以美國國防部與 CMMC 為例

美國聯邦政府供應鏈資安管理

美國聯邦政府（USG）對於常見供應商威脅已經發展出供應鏈資安風險管理（C-SCRM）。在供應鏈韌性這必要前提下，企業宜預先完成合規準備並完善資安治理制度，避免因資安的落差所造成的供應鏈排擠，而喪失商業機會。

文／梁日誠

近年來，供應鏈一直被美國聯邦政府（USG）視為國家安全的重要一環，供應鏈風險管理（Supply Chain Risk Management, SCRM. Committee on National Security Systems Directive No. 505）也於 USG 各部門間持續的運作，以有效降低供應鏈風險對關鍵生產能力與關鍵物料、產品及服務的可用性和完整性的衝擊，亦即建立供應鏈韌性（Resilience）。在常見的供應商威脅中，如：偽造（Counterfeit）、可靠性失效（Reliability Failure）、惡意滲入（Malicious Insertion）、品質異常（Quality Escape）、篡改（Tamper）、新興威脅（Emerging Threats）等，資通安全（Cybersecurity，資安）也成為必要的防護領域，發展出供應鏈資安風險管理（Cybersecurity Supply Chain Risk Management，C-SCRM），以健全整體供應鏈資安管理作業。

美國聯邦政府供應鏈資安的發展

USG 於2021年2月頒布 14017 號總統令（Executive Order，EO），主題為「美國的供應鏈（America’s Supply Chains）」，在 EO 14017 中指示商務部、能源部、國防部、衛生及公共服務部於 100 天內，就其個別主責的產品：半導體製造與先進封裝、高容量電池、關鍵礦物與戰略性物資、藥物與活性藥物成分的供應鏈進行風險識別並提出

USG 部門	EO 14017 產出
100-Day Supply Chain Review	
商務部、能源部、國防部、衛生及公共服務部	Building Resilient Supply Chains, Revitalizing American Manufacturing, And Fostering Broad-Based Growth
One Year Sectoral Supply Chain Assessments	
國防部	Securing Defense-Critical Supply Chains
衛生及公共服務部	Public Health Supply Chain and Industrial Base
商務部與國土安全部	Assessment Of the Critical Supply Chains Supporting the U.S. Information And Communications Technology Industry
能源部	America’s Strategy to Secure the Supply Chain for a Robust Clean Energy Transition
運輸部	Supply Chain Assessment of the Transportation Industrial Base: Freight and Logistics
農業部	USDA Agri-Food Supply Chain Assessment: Program and Policy Options for Strengthening Resilience

表 A

建議作為;於一年內，國防部、衛生及公共服務部、商務部與國土安全部、能源部、運輸部、農業部就其領域內的主責項目提出供應鏈評鑑報告，如**表 A**，可以了解 USG 的核心關注議題。

國防部（DoD）提出的供應鏈評鑑報告的主要範圍為依 EO 14017 所指示的國防工業基礎（Defense Industrial Base，DIB），並列舉了勞動力（Workforce）、資安態勢（Cyber Posture）、製造（Manufacturing）、小型企業（Small Business）四個戰略賦能者（Strategic Enablers）以建立整體的供應鏈韌性。針對資安態勢，DoD 的建議如**表 B**。

DoD 持續推動供應鏈政策（如**表 C**），並納入資安控管，如：DODI 5000.90 政策（2020年12月），陳述於 SCRM 中包含 Cyber-SCRM（對應標準 SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and

行動群組 (Actionable roupings)	建議 (Recommendations)
Internal (DoD organizations)	CP1.1: Expand resources for cybersecurity
	CP1.2: Develop C-SCRM best practices to support implementation of DoDI 5000.90
	CP1.3: Enhance the conduct of C-SCRM
	CP1.4: Enhance the quality of Cyber Threat Intelligence
	CP1.5: Expand cybersecurity information sharing
	CP1.6: Ensure the use of mature cybersecurity practices
	CP1.7: Enhance cybersecurity of critical companies
Interagency (Other agencies)	CP2.1: Facilitate cyber threat sharing and coordination on defending mission critical cyber terrain
International (International allies)	CP3.1: Develop international cybersecurity approaches
Industry (Industry partners)	CP4.1: Enhance DIB cybersecurity information management

表 B

政策名稱	主旨
DODI 4140.01	DOD Supply Chain Materiel Management Policy establishes policy and assigns responsibilities for management of materiel across the DOD supply chain
DODM 4140.01	DOD Supply Chain Materiel Management Procedures implements policy, assigns responsibilities, and provides procedures for those who work within or with the DOD supply system
DODI 4140.67	DOD Counterfeit Prevention Policy establishes policy and assigns responsibilities necessary to prevent the introduction of counterfeit materiel at any level of the DOD supply chain
DODI 5000.90	Cybersecurity for Acquisition Decision Authorities and Program Managers establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers in the DOD acquisition processes
DODI 5200.44	Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, known as TSN, establishes policy and procedures for managing supply chain risk
DODI O-5240.24	CI Activities Supporting Research, Development, and Acquisition establishes policy and assigns responsibilities for conducting and reporting Counterintelligence Functional Services, or CIFS, activities

表 C

Organizations），並將至少以包含已經取得 CMMC 驗證等級的考量，來評鑑潛在的供應鏈廠商。於2020年1月，DoD 公布了 Cybersecurity Maturity Model Certification（CMMC）1.0 版，並於2021年11月轉換為 2.0 版。

接續的，USG 在2021年5月的 EO 14028「改善國家資通安全（Improving the Nation's Cybersecurity）」總統令中，要求增強軟體供應鏈安全（Enhancing Software Supply Chain Security），持續地完善供應鏈資安管理的面象，直到2023年5月之前的軟體供應鏈安全相關規範與標準綜整如**表 D**。

USG 在數位轉型的過程中廣泛地使用雲端服務，也使得雲端服務供應商或使用雲端服務的供應商成為供應鏈資安管理的一環，美國總統於2022年底簽署了 FY23（2023 財務年度）的 NDAA

發布單位	規範與標準名稱
Office Of Management and Budget	M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices
National Institute of Standards and Technology (NIST)	SP 800-218 Secure Software Development Framework (SSDF)
National Institute of Standards and Technology (NIST)	Software Supply Chain Security Guidance
National Telecommunications and Information Administration (NTIA)	The Minimum Elements for a Software Bill of Materials (SBOM)
National Telecommunications and Information Administration (NTIA)	Framing Software Component Transparency: Establishing a Common Software Bill of Materials (SBOM)
Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)	Secure Software Development Attestation Form(Draft)

表 D

（National Defense Authorization Act 國防授權法案），於 NDAA 的 Section 5921，也將 FedRAMP（Federal Risk and Authorization Management Program）Authorization Act（FedRAMP Act）入法，對於涉及美國聯邦政府（包含美國國防部）供應鏈的雲端產業及其合規產生直接的影響。

美國聯邦政府供應鏈的建立及法源

USG 藉由採購（Acquisition）取得各項產品與服務以維持政府運作，也建立了龐大的美國與全球供應鏈，而此等供應鏈的基礎根植於聯邦採購法規與各聯邦部門對應的補充法規，以美國國防部 DoD 與其 CMMC 為例，可以窺見供應鏈與對應法源的相關性，對於有意進入美國聯邦政府供應鏈的廠商而言，投資合規的預防性成本將遠低於違規的罰款及/或協商款項，也同時避免了競爭對手可能引發的法律戰。DoD 的武器系統相關的全球供應鏈通稱為 Defense Industrial Base（DIB），一直以來，DIB 也是全球有心人士所覬覦的對象，DoD 累積了過往的經驗，在 DIB 供應鏈的資安防護思維上做了調整，將防護系統（System）的思維導向為防護資訊（Information），也因此，由保護機密性（Confidentiality，C）、完整性（Integrity，I）、可用性（Availability，A），轉為重點保護機密性（C）。

以 DoD 的 CMMC 領域為例，若以 USG 資通安全合規的相關法律（Laws，L）、法規（Regulations，R）、政策（Policies，P）來分析，L 包含了如：FISMA（Federal Information

Security Modernization Act）與總統令（EO）；R 包含了如：Chapter 1 Title 48 Code of Federal Regulations（CFR）（亦即 Federal Acquisition Regulation, FAR）的 Clause 52.204-21（簡稱 FAR 52）與相關的 Defense Federal Acquisition Regulation Supplement（DFARS）；P 包含了如：資通安全主責機關（如：National Archives and Records Administration，NARA）所頒布的泛政府（Government wide）政策與相關標準，USG 與 DIB 供應商間因合約而發生的資訊流中，包含了可公開與不可公開兩類，不可公開的資訊包含「機密性資訊（Classified Information）」、「聯邦合約資訊（Federal Contract Information, FCI）」與「受控非機密性資訊（Controlled Unclassified Information, CUI）」等，CMMC 的防護標的包含了 FCI 與 CUI 資訊（不含機密性資訊）。

資訊類別 / 法規層級	機密資訊 Classified nformation	聯邦合約資訊 FCI	受控非機密資訊 CUI
法律 (L) Laws	FISMA EO13526	FISMA	FISMA EO 13556
法規 (R) Regulations	FAR Subpart 4.4 32 CFR Part 117	FAR 52	FAR CUI Rule* 32 CFR Part 2002 DFARS 252.204-7012 DFARS 252.204-7019 DFARS 252.204-7020
政策 (P) Policies	DoDM5200.01		CUI Notices: ✓ NIST SP800-171/2 ✓ NIST SP800-171A DoDI 5200.48 CMMC*

表 E（*：FAR CUI Rule and CMMC are under Rulemaking process）

USG 的供應鏈廠商均有機會涉及機密資訊（Classified Information）、FCI 與 CUI 等受 L、R、P 所規範（綜整如**表 E**）保護的資訊，廠商在取得合約前即應合規，並展現相關證明文件，在美國 The Christian Doctrine 與 False Claims Act 的大傘覆蓋下，相關的司法判例（如：Case No. 2:15-cv-02245-WBS-AC）中的罰款與協商款項已提供前車之鑑。以 CMMC 為例，CMMC 2.0 已經正式公告，目前正處於法制化（Rulemaking）階段，將於法制化完成後施行，屆時未取得相應 CMMC 層級評鑑完成/通過的廠家將失去取得合約的機會，然將來適用於 CMMC 的供應鏈廠商目前已經受到 L/R/P 的法遵要求，CMMC 如同一個確認（Validation）機制，透過外部（如：第三方）評鑑來確保合規的真實性，現在的法遵要求與將來的 CMMC 要求，同時適用於 DIB 中的廠商。CMMC 是 DoD 基於過去數十年來的經驗所付出的代價（包含智財權與領先優勢），將過往以自評（Self Assessment）或自我具結（Self Attestation）為主的法遵機制，轉向為第三方獨立評鑑，以消弭供應鏈資安防護的實際落差。

CMMC 架構與法遵

DoD 的 CMMC Program 與現有的 FAR 與 DFARS 兼容，同時提供對 DIB 供應鏈 FAR/DFARS 合規的確認機制，現行 DFARS 的法遵評鑑依 DFARS 252.204-7019/7020，分為 Basic（自評）、Medium（政府評鑑-文件審查）、High（政府評鑑-現場審查）三級，目前 DoD 偕同 Cyber AB 正推動聯合評鑑（Joint Surveillance Voluntary Assessment Program, JSVAP），JSVAP 結合了 DFARS High Assessment 與 CMMC Level 2 評鑑，由國防部 DIBCAC 與 Cyber AB 認證的獨立第三方評鑑機構（C3PAO）的評鑑員共同進行評鑑活動。DFARS 相關的評鑑將產出 Summary Level Score（SLS），並須連同 CAGE Code（s）及 System Security Plan（SSP）上傳到 DoD 與 Supplier Performance Risk System（SPRS）系統中，SPRS 系統於 CMMC 法制化完成後，也將支援 CMMC 的評鑑結果，於近期公告的 DFARS 252.204-7024 中，陳述了 DoD 對於 SPRS 中對供應商風險與供應鏈風險評鑑的使用，DFARS/CMMC 的評鑑活動也正成為 SCRM 與 C-SCRM 的重要一環。CMMC 的三層架構與相關標準及法規的關聯性，展現於**表 F** 中。

與 CUI、DFARS、CMMC 息息相關的 NIST 標準為 NIST SP800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations（目前為 Rev 2），於2023年5月，NIST 公告了 NIST SP800-171 Rev 3 Initial Public Draft（IPD），其中之一值得關注的改變為 Rev 3 納入了 Supply Chain Risk Management（SCRM）成為17個安全要求成員（Security Requirements

CMMC 層級 / 關聯項目	Level 1	Level 2	Level 3
防護資訊類別	FCI	CUI	CUI
相關標準	CMMC Self-Assessment Guide Level 1	NIST SP800-171，CMMC Assessment Guide Level 2	NIST SP800-171，NIST SP800-172*
相關評鑑標準	CMMC Self-Assessment Guide Level 1	NIST SP800-171A，CMMC Assessment Guide Level 2	NIST SP800-171A，NIST SP800-172A*
資安實作 Practices	17	110	110+
相關法規	FAR 52	DFARS 252.204-7012/7019/7020	DFARS 252.204-7012/7019/7020
合規要求^	YES	YES	YES
CMMC 評鑑^	Self Assessment/ Affirmation (Annual)	Self or 3rd Party (Triennial)	Gov.-led (Triennial)
DFARS 評鑑	NO	Base and/or Medium/High	Base and/or Medium/High
JSVAP 評鑑	NO	YES	YES
雲合規要求	NA	FedRAMP Moderate Baseline Equivalent	FedRAMP Moderate Baseline Equivalent

表 F（*：Subset；^：Under Rulemaking）

Families）之一（Rev 2 為14個領域），包含了以下四項要求，顯示 USG 對其供應鏈（非聯邦組織）資安的殷切期望：

1. **Supply Chain Risk Management Plan**
2. **Acquisition Strategies, Tools, and Methods**
3. **Supply Chain Controls and Processes**
4. **Component Disposal**

對全球市場可能的影響

USG 對於供應鏈的廠商並不限於美國公司，也因此，USG 可預見的涉及供應鏈資安要求也將擴及全球供應鏈，例舉以下數項說明：

‖ 國際軍事合作頻仍

USG 在國際武器市場居於主導角色，不論是「直接商業銷售（Direct Commercial Sales）」、「外國軍事銷售（Foreign Military Sales）」、「國際合作計畫（International Cooperative Programs）」等，資安管制都有嚴格要求，DIB 全球供應鏈正是 DoD 管制的對象，也代表 CMMC 的推動將對全球 DIB 供應鏈的廠商帶來直接影響。

‖ FAR CUI Rule 的法制化

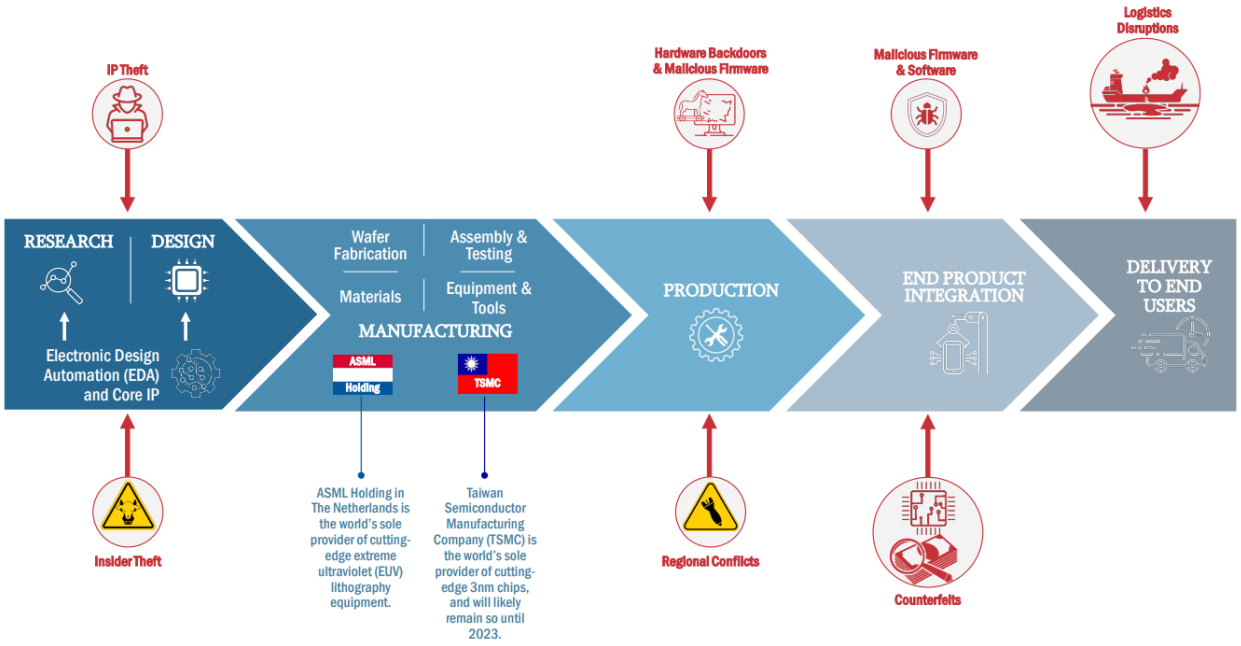
目前 USG 對於 CUI 的管制已有 32CFR Part 2002 法規，然尚未納入聯邦採購法規（FAR）中來要求供應鏈，DFARS 252.204-7012 法規僅適用於 DoD 中涉及 CDI/CTI/CUI 的供應鏈資安要求，CMMC 也僅適用於 DIB 產業，若 FAR CUI Rule 完成法制化，將適用於所有 USG 各部門供應商的資安要求，影響層面將較 CMMC 更廣。同時，國土安全部正將其採購法規「Homeland Security Acquisition Regulation（HSAR）Safeguarding of Controlled Unclassified Information（HSAR Case 2015-001）」法制化，其中的合規展現包含了 NIST SP800-171 標準與 CMMC 2.0。

‖ 軟體供應鏈資安要求法制化

於 EO 14028 中推動的軟體供應鏈資安要求，目前已進入法制化，國土安全部下的 CISA 爰因 Executive Order 14028 與 OMB M-22-18 文件，公告了 Secure Software Self-Attestation Common Form 的徵求意見程序，要求中納入了 NIST Secure Software Development Framework（SSDF, NIST SP 800-218）與 SBOM（Software Bill of Material）以及獨立評鑑方法，適用對象將涵蓋 USG 各部門的軟體相關供應商。若無進一步變更，M-22-18 原規劃 2023-06-12 將針對「關鍵軟體（Critical Software）」實施，2023-09-14 將針對所有其他軟體實施。值得留意的是，M-22-18 中所指的軟體，包含了：韌體（Firmware）、作業系統（Operating Systems）、應用（Applications）、應用服務（Application Services，如：雲端軟體 Cloud-based Software）與包含軟體的產品（Products Containing Software），如：目前，美國食品藥物管理局（Food and Drug Administration, FDA）正進行「Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions」法制化，其中亦包含 Software Bill of Materials（SBOM）。

‖ 對關鍵科技的保護

於2021年，美國政府 NCSC（National Counterintelligence and Security Center）將 Artificial Intelligence（AI）、Bioeconomy、Autonomous



圖一（資料來源：NCSC）

Systems、Quantum、Semiconductors 等，列為優先保護的關鍵科技，也陸續立法規範（如：美國晶片法）。於2022年，NCSC 針對半導體產業提出的供應鏈風險中，多項與資安有關，如圖一，台灣廠家也因其獨特性而列名其中。2023年5月，USG 公告了 UNITED STATES GOVERNMENT NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY，其中資安（Cybersecurity）與隱私（Privacy）被列為對新興科技研發及資料與思緒，可信任且自由流通的關鍵橫切（Cross-Cutting）議題，若有意涉入關鍵科技供應鏈的廠商，資安與隱私保護都將是入場券之一。

‖ 安全架構的全球化推動

USG 因 EO 14028 總統令，近年來於其部門間及偕同其他國家資安機構，在各領域推動安全架構，因為 USG 依賴第三方科技的程度越來越高，Zero Trust 政策對於全球供應商的產品與服務對 Zero Trust 的支援能力，也產生了連帶影響，對於供應商的信任機制也轉向為 Zero Trust，USG 推動 Zero Trust 的過程中，已公告了如**表 G** 的政策與指引文件。2023年4月，美國 CISA 偕同 NSA 與 FBI，和澳洲、加拿大、英國、德國、荷蘭、紐西蘭等國的資安機構共同發表「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default」，其中包含了 SSDF 與 SBOM；CISA、NSA 與 FBI 於2023年4月也與澳洲、加拿大、英國、紐西蘭等國的資安機構共同發表「Cybersecurity Best Practices for Smart Cities」，其中包含了 ICT 供應鏈與廠商的風險、主動式供應鏈風險管理等議題。

發布單位	政策與指引名稱
NIST	800-207 Zero Trust Architecture
OMB	M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
CISA	Zero Trust Maturity Model
CISA	Applying Zero Trust Principles to Enterprise Mobility
DoD	Zero Trust Reference Architecture
DoD	Zero Trust Strategy
DoD	Zero Trust Capability Execution Roadmap (COA 1)

表 G

結語

相對於 USG 對於供應鏈資安管理的重視，ISO&IEC 國際標準也具備相對應的供應鏈

Cybersecurity、Privacy 與韌性相關指引和要求，供參考及使用，如：IT 安全的 ISO 27036-2 供應商關係資通安全要求、OT 安全的 IEC 62443-2-4 IACS 服務供應商安全計畫要求、ISO 27701 隱私資訊管理系統附錄 B：PII 處理者（Processors）控制措施、ISO 22301 安全與韌性之營運持續管理系統、ISO 22318 供應鏈持續管理、ISO 28000 安全與韌性之安全管理系統要求等，廠商可建置並維運適當的管理系統或整合式管理系統（Integrated Management System，IMS），並將供應商資安的合規要求（如：資安法、個資法、CMMC、SSDF、GDPR 等）納入相關管理系統中持續的管理，以確保合規。

對於美國聯邦政府供應鏈資安的議題，廠商可就其所涉及的行業領域或關鍵科技，識別現有的合規要求，並關注發展中的合規趨勢，敏捷而落實地去應對並建立韌性（Resilience），自然而然就會於供應鏈中穩定成長，甚至脫穎而出；資安對於企業而言，既是風險也是機會，在供應鏈韌性這必要前提下，企業宜預先完成合規準備並完善資安治理制度，避免因資安的落差所造成的供應鏈排擠，而喪失商業機會。

作者梁日誠現為 CMMC PI/CCP/CCA Candidate/SME，ISO/IEC JTC1/SC27、SC42、ISO/TC22/SC32、IEC/TC65 技術組委員，ISO 27001/ISO 27701/ ISO 22301/ ISO20000-1/IEC 62443-2-1 主導稽核師及講師，TCIC 環奧國際驗證公司全球營運總經理。