美國推動國防供應鏈 CMMC 歷程暨近況

黃希儒

網路安全與決策推演研究所

壹、前言

美國政府為肆應全球戰略競爭情勢與威脅，強化國家與國防安全目標，並鞏固其科技關鍵能力優勢與經濟利益，近年針對國家整體國防工業基礎（Defense Industrial Base，DIB）供應鏈安全問題，傾聯邦政府行政、立法部門之全力，從總統公布國家網路（安全）策略、國會通過各項授權法案、明確權責分工、制定安全標準、檢討修訂法規，至國防部（Department of Defense，DoD）提出國防供應鏈「網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC）機制的全新運作架構與方案，並充分協調、輔導國防產業界配合政府政策按規劃步步到位的推動中。美國國防部建置 CMMC 機制的主要目標，係期望透過完備的國防供應鏈風險管控制度與齊一的資安規範基準，要求未來所有參與美國國防採購的主、次合約商，對聯邦法令及採購合約所定義必須進行保護的管制資訊，在廠商端的網路、資訊管理系統與程序，均須符合一定的安全標準，並取得相對應的安全級別認證；同時亦藉以建構聯邦政府與國防工業界，針對網路攻擊與威脅情資預警、分享、事件回報、技術支援及損害控管的完整資安聯防機制。

貳、美國推動 CMMC 的背景

美國國防供應鏈 CMMC 機制的發展，完全是一個由政府趨動（Government Driven）主導政策目標設定與規劃執行的歷程，事實上，在 SolarWinds 網攻事件[1]與全球戰略競爭情勢尚未造成美國聯邦

[1] "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," *Government Accountability Office*, April 22, 2021, https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic; 〈重大資安事件—美國國土安全部發布緊急指令，要求聯邦機構立即關閉被植入木馬的 SolarWinds 系統〉,《Art of Cyber

供應鏈安全重大警訊之前，前總統川普於 2018 年 9 月所簽署發布的美國史上第一份 15 年期（First fully articulated strategy in 15 years）「國家網路策略」（National Cyber Strategy），[2]已曾揭示「強化國家整體關鍵基礎設施及聯邦供應鏈安全」的指導方針；五年之後，在 CMMC 推動工作已如火如荼展開的 2023 年 3 月，總統拜登亦公布其「國家網路安全策略」（National Cybersecurity Strategy），更是進一步地，闡明聯邦整體供應鏈的網路安全政策目標與執行方針。[3]

全球知名資訊雲端公司 SolarWinds 於 2020 年被入侵，引發堪稱史上最嚴重的「全球性」網路攻擊事件，[4]造成包括美國各級聯邦政府、國際組織與上萬個企業機構，疑有大量機敏資料外洩情事，算是催化美國政府加速對國家整體供應鏈安全，尤其國防有關的戰略性高科技供應鏈，啟動一連串嚴密管控保護措施的重大事件節點。此外，2020 年 2 月，據報導，美國聯邦調查局（Federal Bureau of Investigations，FBI）及司法部（Department of Justice，DoJ）高階官員於華府一場研討會揭露，[5]中國政府近年來頻頻運用情報機構（intelligence services）、國營企業（state-owned enterprises）、私人公司（private companies）及學術研究（researchers and graduate students）等人員，廣泛地對美國各領域高科技相關資訊，進行大量

War》，2020 年 12 月 18 日，https://www.acw.org.tw/News/Detail.aspx?id=1164。

[2] "National Cyber Strategy of the United States of America," *The White House*, September 2018, https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; Terri Moon Cronk, "White House Releases First National Cyber Strategy in 15 Years," *DoD News*, September 18, 2018, https://www.jcs.mil/Media/News/News-Display/Article/1643010/white-house-releases-first-national-cyber-strategy-in-15-years/.

[3] "Biden-Harris Administration Announces National Cybersecurity Strategy," *The White House*, March 2, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; and https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

[4] "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," *Government Accountability Office*; 〈重大資安事件—美國國土安全部發布緊急指令，要求聯邦機構立即關閉被植入木馬的 SolarWinds 系統〉，《Art of Cyber War》。

[5] Catalin Cimpanu, "FBI is investigating more than 1,000 cases of Chinese theft of US technology," *ZDNet*, February 8, 2020, https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/; "China Initiative Conference," *CSIS*, February 6, 2020, https://www.youtube.com/watch?v=M1dtxt82HFE&ab_channel=CenterforStrategic%26International Studies.

竊取活動；依當時資料統計，尚有逾一千件個案由聯邦調查局進行調查中；另美國防部於 2021 年 1 月向國會（Congress）所提出的年度「國防工業能量報告」（Defense Industrial Capabilities Report to the Congress）亦特別將中國競爭野心視為對其國防工業發展進程的主要「干擾者」（major disruptor）。[6]

因此，上揭近年來有關全球供應鏈安全威脅情勢的變化，以及中國與美國國際安全戰略競爭的日漸成形，均促使美國政府意識到強化整體聯邦供應鏈安全管控的迫切性；而美國在面對上揭聯邦整體供應鏈安全問題，基於維護國防安全及軍事科技為優先的考量之下，國防部因而成為國會率先要求須制定完整管控機制與執行計畫的先導單位，以便後續作為全聯邦共同依循推動的標準典範。

參、對美國推動 CMMC 的觀察

一、保護對象的明確定義

美國聯邦政府依其現行國家機密保護相關法令，對於涉及「密（Confidential）」、「機密（Secret）」與「極機密（Top Secret）」等具有分類保密等級相關資訊（Classified information）的保護工作，從保密等級劃分賦予、安全基準訂定、涉密廠商實質查核，到異常狀況回報等面向，原本就有非常完備的法律基礎與嚴密的管控機制與措施。

因此，具體而言，美國政府現推動的 CMMC 機制最主要的保護標的，並非上揭原即已受到嚴格管控「具有分類保密等級」（classified）的資訊；而是雖未被賦予分類保密等級（unclassified），但依其他法令或基於政府政策，存管於非屬聯邦體系組織（nonfederal systems & organizations）惟仍須受到管控

[6] "The Department of Defense released the Fiscal Year 2020 Industrial Capabilities Report," *Office of Under Secretary of Defense for Acquisition & Sustainment, Department of Defense*, January 15, 2021, https://www.acq.osd.mil/news/office-news/indpol/2021/dod-releases-industrial-capabilities-report.html.

（identified as needing safeguarding）的相關資訊，此類資訊經美國總統發布 Executive Order 13556 執行命令，明確定義為「受控非具分類保密等級資訊（Controlled Unclassified Information，CUI），[7]用以取代政府部門過去慣用的「限官方運用（For Official Use Only，FOUO）」或「敏感但非具分類保密等級（Sensitive but Unclassified，SBU）」等資訊及文件標記方式（marking）；一般常見的 CUI 有：個人身份識別資訊（personally identifiable information，PII）、商業專屬權利資訊（proprietary business information，PBI）、非具分類保密等級技術資訊（unclassified technical information，UCTI），以及具法律強制執行的敏感資訊（law enforcement sensitive，LES）等。

其次，遂行 CMMC 機制的目標，既是為強化整體聯邦採購供應鏈的安全，保護對象當然須包括所謂的「聯邦合約資訊」（Federal Contract Information，FCI），此類資訊則明確定義於《聯邦採購規則》（Federal Acquisition Regulations，FAR, under Title 48 CFR）第 52.204-21 節，[8]即聯邦採購合約履行過程，原由政府提供予廠商或由廠商產出預計交付予政府（provided by or generated for the government under a contract），經考量不宜對外公開釋出的資訊；例如：研發需求與產品規格（R&D requirements and product specifications）、產品相關商業活動（Products or business activities）、財務資訊（Financial information）、往來客戶清單及行銷計畫（Client lists and marketing

[7] 美國政府針對「受控非具分類保密等級資訊」（CUI）的完整定義及管制規範，可參考以下系列的法規命令：總統 Executive Order 13556 行政命令（https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information）、國家檔案暨紀錄管理局（NARA ISOO National CUI Registry, https://www.archives.gov/cui）、聯邦法規（32 CFR Part 2002, https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2002）、國防部相關規定及手冊（DOD CUI Registry, https://www.dodcui.mil/Home/DoD-CUI-Registry/, DoDI 5200.48, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF and DoD Manual 5200.01, Volume 4, https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol4.pdf）等。

[8] 詳請參閱《聯邦採購規則（Federal Acquisition Regulation, FAR）》48 CFR 52.204-21 “Basic Safeguarding of Covered Contractor Information Systems,” *ACQUISITION.GOV, General Services Administration*, https://www.acquisition.gov/far/52.204-21

plans）及資訊管理系統與程序（MIS programs and processes）等。

二、政府主導的策略規劃與推動

除前揭美國總統公布的「國家網路策略」已確立聯邦供應鏈安全管控機制的政策指導之外，美國國會於 2020 及 2021 年間，亦密集透過一連串國防授權法案（National Defense Authorization Acts，NDAAs）的提案，[9]要求美國行政部門，尤其是國防部，須加快整體管控機制建立與實務推行的腳步，提案內容包括：於一定期限內向國會研提出完整機制運作架構報告、主動與國防產業供應鏈進行協調溝通並提供必要協助，以及同步建立 CMMC 實務運作機制的組織分工與完整能量等。而美國國防部則係責由「武獲暨維持次長辦公室」（Office of Under Secretary of Defense for Acquisition and Sustainment，OUSD/A&S）」及其所屬執行機構「國防合約管理局」（Defense Contract Management Agency，DCMA），協同國防部「資訊長」（Chief Information Officer，CIO）辦公室負責機制全般規劃與推動。

國防部受命後，隨即針對可支撐任務推動的法源《聯邦採購規則－國防增補規定》（Defense Federal Acquisition Regulation Supplement，DFARS）相關章節條文的適用情形進行審閱，其中 DFARS 第 252.204-7000 章「聯邦合約資訊揭露」（Disclosure of Information）第 252.204-7012 節，前於 2019 年 12 月曾經增補修訂有關「國防資訊保護暨網路事件回報」（Safeguarding Covered Defense Information and Cyber Incident Reporting）的條文內容，[10]咸認可作為整體管控機制據以檢討的法規基礎，加上「國家標準暨技術研究

[9] 美國會推動與 CMMC 機制運作相關的重要國防授權法案提案包括：FY20 NDAA, Section 1648 "Develop a Comprehensive Framework to Enhance the Cybersecurity," FY21 NDAA, Section 1738 "Communicate with and Provide Assistance for Manufacturers in the Defense Industrial Supply Chain," FY21 NDAA, Section 1742 "Cyber Security Practices (CMMC) Capabilities".

[10] "Safeguarding Covered Defense Information and Cyber Incident Reporting," 48 CFR § 252.204-7012, *eCFR*, https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012 (new); https://www.govinfo.gov/content/pkg/CFR-2018-title48-vol3/pdf/CFR-2018-title48-vol3-sec252-204-7012.pdf (old).

院」（National Institute of Standards and Technology，NIST）當時亦已同步陸續發布多項與 CUI 保護及資安管控有關的特別標準（即 NIST 800-171, 172 系列）[11]，復經國防部專案小組就實務面評估這一系列的資安基準，亦認定完全可以滿足並落實上揭 DFARS 第 252.204-7012 節法規增補要求條件的實踐，國防供應鏈 CMMC 機制的整體運作架構因而成型。隨後國防部即於 2020 年 9 月發布 CMMC 1.0 初版，再於 2021 年 11 月參酌各界意見後，修正發布 CMMC 2.0 版，確定機制得以落實的最佳實務執行架構；[12]期間再進一步審視、檢討修訂現行法規，並分於 DFARS 第 252.204-7019、252.204-7020 及 252.204-7021 等節，增補與 CMMC 實務運作及安全評鑑條件有關的條文內容[13]，以取得機制推動的完整法源基礎。另國防部為求機制未來運作周延，最終版的 CMMC 架構，目前仍配合國家標準暨技術研究院徵詢業界對 NIST 相關安全標準回饋意見的持續修調，尚待定案公布。至於 CMMC 機制推動仍須續予以關注的發展[14]，則有：

（一）美國防部對 CMMC 機制的推展，原設定係一個漸進式五年期

---

[11] 美國國家標準暨技術研究院發布與「受控非具分類保密等級資訊」（CUI）保護及網路安全有關的特別標準 NIST 800-171, 172 系列包括：NIST SP 800-171 Revision 2 “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” *NIST*, February 21, 2020 (includes updates as of January 28, 2021), https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final; NIST SP 800-171A “Assessing Security Requirements for Controlled Unclassified Information,” June 13, 2018, *NIST*, https://csrc.nist.gov/pubs/sp/800/171/a/final; NIST SP 800-172 “Enhanced Security Requirements for Protecting Controlled Unclassified Information: a Supplement to NIST Special Publication 800-171,” *NIST*, Updated February 10, 2021, https://csrc.nist.gov/publications/detail/sp/800-172/final; NIST SP 800-171B(draft)“Protecting Controlled Unclassified Information in Nonfederal Systems & Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets,” *NIST*, August 2, 2019, https://csrc.nist.gov/Pubs/sp/800/171/b/IPD.

[12] “Strategic Direction for Cybersecurity Maturity Model Certification Program,” *Chief Information Officer, U.S. Department of Defense*, November 4, 2021, https://dodcio.defense.gov/CMMC/about/; https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/.

[13] 美國因應 CMMC 機制建立於《聯邦採購規則－國防增補規定（DFARS）》所增修的條文包括：“Notice of NIST SP 800-171 DoD Assessment Requirements,” https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7019; “NIST SP 800–171 DOD Assessment Requirements,” https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7020; “Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirement,” https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7021.

[14] “CMMC FAQS,” Chief Information Officer, *DoD*, https://dodcio.defense.gov/CMMC/About/ and https://dodcio.defense.gov/CMMC/FAQ/

的中程執行計畫（a five-year phase-in period），現階段僅部分合約商被選為先導試行對象（only required in select pilot contracts）；但實際情況是國防工業基礎（DIB）絕大部分的主、次合約供應商均已受到通知要求進行安全認證及合規的整備。

（二）依其行動要項規劃，美國政府係期望利用 24 個月（原規劃至 2023 年 11 月）針對現行《聯邦採購規則》（FAR, under Title 32 CFR）及《聯邦採購規則－國防部增補規定》（DFARS, under Title 48 CFR）相關法規條文再進行完整的檢視修正，以完備行政規則的修（制）定。目前 DFARS 部分，除了第 252.204-7021 節有關 CMMC 整體架構的安全條件待最終定案外（on hold），其餘概均已完整法規修正程序；而 FAR 部分，因涉及美國聯邦所有機構一體適用問題，修法進度則仍尚待觀察。

（三）CMMC 機制一旦正式施行（預於 2026 年財政年度起全面實施），針對未來聯邦國防採購個案涉及 CUI 及 FCI 保護要求事項者，並相對應的 CMMC 網路安全認證級別，必將一併納為招標公告的條件（specify required level in solicitation）；即招標時，廠商參標的必要資格條件之一。

（四）有關 CMMC 機制的三層安全認證級別，屬第一級（Level 1）、基礎防護、廠商自評者（self-assessment），至少須符合《聯邦採購規則 FAR 52.204-21 節所列 FCI 的 15 個安全控制項，[15]每年須自評乙次（annual basis）；屬第二級（Level 2）、進階防護、由第三方認證機構評鑑者（C3PAO assessment），則須符合 NIST SP 800-171 安全標準的全部要求，認證效期則為三

[15] "FAR 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems," *Acquisition.Gov*, General Services Administration, https://www.acquisition.gov/far/52.204-21

年（triennial basis）；而列屬第三級（Level 3）、專家防護、由政府指定機構評鑑者（Government assessment），除須符合第一、二級全部的安全標準要求之外，另須加上 NIST SP 800-172 部分要求（尚研議中），認證效期亦為三年（triennial basis）。

三、實務運作的權責分工

針對美國推動國防供應鏈 CMMC 機制的權責分工，政策面除前揭已提及的國防部武獲暨維持次長協同資訊長辦公室完備全般法制修訂與執行規劃，國家標準暨技術研究院負責制定及發布相關安全標準之外，在涉及國防工業廠商的「網路安全需求條件暨評鑑機制」（cybersecurity requirements and assessment mechanisms）實際作業面，則包括：國防合約管理局及其為因應未來認證評鑑工作實需所新設立的「國防工業基礎網路安全評鑑中心」（Defense Industrial Base Cybersecurity Assessment Center，DIBCAC），[16]以及由國防部授權整合的非官方外部單位「網路安全認證機構」（Cyber Accreditation Body，Cyber AB）與經認證的第三方評估組織（Certified Third-Party Assessor organizations，C3PAOs）。[17]其中，國防合約管理局為美國防部直屬執行機構（implementing agency），現階段負責逾 3.5 兆美元的國防合約履約管理工作，其上級督管即為國防部武獲暨維持次長，因此，其被賦予為 CMMC 認證與評鑑工作的主要執行機關，乃職責使然；從該局被賦予任務後，在極有限時間內（約四個月）即成立全新附屬單位「國防工業基礎網路安全評鑑中心」，並規劃完成將外部的網路安全認證機構（Cyber AB）及第三方評估組織（C3PAOs）同步納入全般機制協同運作，此為美國

[16] "Welcome to the Defense Industrial Base Cybersecurity Assessment Center Contractor Resource Page," *DCMA, DoD*, https://www.dcma.mil/About-Us/; https://www.dcma.mil/DIBCAC/

[17] "The Cyber AB, About Us," *Cybersecurity Maturity Model Certification Accreditation Body, Inc.*, https://cyberab.org/About-Us/Overview; "Ecosystem Professions, Assessing and Certification," *Cybersecurity Maturity Model Certification Accreditation Body, Inc.*, https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Assessing-and-Certification

政府充分整合運用民間資源與專業能量，共同遂行國家政策安全目標，非常具體的實踐典範。

另為達成 CMMC 機制於 2026 年前可如期實施的目標，針對國防供應鏈廠商於過渡期的漸進式輔導措施上，國防工業基礎網路安全評鑑中心近期並已啟動「自願評估聯合監管」計畫（Joint Surveillance Voluntary Assessment，JSVA program），[18]就現階段自願參加由第三方評估組織（C3PAOs）預先執行相當於 CMMC 第二級（Level 2）安全基準合規廠商的評鑑與結果，由國防工業基礎網路安全評鑑中心進行全面監管，並將先期通過評鑑者視同已成功完成高可信度的合規評估作業，後續則待前揭聯邦相關法規（DFARS 252.204-7021）完備最終修訂規範並公布後，即可直接轉換為業經授權完成評鑑並擁有為期三年效期的 CMMC 第二級（Level 2）安全認證資格。

其次，在網攻威脅情資分享與回報機制的建構方面（Cyber Threat Information/Intelligence Sharing and Incident Reporting），則是由國防部資安長（DoD CISO）、國防部網路犯罪防制中心（DoD Cyber Crime Center，DC3）及國防反情報暨安全局（Defense Counter-intelligence and Security Agency，DCSA），協同國家安全局（National Security Agency，NSA）整合運用聯邦政府與民間現有相關資源，針對國防供應鏈安全可能遭受到的威脅預警、事件回報與損害管控等各面向，建構政府與業界完整的安全防護網與情資、技術、工具分享平台；[19]主要包括，國防工業基礎資訊分享整合環境（DoD-DIB Collaborative Information Sharing Environment，DCISE）及國防工業基礎網路安全計畫（Defense Industrial Base Cybersecurity

[18] "Gain a Competitive Edge with a Joint Surveillance Voluntary Assessment," *KLC Consulting*, https://klcconsulting.net/joint-surveillance-voluntary-assessment/; Sara Friedman, "First CMMC voluntary assessment scheduled for August as DOD 'joint surveillance' program begins," *Inside Cybersecurity*, July 28, 2022, https://insidecybersecurity.com/share/13748

[19] "Current DoD DIB Cybersecurity Efforts," *Office of Prepublication and Security Review, DoD*, November 15, 2021, https://cmmctraining.academy/wp-content/uploads/2022/07/DIB-Cybersecurity-Activities-Placemat.pdf

Program）等兩項計畫；[20]其中，國防部網路犯罪防制中心與國家安全局網路安全合作中心（Cybersecurity Collaboration Center）近期於 2023 年 6 月，並已合作共同針對國防工業基礎（DIB）廠商發布一項稱為「資安即服務」（Cybersecurity-as-a-Service，CSaaS）的具體執行方案，[21]期望能主動在資安威脅預警、事件回報與損害管控等作為，對通過安全認證、查核無虞的國防供應鏈廠商，提供政府可完整支援的專業技術服務。

肆、結語

由於美國在全球武器裝備及相關國防物資的研究發展、生產製造及輸出，仍居主導地位，從其推動 CMMC 機制所要求的管制對象並不侷限於美國本土廠商，而是全球與其國防工業供應鏈有關連的所有主、次合約商，可以預見的，CMMC 機制及 NIST 安全標準，終將擴及與美國有軍備合作的各個盟友邦，甚至影響國際標準組織或各國對供應鏈資安相關標準的重新審視及檢討，進而對全球的供應鏈安全與風險管理模式帶來引導式的影響。

台灣搭上推動 CMMC 潮流，除部分業界廠家已被美國國防部主合約商通知要求，或自發性地為「接軌美國國防供應鏈商機」在進行安全認證的因應準備之際，試想台灣本身長年投入大量國家資源所扶植發展的國防產業與相關高科技供應鏈，日常所遭遇到的潛在安全威脅與相較於他國有過之而無不及的網攻頻次，在建構自主國防供應鏈安全韌性（Resilience）的前提下，台灣要如何務實地去看待與借鏡美國推動 CMMC 歷程及其他各國導入類同機制的經驗，進

[20] "Defense Industrial Base Cybersecurity Program," *Chief Infomation Officer, Department of Defense*, https://dodcio.defense.gov/Portals/0/Documents/DIB%20Fact%20Sheet.pdf; "DCISE Fact Sheet and Overview," *DoD Cyber Crime Center- DC3*, https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/; "DCISE Fact Sheet," *DoD Cyber Crime Center- DC3*, https://www.dc3.mil/Portals/100/Documents/DC3/Products/Factsheets/DCISE/DC3-DCISE-FactSheet-4JAN2023.pdf?ver=qUFUSGuVSAu0jYCkDMKf2Q%3d%3d&timestamp=1673446156286.

[21] "DoD DIB Cybersecurity-as-a-Service (CSaaS) and Support," *Inside Cybersecurity*, June 5, 2023, https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2023/jun/cs2023_0124.pdf; Jacob Livesay, "Pentagon highlights free cyber services to defense industrial base partners as CMMC rulemaking looms," *Inside Cybersecurity*, June 26, 2023, https://insidecybersecurity.com/daily-news/pentagon-highlights-free-cyber-services-defense-industrial-base-partners-cmmc-rulemaking.

而思考發展契合台灣整體安全環境及國防產業實需的可行機制，殊值探究。

本文作者黃希儒為南非普利托利亞大學系統工程管理碩士，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資深研究員。主要研究領域為：美國安全合作體制、軍購管理、政府採購、武獲策略。

The Evolution and Progress of Implementation of the U.S. Defense Supply Chain CMMC Initiative

Raymond H.J. Huang

Division of Cyber Security and Decision-Making Simulation

Abstract

In response to global security threats and strategic competition between the U.S. and China, the U.S. government is committed to safeguarding its overall national economic interests and reinforcing the critical capabilities and security of its defense industrial base. In recent years, the promotion of Cybersecurity Maturity Model Certification (CMMC) has been driven by a unified goal established by federal government executive and legislative bodies. Its progress encompassed various efforts, starting from the U.S. President's announcement of the National Cybersecurity Strategy, then passage of congressional authorization, delineation of clear roles & responsibilities for different departments, formulation of cybersecurity standards, review & revision of current administrative regulations, and intensive communication with industry. They culminated with the introduction of an entirely new framework and plan by the Department of Defense. The overall implementation process holds valuable lessons. However, comparing the scale of Taiwan's defense industry supply chain and suppliers with the huge defense industrial base of the United States, collective exploration of how to establish a constructive mechanism similar to the CMMC that aligns with Taiwan’s industrial environment and national security needs requires the collaborative efforts of diverse stakeholders.

Keywords: CMMC, Supply Chain Security, Defense Industry, Cyber Security, Information Security Threats