該系統預計擴充納入 SBOM 比對功能，未來將可供機關登錄並進行弱點比對及通報，由制度面強化資訊資產之風險管理。

結語

提高國家關鍵基礎設施軟體供應鏈之安全性，已是刻不容緩的任務。期待未來借鏡美國有關法規與政策，持續推動我國 SBOM 系統並健全國家關鍵基礎設施之資安管理機制。

本文摘自清流雙月刊中華民國113年5月號P.46-P.50