美國新版 CMMC 2.0 最新發展

洪嘉齡

網路安全與決策推演研究所

壹、前言：CMMC 發展歷程

從 2013 年史諾登竊密事件之後，美國防部提高對委外廠商的安全管控，但近 10 年期間美國仍發生了多件重大網路攻擊事件，尤其是 2020 年底的 SolarWinds 供應鏈安全事件，這事件影響了美國幾大電信商、國防單位、軍火商、國務院、政府機關以及許多重要的軟體供應商，當時的川普政府也因此針對供應鏈安全擬定 CMMC 1.0 安全規範，並在 2020 年 11 月底正式公佈參考施行。經過一年的施行之後，美國防部發現要求國防工業承包廠商落實執行安全相關控制有一定的難度且耗費成本，且網路攻擊及商業竊密事件持續上演，因此在重新檢視 CMMC 的引用標準、實施步驟及輔導驗證等程序之後，2021 年 11 月美國防部資安長辦公室再次研擬 CMMC 2.0 草案，其管理、監督、驗證、輔導、教育等相關機構及生態系統都逐步規劃完善並成立，為的就是能落實執行 CMMC 制度，並以國家的力量來協助廠商做好資安、確保供應鏈安全，保護好美國的國家利益及智慧財產權。要注意的是，CMMC 制度迄今還是一個參考性規範，它並不是一個強制性的法律條文，因此美國防部打算在《聯邦法規》（Code of Federal Regulation，CFR）第 32 部分以及《聯邦法規》第 48 部分的《國防聯邦採購管制補充條例》（Defense Federal Acquisition Regulation Supplement，DFARS）中訂定規則，希望明確律定如何在美國防部採購合約中落實相關規範。依據官方之前說法應該是在今年（2023 年）的秋季會通過立法，於 2026 年全面採行該制度，可是按照目前最新的審議進度來看，CMMC 2.0 要能夠成為正式的法規至少要等到明年。圖 1 呈現 CMMC 的發展歷程。

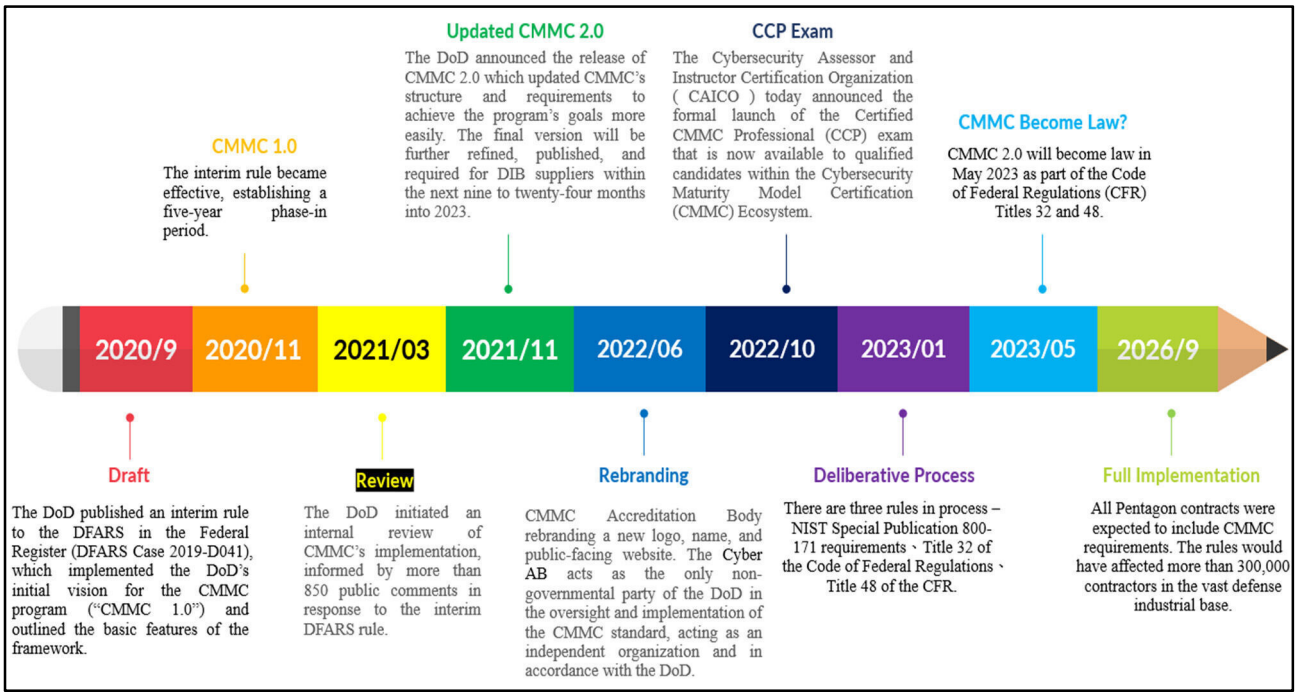

圖 1、CMMC 發展歷程

資料來源：作者洪嘉齡整理 CyberAB 資訊自行繪製。

貳、CMMC 生態系統

CMMC 規範的主導單位是美國國防部，所以除了資安長辦公室研訂整個管控程序外，內部也需要有採購契約要求（國防合約管理局，DCMA）及國防廠商管理（國防工業基礎網路安全評估中心，DIBCAC）相關單位協助，DIBCAC 也肩負對第三方驗證機構（C3PAOs）及最高控管等級的國防廠商定期實施稽核評估。整個 CMMC 制度的市場推動，國防部委託給 Cyber AB 機構來執行，Cyber AB 監管驗證機構（C3PAOs）、講師及輔導師訓練機構（CAICAO）、評估師（Independent Assessors），這些機構須定期接受 CyberAB 的稽核認證來確保組織及人員的專業性以及有效性。以下圖 2 揭露 CMMC 組織架構及生態系統。

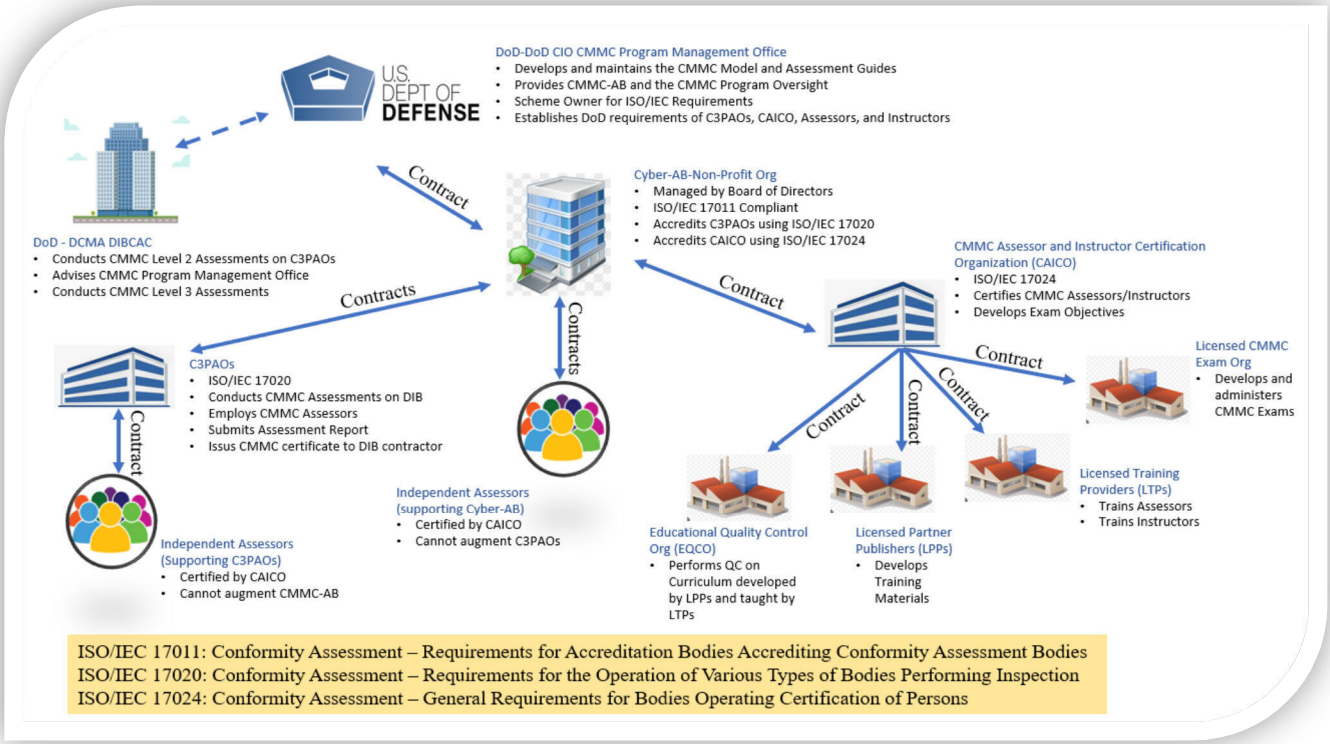

圖 2、CMMC 生態系統

資料來源：US DoD CIO CMMC Management Office 簡報資料。

參、CMMC 驗證模型

CMMC 驗證模型的演變，從網站蒐整其模型經歷了四次的調整。CMMC 1.0 正式發布於 2020 年 11 月 30 日，共分為五級驗證，每一個等級的控制項及驗證程序都相當繁複；2021 年 11 月 17 日則推出 CMMC 2.0，改為三級驗證，CMMC 2.0 版本驗證模型簡化成三個等級且精簡了控制項及驗證程序，其目的就是希望能夠協助廠商以更便捷、更省成本、更好的去落實 CMMC 控制項的要求；然後到了近期立法審議的時期，因為草案目前是處在對外公開討論及協商的過程，所以三個層級裡的控制項還有標準的引用都在動態的調整當中，因此美國防部資安長辦公室暫時將控制項的內容拿掉，相關討論及修改仍在繼續，因為關乎廠商利益及國家安全，因此立法時程才會拖長。2022 年 10 月 25 日起該三級不再刻意區別為基礎、進

階與專家等級，第一級管制可以採自我認證、第二級管制可以自檢兼採第三方認證、第三級管制則政府部門認證。[1]整個 CMMC 圍繞著國防採購合約制度，對於國防採購合約驗證等級的認定，係由美國國防部國防合約管理局釋出。對於「受控非具分類保密等級資訊」（Controlled Unclassified Information，CUI）的範圍認定，除了由國防供應鏈廠商界定純粹自己產出的資訊外，其餘多由採購合約甲方，亦即由國防合約管理局會同作需單位予以界定。[2]圖 3 顯示 CMMC 不同時期的驗證模型。

圖 3、CMMC 驗證模型

資料來源：作者洪嘉齡整理 USDoD CIO：
https://dodcio.defense.gov/CMMC/about/網頁資訊繪製。

[1] 參閱美國國防部武獲與維持次長室官方網頁對於 CMMC 的說明，https://www.acq.osd.mil/cmmc/about-us.html。

[2] Jim Goepel, "Are Contractors Authorized to Mark Legacy Information or Unmarked Information as CUI?," *CMMC Information Institute*, October 10, 2022, https://cmmcinfo.org/2022/10/10/are-contractors-authorized-to-mark-legacy-information-or-unmarked-information-as-cui/.

肆、CMMC 重要觀點

一、採購契約硬性規定

CMMC 的認證將成為美國國防部用來判定國防承包商合格與否的硬性二元標準，主承包商與分包商一體適用、個別審認，不同於以往只用來當作參考（成為採購作業中的廠商基本資格審查，而非需求建議或評選加分項目）。取得認證之廠商將優先取得國防訂單。若廠商自評造假或稽核不實，國防部將可以虛假申報法（False Claim Act）起訴個人和企業。

二、保護受控非具分類保密等級資訊

CMMC 最主要的保護對象是雖未被賦予分類保密等級、但仍須受控的 CUI，因為這些國防專案 CUI 資訊仍是國家間情蒐重點目標，並用以取代過去文件中常出現的「敏感但非具分類保密等級資訊」（Sensitive But Unclassified，SUB）或「限官方運用」（For Official Use Only，FOUO）等標註方式（對於未核密之採購案件相關專案資訊仍需層層保護控管）。

三、控管供應鏈的資訊流安全

CMMC 控管的是專案資訊流傳遞過程的供應鏈相關部門，這些上下游單位的人員安全查核與管控、環境的隔離與監控、資安的防護與稽核，都須嚴格管控（控管整個供應鏈的人安、物安、資安，而非僅主合約商及次包商的資安治理能力）。圖 4 展示 CMMC 資訊流的安控等級要求。

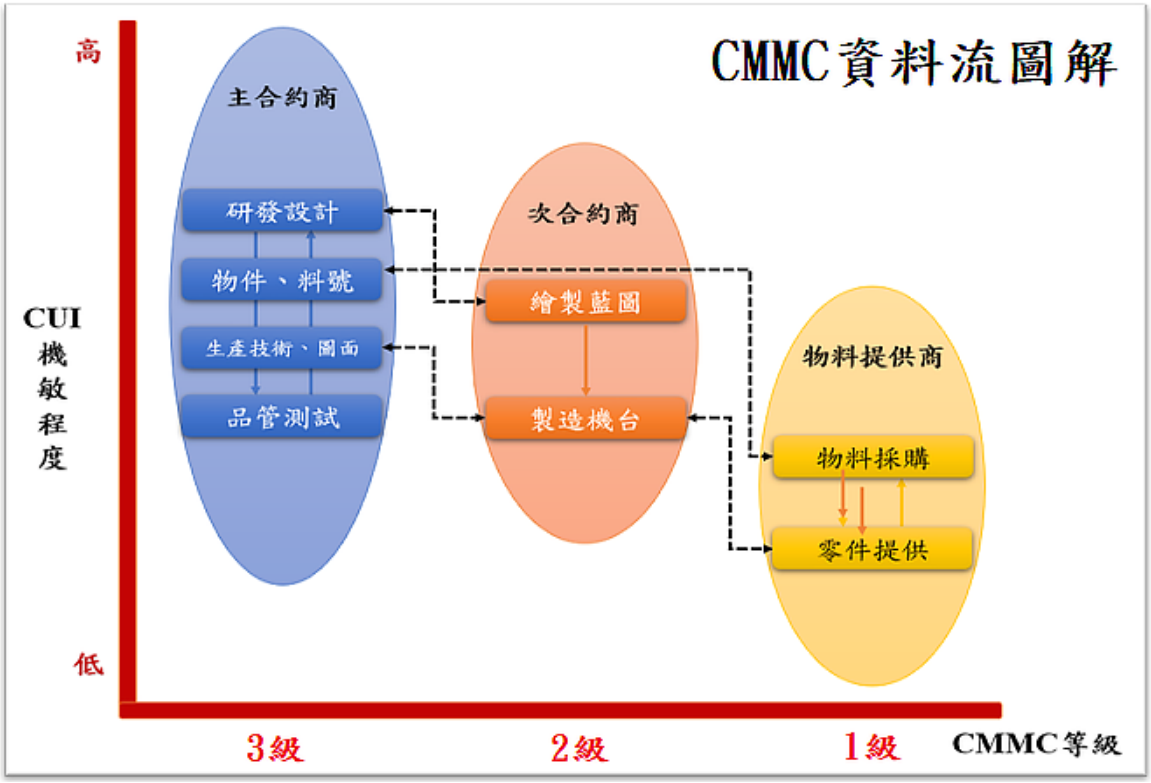

圖 4、CMMC 資訊流安控

資料來源：作者洪嘉齡自行繪製。

伍、CMMC 與 ISMS 差異性

有必要對CMMC與「資訊安全管理系統」（Information Security Management System，ISMS）做有系統的比較，以下比較兩者性質、適用對象、契約角色、防護重點、控制範圍。首先在性質上，CMMC 是以美國國防採購為核心，結合法規與資安標準的供應商認證機制；ISMS 則是資訊安全管理系統的國際標準。其次，在適用對象方面，CMMC 對象是美國國防供應鏈廠商；ISMS 則是廣泛適用任何組織、企業。在契約角色方面，CMMC 是要求競標前要先通過 CMMC 認證，沒有 CMMC 認證就沒有訂單；ISMS 則是企業取得 ISO 認證為佳，沒有亦可。在防護重點方面，CMMC 是保護採購專案的 FCI 與 CUI 確保供應鏈資料流安全；ISMS 則是針對特定組織、全體或特定範圍的資安管理活動，降低弱點風險，提升內部安全性及防護能力。在控制範圍方面，CMMC 要求資料傳遞所經之人員、

場所、設備及系統皆須管控、保護；ISMS 則僅針對認證範圍內之資安控制項目及企業資產。

陸、他國引進 CMMC 面臨問題

鑒於 CMMC 的等級及範圍認定，幾乎都是由國防採購專案業主決定，因此各國之國防部均扮演啟動、引入CMMC的角色。自 2020 年底推出後，美國友盟國家，包括北約國家以及諸如澳洲、日本及南韓等非北約盟國，紛紛加入 CMMC 行列，積極準備與美國國防產業網路安全認證規定對接。這些國家大多派員赴美受訓通過考試後，取得認證專業人員資格。在此必須指出的是，除非派訓國與美國另行協商簽訂協議，否則非美籍人士是無法取得合格評估師的訓練及授證的。這也意謂著，該國取得認證合格的專業人員、講師、專師回國後，按照授權可進行第一級管制認證，並協助第二級管制認證的諮詢輔導。但是若要成立第三方認證機構、或要對受第二級管制要求之廠商從事認證，則必須結合具美籍之合格評估師，再去要求 Cyber AB 檢核、授證與授權。

引進 CMMC 的美國友盟國家之中，以南韓徹底套製 CMMC 最為顯目，成為最佳範例。[3]除了與五角大廈達成協議，並且展現超強決心，按照自身體制，照搬對接美式體制。[4]如此的努力換來豐厚成果，南韓在烏俄戰爭後，得以成功對北約波蘭輸出具有美國軍工技術背景的軍武，[5]進一步擴大南韓國防產業規模，朝向成為全球前四大武器出口國大步邁進。[6]然而，即使有南韓這個成功範例，其他國家引進 CMMC 時，往往面臨以下問題。首先，關於 CMMC 法規及

[3] 曾怡碩，〈美國國防產業供應鏈網路安全認證〉，《國防安全雙周報》第 67 期，2022 年 11 月 18 日。

[4] 萬幼筠，〈CMMC 推動正殷，供應鏈資安需要明白什麼?〉，台灣資安大會「CMMC 國防產業安全供應鏈論壇」演講內容，2023 年 5 月 11 日。

[5] Soo-Hyang Choi, “Poland Buy S.Korean Rocket Launchers after Tank, Howitzer Sales,” *Reuters*, October 19, 2022, https://www.reuters.com/world/europe/poland-expected-buy-skorean-rocket-launchers-after-tank-howitzer-sales-2022-10-19/.

[6] 蔣巧薇，〈上任 100 天展雄心! 尹錫悅：希望韓國成為世界前 4 大國防出口國〉，《Newtalk》，2022 年 8 月 17 日，https://newtalk.tw/news/view/2022-08-17/803059。

標準的遵循，CMMC 制度涉及多個法律、行政命令、標準、指引的內容規範（CFR、DFARS、NIST SP800-171、 NIST SP800-172、False Claims Act），台灣中小企業不懂如何做資安，更不知道如何歸納綜整適用法規，以符合美國對供應鏈廠商的 CMMC 認驗證要求。

其次，面臨 CUI 由誰界定、分類分級、管控邊界的問題，專案資訊哪些屬於 CUI，是廠商自行認定還是由上一級承包商指定，CUI 控管範圍的大小、多寡都與投入成本息息相關。

第三、如何在國內取得 CMMC 的合規性輔導、認驗證及合格證書的問題，由於 CMMC 是美國國防部訂定的供應鏈資安規範，認驗證機構僅許設置在美國境內，想打入美國國防供應鏈的台灣廠商可否尋找國內資源輔導驗證，以最符合效益方式取得 CMMC 認證資格。

第四，國內的合規性輔導是否符合美國 Cyber AB 及 C3PAO 的發證要求（台美認驗證對接）的課題，台灣若推動在地化 CMMC 合規性輔導機制，其評估、審認、內稽、外稽的控制項目及認定標準是否與美方稽核驗證機構一致，以避免受驗廠商要花兩次工時及費用才能通過認證。

第五，中小企業合規成本負擔太重的挑戰，台灣中小企業資本額及規模不大，而資安是燒錢的投資且不會有實際的營利回饋，在取得 CMMC 認證過程猶如企業流程及系統再造，需耗費大量的人力及金錢，這對想打入美國國防供應鏈的台灣廠商是個難題待解。

最後，取得 CMMC 認證之優勢廠商，如何爭取美國國防合約或國際訂單的難題，對於已經取得 CMMC 認證之台灣廠商，政府部門或公協會如何運用法規及產品創造競爭優勢，協助這些台灣隱形冠軍企業爭取美國及世界各國的採購訂單，擴展國際拓銷。

柒、結語：台灣應思考方向

簡單來說美國 CMMC 這個制度在 2026 年全面推展之後，想要跟美國做生意的台灣廠商就必須取得認證，沒 CMMC 認證就沒採購訂單，面對這樣子一個如火如荼在推動的制度，台灣應提前研擬因應做法，一方面協助產業進行合規性評估、預算補助、在地化人才訓練及輔導驗證，另一方面藉由強化供應鏈安全來提升台灣的數位韌性、加深台美合作夥伴關係。

台灣落地推展 CMMC 則可以從以下三個層面來思考。首先，在組織架構方面，需釐清主責單位、協辦單位、生態系統（認驗證機構、輔導公司、訓練單位）。其次，在法規採納面向，包括供應鏈安全政策、採購法、檔案法、國防產業發展條例、國防採購契約等。最後，在推動策略方面，可考量選項包括自建對接、引進導入、台美合作、企業補助、示範性驗證等。

本文作者洪嘉齡為銘傳大學資管所碩士，現為財團法人國防安全研究院網路安全與決策推演研究所委任助理研究員。主要研究領域為：網路戰略、新興科技、網路安全、威脅趨勢、數位治理、資安／國安政策。

The Latest Development of CMMC 2.0

Chia-Ling, Hung

Division of Cyber Security and Decision-Making Simulation

Abstract

CMMC centers on defense contracts, and controlled unclassified information, or CUI, is scoped by defense contractor-generated information, with the rest co-defined by demand side agencies together with DIBCAC. From October 25, 2022, the three certification levels of the CMMCco have no longer been divided into Fundamental, Advanced and Expertise. Instead, Level 1 may be self-assessment, Level 2 may incorporate self-assessment with third-party certification, and Level 3 requires government certification.

Other countries often faced the following issues upon their adoption of CMMC: absence of guidelines for CMMC compliance, unclear scope of CUI, uncertainty as to where to go to enquire about domestic CMMC compliance consultation and certification, unaffordability of compliance cost for SME, compatibility of domestic compliance consultation with the issuance requirements imposed by the US Cyber AB and C3PAO, as well as how CMMC-certified enterprises make US defense contracts

To promote and implement CMMC in Taiwan, the following three dimensions require attention. First, the institutional framework needs to clarify primary responsible actor, faciliatory actors, and ecosystem, including certification party, consulting agency, and training agency. Secondly, the adoption of regulations shall cover supply chain security, acquisition, records and filing, defense industrial base development, as well as defense acquisition contracts. Finally, promotion strategies may take into consideration self-built compatibility, import and introduction,

enterprise subsidy, as well as best-practice certification.

Keywords: Supply Chain Cybersecurity Certification, CMMC, Defense Contract Management