編輯報告

隨著國際及區域情勢變遷，台灣國防工業發展的重要性開始受到關注之餘，其成果也逐漸展露頭角。除了中科院與漢翔早有外銷實績，近來不少媒體揭露，不少中小企業廠商其實也多年接受美國軍火大廠委託，早已是業界所謂的隱形冠軍。

在此同時，美國鑒於國防工業基礎供應鏈不時遭受惡意網路滲透竊密，美國國防部於 2020 年 1 月首次推出「網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC），並於 2021 年 11 月推出 CMMC 2.0 版，針對主、次承包商之間生成、處理、儲存、傳輸的「受控非具分類保密等級資訊」（Controlled Unclassified Information，CUI），加強對其保密性的分級控管。CMMC 可望最快於 2025 年第一季上路，未來只要是想要承接美國國防採購案的主次承包商，在參加競標或簽訂合約之前，都必須先通過 CMMC 認證。

CMMC 相當於取得合約的入門票，其基本 110 項認證要求與數百個稽核要點，雖然讓美國國防工業基礎廠商——尤其是中小企業——咸感壓力沉重，但對於美國友盟國家的國防工業廠商而言，無異於開了一扇門，只要通過符合要求的網安認證，就有機會加入美國國防工業基礎供應鏈，擴大了市場規模的前景，而這也讓投資注入網安認證合規的誘因隨之增加，加拿大、澳洲、法國、日本及韓國的國防部門紛紛結合數位專責部會積極引進。

對於台灣有意打進美國國防工業基礎供應鏈但多為中小企業規模的廠商而言，越早了解、準備而通過 CMMC 認證，屆時越早取得進入供應鏈的合規身分，就能先一步搶得龐大商機。但台廠多半對於 CMMC 陌生，對於如何引進或適用更是不知從何著手。國防安全研究院身為國家級國防智庫，對於了解掌握其緣由背景、當前進

展、側重要點、如何引進，自是責無旁貸。自 2022 年網羅國軍負責採購與資安之退役將領與軍官，成立 CMMC 研究專案團隊、並運用資安大會、刊物與美國在台協會等不同場合平台解析 CMMC 之後，現更以特刊專輯方式，讓讀者能有系統地理解 CMMC。

在本期特刊中，曾怡碩指出美國國防供應鏈核心廠商與協力廠商遭受來自惡意網路攻擊以及竊取營業秘密，讓美國先進科技優勢不斷流失，而管控網安風險其實是伴隨著需受保護控管資料流之輸送、儲存或處理的實體或虛擬空間位置而定，「網路安全成熟度模型認證」（CMMC）應運而生。黃希儒則說明 CMMC 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、制定資安標準、檢討修訂行政規則、與業界密集進行溝通，至國防部提出全新運作架構與計畫之推行歷程。

洪嘉齡除說明 2022 年 10 月 25 日起 CMMC 的最新版，並點出整個 CMMC 圍繞著國防採購合約制度，對於「受控非具分類保密等級資訊」（CUI）的範圍，多由國防合約管理局會同作需單位予以界定。曾怡碩接續強調，美國決心要管控 CUI 等於昭告世人，美國的敵手正積極蒐取這些 CUI，因此必須採取行動加以保護。保護 CUI 的重心在於防止外敵竊取知悉，因此資訊安全的重心絕大部分置於保密性。

黃希儒提出台灣引入 CMMC 的推動策略，並以台廠千附精密引入實務為例進一步闡述說明，進而在實務層面提出建置官方資源分享平台、成立合規專家支援團隊、盤點潛在優先輔導合規對象及制定補助獎勵措施等建議，期在政府的主動整合協助下，台灣企業投入 CMMC 合規及程序改善的成本得以節約，導入整備的效率也進而提升。另從策略層面敦請政府設定更積極的導入目標，發展符合國內國防產業環境實需的「台灣版 CMMC」，維護台灣自主國防產業整體供應鏈的安全，並就安全情勢與產業環境、保護標的資訊定

義、適用法規檢討、跨部門責任分工及政府民間技術資源整合等方面提出相關推動策略。

最後，誠如黃希儒所點出，鑒於台灣國防產業與美國龐大的國防工業基礎（DIB）規模相去甚遠，我國政府與國防產業更需要共同研議如何攜手整合國家有限資源，建構符合台灣自主國防產業環境所需的 CMMC 機制，並達成與美國或其他國家一致、高規格的資訊與網路安全標準。

供應鏈網路安全的地緣政治因素

曾怡碩

網路安全與決策推演研究所

壹、前言

網路空間即使根路由與域名有地域區別，在過去基本運用上並無地域與國界考量。多年來網路攻擊事件頻傳、加上國家行為者紛紛將網路空間視為另一戰場之後，地緣政治逐漸成為網路安全防禦的重要考量。與此同時，過去依據地緣關係以及比較利益優勢形成的全球供應鏈，隨著資訊化運籌管理的普及，被迫必須面對逐步升高的網路攻擊威脅—特別是網路竊取營業秘密與勒索軟體。此外，美國自川普政府開始，對中國大陸發動貿易戰之餘，更加緊對中國大陸施行高科技管制出口以及乾淨網路的科技脫鉤（decoupling）或去風險（derisking），這除了讓供應鏈安全成為國家安全關鍵要素、並全面拉高網路安全防護在供應鏈安全中的優先次序，地緣政治儼然躍升成為供應鏈網路安全的核心考量之一。

然而，對於供應鏈網路安全如何考量地緣政治因素，猶待進一步研析。有鑒於此，本研究運用文獻分析法，首先探討 2018 年迄今，在美中科技脫鉤潮流下，美國如何驅動供應鏈安全加入網路安全認證；其次則是探究該樣態供應鏈網路安全認證如何結合地緣政治考量。

貳、地緣拒止戰略下的科技脫鉤

從地緣政治觀點來看，在自由開放的印太戰略之下的美中戰略競爭不再一昧依循圍堵，美國對中共除戰略嚇阻外，在高科技領域已逐步形成 2021 年美國國防次助卿 Elbridge Colby 在軍事上所論述之「拒止戰略」（Strategy of Denial），[1]依循地緣考量，設立各式資

[1] Elbridge A. Colby, The Strategy of Denial: American Defense in an Age of Great Power Conflict

訊流通關卡，拒絕、防止中共竊取或取得高科技關鍵技術，避免讓中共在高科技領域突破、甚至稱雄，在現下與未來都將極端困難。主要的操作策略呈現為科技脫鉤，鞏固此一拒止戰略的背後理念則為民主對抗威權的陣線串聯。

一、美中科技脫鉤

「美中科技脫鉤」的成型並非一蹴可及，中方考量到中國大陸、俄羅斯及「一帶一路」沿線國家的市場接受度，不太可能一開始就完全切斷與歐美國家之作業系統、通訊協定及社群媒體軟體規格之相容性。歐美科技大廠考慮到前述陣營之龐大市場與訂單，也會在利益驅動下遊說，緩步進行全面禁止支援中方技術規格與系統服務。如此將讓中國大陸自主開發的軟硬體一開始將強調相容性，以換取市場空間與研發時間。但隨著「美中科技脫鉤」的成形，國安因素將不斷介入，強化雙邊陣營間技術與服務的區隔，這將讓技術規格與市場也漸趨涇渭分明，進一步明確劃出技術限制移轉界線，導致市場區隔藩籬與技術限制鐵幕將趨向一致。

如同過去美蘇冷戰一般，科技脫鉤藩籬界線的劃訂，主要還是以民主與專制為區隔基準。中共代表的專制威權，隨著網路與人工智慧科技成熟而更加無所遮掩。在意識形態影響與思想控制上，中國大陸網路各式媒體興起，自媒體與簡訊、短影片尤其蓬勃發展。中國大陸字節跳動推出的「抖音」應用程式，不僅在中國大陸境內廣受歡迎，更是風靡全球。

然而在境內，北京除嚴加監控網路新媒體上的言論與行徑以進行輿情監測，更對於中共官方認定的有害資訊內容，予以嚴密審查管制。網路媒體內容審查的監管，落在「中央網路安全和資訊化委員會辦公室/國家互聯網資訊辦公室」，即「網信辦」身上， 每年「網路清朗活動」以網路生態治理為名，要求網路資訊內容服務平

(New Haven: Yale University Press, 2021).

台業者，擔負起內容審查的責任。對於推薦演算法與生成式大型語言模型，中共也加以管制，實現從資料到演算法到生成語言的一條龍管控。

循此發展可能導致中共借助俄羅斯獨立自主根伺服器之網路系統 Runet，並在中國大陸的國內市場與「一帶一路」沿線國家之外，把反圍堵陣線擴大到俄羅斯廣大市場，以形成中俄陣營與美歐陣營之間壁壘分明的對峙。華為已針對俄羅斯提出以 Aurora 為架構的作業系統，而希望順利進入俄羅斯市場。此外，在二分的格局下，不排除華為可能買回已售出之華為海纜，為將來中俄陣營進行海纜布局，形成從資料傳輸到消費者使用端設施均為完整自主系統局面。

二、價值取向的友盟鏈結

隨著「一帶一路」倡議推展到東南亞、南亞、南太平洋，以及歐亞大陸、巴爾幹等中東歐國家，北京藉由「一帶一路」倡議中的基礎建設，佈建海外航港營運與 5G 通訊系統。這些舉措的戰略性質引起美國嚴密警覺與注目，川普政府開始以「印太戰略」作為因應對策。在美中兩強之外，歐盟是唯一具有空間與實力提出「印太戰略」與「一帶一路」以外的戰略途徑，但受英國脫歐、歐盟決策模式的影響，歐盟在經過數年謹慎觀察與評估之後，在 2018 年先提出「歐洲與亞洲連結戰略」（Connecting Europe and Asia – Building Blocks for an EU Strategy），時隔近 3 年，才在美國拜登政府多邊合作戰略架構下，於 2021 年 4 月提出《歐盟印太合作戰略》（EU Strategy for Cooperation in the Indo-Pacific）。針對其中鏈結的部分，尤其是基礎建設發展議題，緊接著 G7 在 2021 年 6 月提出的《Build Back Better World（B3W）夥伴倡議》，歐盟於 2021 年 7 月 12 日發布「全球連結的歐洲」（A Globally Connected Europe），有意在「印太戰略」與「一帶一路」之外，提供另一個戰略路徑選項。

面對美國「印太戰略」與中共「一帶一路」在基礎建設全球布局的開展，「全球連結的歐洲」意味著歐盟在對自身境內基礎建設布局之外，也將觸角延伸面向全球，對於歐洲以外地區展開以歐盟價值為依歸的連結戰略。

參、供應鏈網路安全的地緣政治因素

各式鏈結倡議所構建的產品或服務之供應鏈的輸送通道，在現今數位年代，互通有無過程生成資料通訊網路即面臨網路安全的議題。民主陣營主要依循美國「乾淨網路」倡議，原則上硬體、韌體與軟體均須注意網路安全管理，具體而言，硬體方面還包括資料傳輸所經地、資料傳輸管線通路、資料儲存中心所在地，以及天線、路由器、伺服器、晶片，與硬體維運及軟韌體開發維運人員等人事物地之安全認證，均須列入分級管理。

一、資料傳輸安全

近年引人矚目的光纖纜線，由於佔全球資料傳輸量的九成以上，在資料已然成為生產要素大宗物資之際，隨著數位化的普及，資料產出與流通的需求與日俱增，大型網路營運平台業者近年自建海纜，已然為時勢所趨。海纜經過國家所設之海纜登陸站及資料中心，尤其在美國更動海纜規劃以避開中國大陸後，海纜路線儼然成為地緣政治熱門議題。美國提出「乾淨網路」倡議，此關鍵資訊基礎設施的硬體便是海纜，受海流、海底地形變化、漁撈拖網及海底生物啃咬，均可能造成「斷線」，必須依賴國際專業維修船業者。此外，陸上海纜接收站軟體也必須定時更新，這二項維運極易成為情蒐目標，因而必須納入國安考量。

二、資料儲存安全

資料中心的地點選擇，除避開地震帶、電力基礎設施與電價考量，例如中共「東數西算」工程，將東部資料輸往西部資料中心儲

存暨運算。其餘還有在資料落地趨勢下，各國基於司法互助而進行之資料存取，例如美國與他國簽署之《雲端法案》，可作為資料中心選擇之依據之一。抖音海外版 TikTok 備受美國官方與國會質疑美國用戶資料會遭中共官方以情報法要求存取，TikTok 提出解決方案之一，即為將資料存於與美國具司法互助關係之國家的雲端資料中心。

三、資料運算及晶片安全

至於資料中心所需算力，一來仰賴不斷修正精進之演算法更新，對此中共視為網路主權，除立法管制出口，還出言制止美國要求 TikTok 出讓股權成為美國控股公司。[2]另一方面，算力還仰賴高階晶片，而美國拜登政府為釜底抽薪，於 2022 年推出的《晶片與科學法案》，為美國半導體生產提供約 520 億美元的政府補貼，對晶片製造投資實施稅收抵免，並計畫在此後 5 年內授權超過 1,700 億美元的預算，以提升美國半導體產業的競爭力，並紓解晶片持續短缺的現象。[3]在此之前拜登在 2021 年還簽署行政命令點名台灣、日本、韓國與美國組成半導體 CHIP 4 聯盟，後續搭配 2022-23 年諸多出口管制新措施，[4]以遏制中國大陸半導體產業的增長，並嚴密管控中共借殼規避晶片出口管制。[5]

由於台積電已成為高階晶片最大宗來源，鑒於資安考量與台海衝突之地緣政治風險，要求台積電前往亞歷桑納州設廠。美國官員並不諱言台積電晶片攸關美國國防產業之供應鏈安全，美國在台協會日前針對台積電的決定，即直指台積電晶片為 F-35 關鍵零組件。

---

[2] 〈中國批美禁 TikTok 是「沒自信」 中網友反酸：那你禁推特臉書是?〉，《自由時報》，2023 年 3 月 1 日，https://news.ltn.com.tw/news/world/breakingnews/4225095。

[3] 黃松勳，〈拜登簽署《晶片與科學法案》以鞏固美國在未來科技的領導地位〉，《科技產業資訊室》，2022 年 8 月 11 日，https://iknow.stpi.narl.org.tw/post/Read.aspx?PostID=19456。

[4] 蕭逸夫，〈晶片四聯盟 (Chip-4) 和美國新晶片出口管制對台灣與中國晶片產業的影響〉，《Newtalk 新聞》，2022 年 10 月 13 日，https://newtalk.tw/citizen/view/58922。

[5] 陳昭宏，〈晶片大戰！華為正在中國建秘密晶片網絡 規避美國制裁〉，《Newtalk 新聞》，2023 年 8 月 23 日，https://newtalk.tw/news/view/2023-08-23/885350。

其餘多國也提出比照設廠需求，而台積電則選擇性進行海外布局，除在美國亞利桑那州廠投資金額擴增至 400 億美元，將投入 4 奈米及 3 奈米製程生產，並在日本熊本投資建廠，預計 2024 年底前以 28 奈米、22 奈米、16 奈米及 12 奈米製程生產。[6]

肆、轉向資料流安全管控

美國國防部鑑於國防供應鏈核心廠商與協力廠商遭受來自惡意網路攻擊以及竊取營業秘密，讓美國先進科技優勢不斷流失，尤其眼睜睜看著中共毫不遮掩地仿造美式武器，面對中共點點滴滴的全面情蒐模式，聯邦機構及國防廠商所產生、經手、儲存與處理的諸多類似「受控非分類保密等級資訊」（Controlled Unclassified Information，CUI），自然而然成為中共之情蒐高價值目標，也讓美國國防部採購部門與反情報部門對於國防工業基礎網路安全防護繃緊神經，積極制定足以拒止中共竊密的機制。[7]

從前述供應鏈網路安全的地緣政治因素考量，可以看出管控網安風險的層級考量，其實是伴隨著需受保護控管資料流之輸送、儲存或處理得實體或虛擬空間位置而定。美國國防部國防合約管理局（Defense Contract Management Agency，DCMA）因而自 2020 年 11 月底即已開始力推「網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC），要求國防廠商在競標國防契約時，必須證明自身於非聯邦機密網路中所儲存、傳輸或處理（含產出）之「聯邦合約資訊」（Federal Contract Information，FCI）及「受控非分類保密等級資訊」的保護，通過其網路安全成熟度層級的各項驗證，以符合美國國家標準與技術研究院（NIST）針對保護非聯邦系統和組織中 CUI 所出版之 *NIST Special Publication 800-171*

[6] 〈亞利桑那州廠明年量產 台積電：工作不以國籍區分〉，《中央社》，2023 年 3 月 2 日，https://www.cna.com.tw/news/afe/202303020200.aspx。

[7] "Controlled Unclassified Information," U.S. DoD CUI Program, https://www.dodcui.mil/. Also see: "Controlled Unclassified Information (CUI)," US Defense Counterintelligence and Security Agency Website, https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/.

規定要求。[8]

伍、結語

俄烏戰爭讓世人感受食物與能源等大宗物資供應鏈因地緣政治衝突而中斷的全球衝擊，而數位時代資料儼然已為新興大宗物資，在美中科技脫鉤形勢下，供應鏈安全的考量還需涵蓋網路安全的地緣政治因素，以達到對中共戰略拒止目標，防止中共竊密轉為對美不利之軍事進展。CMMC 管制國防工業基礎的供應鏈網路安全，尤以資料流所經人地物均端視機敏等級與分類狀況，而可能列為不同等級下之控制項。若我國有意以 CMMC 對「受控非分類保密層級資訊」的管控為參考基準，須注意其最初積極推動應用在採購合約的三個美國政府機構，就是國防部、國家反情報安全中心以及網路安全暨基礎設施安全局。這也反映 CMMC 對供應鏈安全的著眼點，是把資安與反情報融入到從採購到製造、整合與應用端的整個過程。

本文作者曾怡碩為美國喬治·華盛頓大學政治學系博士，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副研究員。主要研究領域為：軍隊與網路安全、網電作戰、認知作戰、中國數位監控。

[8] 參閱 CMMC 認證機構（Accreditation Body）Cyber AB 官方網頁說明，https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/DIB-Companies-OSCs。

Geopolitical Factors Affecting Supply Chain Security

Yisuo Tzeng

Division of Cyber Security and Decision-Making Simulation

Abstract

After the Trump Administration launched a trade war against China, decoupling and de-risking through export control over high technology and the Clean Network closely followed, making supply chain security a key national security concern. Cybersecurity therefore became the top priority in supply chain security, into which geopolitics jumped and became one of the core concerns. As far as supply chain security is concerned, data transmission, storage and computation must take account of related persons, hardware, software, and locations.

US defense industrial base core enterprises have encountered malicious cyberattacks and espionage aiming to steal commercial secrets, thereby compromising the US high-tech edge. With China making no disguise of its desire to copy US weapons through incremental piecemeal intelligence collection, controlled unclassified information (CUI) generated, transmitted, processed, and stored by federal agencies and defense industrial base (DIB) enterprises has naturally been given high priority in China's intelligence collection.

Layered cybersecurity risk control rests on physical and virtual locations of CUI generation, transmission, processing and storage. Following the direction of strategy of denial, US DoD DIBCAC has introduced Cybersecurity Maturity Model Certification, or CMMC, which will require DIB enterprises to satisfy requirements for managing CUI before bidding for and signing procurement contracts.

Keywords: Strategy of Denial, Supply Chain Security, Tech Decoupling, CMMC

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

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。

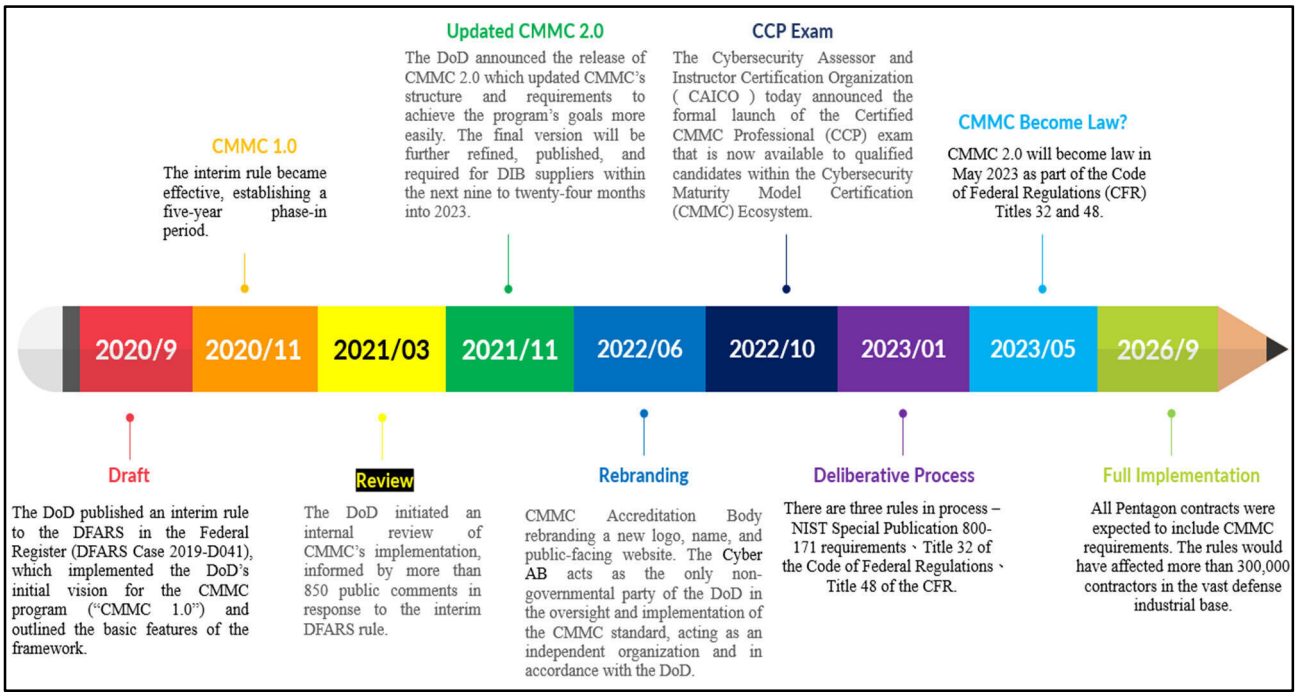

圖 1、CMMC 發展歷程

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。

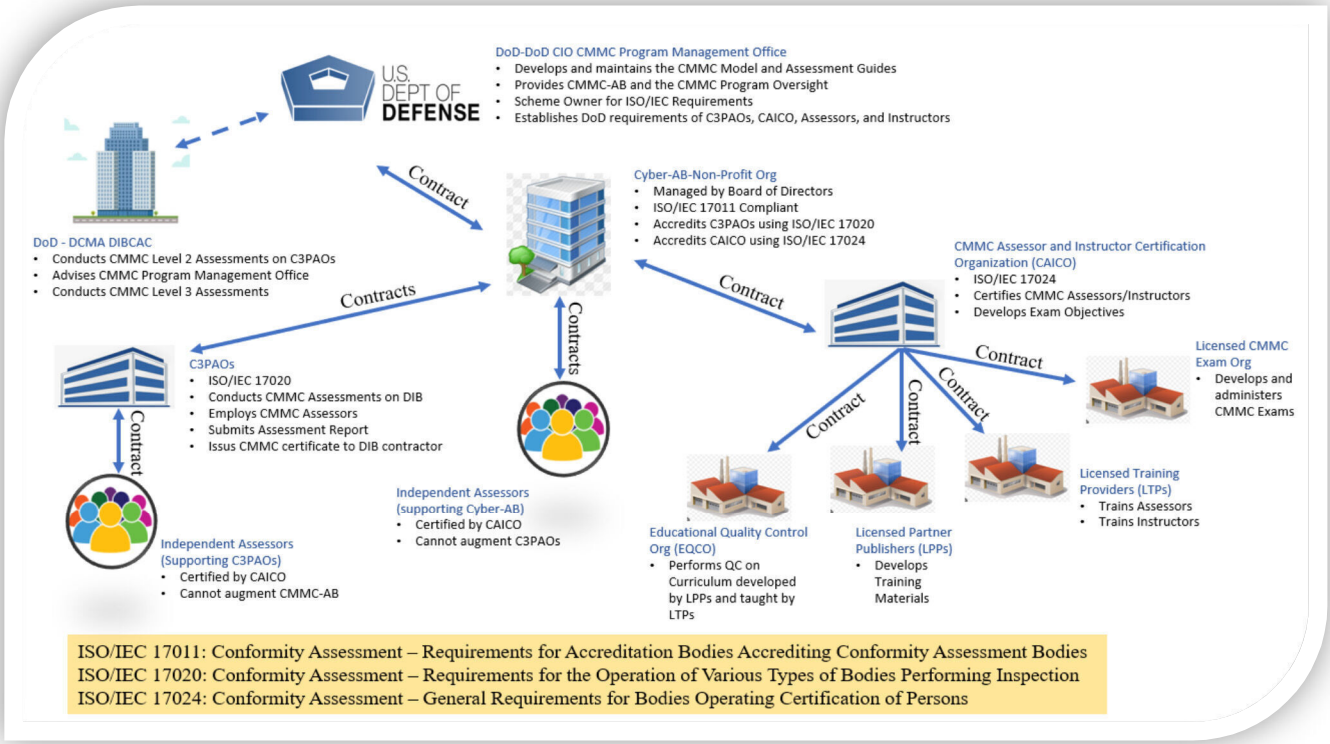

圖 2、CMMC 生態系統

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。

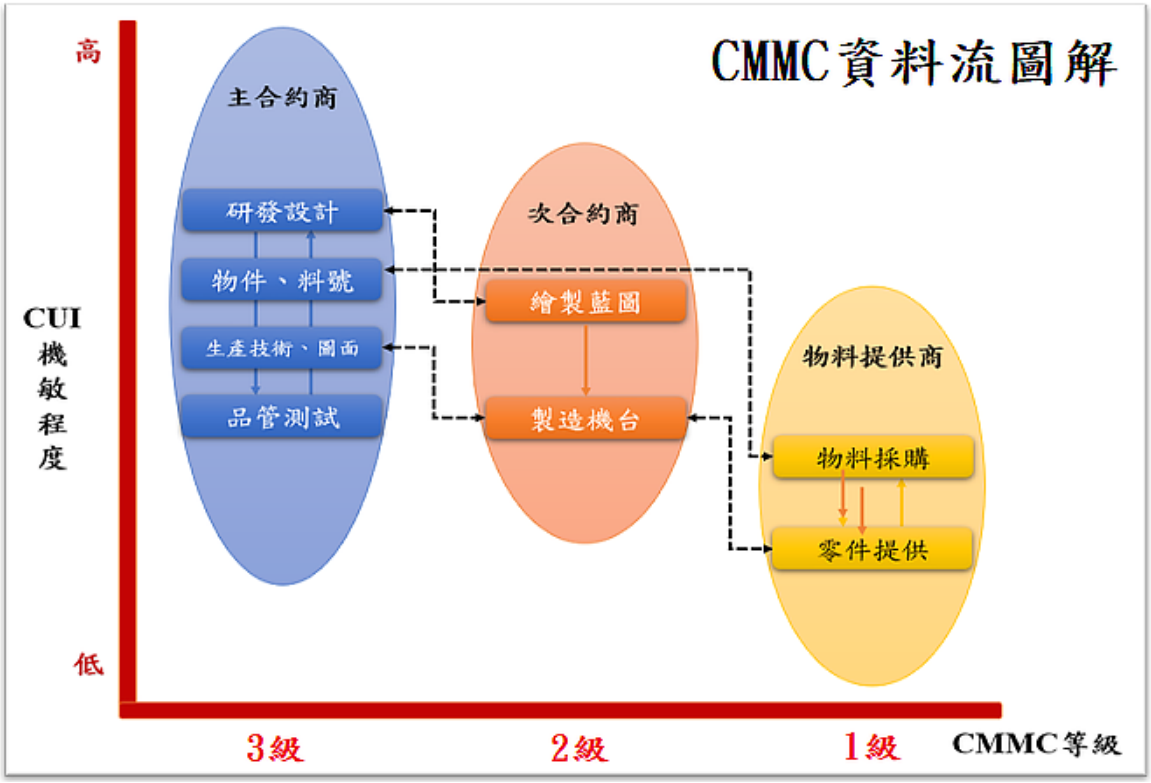

圖 4、CMMC 資訊流安控

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

「受控非具分類保密等級資訊」的安全意涵

曾怡碩

網路安全與決策推演研究所

壹、前言

本期特刊主題為美國國防部推動的「網路安全成熟度模型認證」（CMMC），其重心即為針對國防工業基礎廠商在競逐美國的國防採購合約之前，就已經針對該購案所接觸使用、產生、傳遞與儲存的非機敏資訊進行符合風險等級的管控，尤其是「受控非具分類保密等級資訊」（Controlled Unclassified Information，CUI）所傳經的部分，均必須符合《國防聯邦採購管制補充條例》（Defense Federal Acquisition Regulation Supplement，DFARS）與 NIST 800-171 規範。關於國防工業基礎廠商對於資訊流的保護，是本期介紹 CMMC 認證機制所要傳達的重點，不僅是從虛擬空間到實體空間、也包含從軟體到硬體到操作人員。

在機密資訊之外，美國國防部要整個國防工業基礎大小廠商都要正視 CUI 的管控，不僅讓加入美國國防產業供應鏈的廠商嚴陣以對，也讓對打入美國供應鏈躍躍欲試的外國廠商充滿疑竇，究竟 CUI 為何方神聖，竟值得如此大費周章。以下將就 CUI 緣起、如何界定 CUI 與公開情報、在 CMMC 如何判定 CUI 的範圍與風險等級，逐一予以介紹分析，以期於解惑之餘，有助於我國面對境外敵對勢力積極滲透竊取資訊的同時，能讓國防工業基礎廠商及政府機關加強資訊保護暨反情報作為。

貳、管控非機敏資訊的背景與安全意涵

一、納管 CUI 的緣起

鑒於資安事件頻傳，尤其 2007 年國防大廠洛克希德馬丁遭駭侵，依後來史諾登洩密文件披露，據信當時係中共網路竊取匿蹤戰機技術，[1]國防供應鏈網路安全引起高度重視。白宮於是在 2008 年發布〈指定與分享受控非機敏資訊備忘錄〉（*Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI)*），首次將 CUI 一詞用於聯邦政府文件，並將「敏感但非具分類保密等級」（sensitive but unclassified）資訊納入管制。[2]然而，2009 年美國仍發生國家檔案紀錄管理局（National Archives and Records Administration，NARA）數百萬筆退伍軍人資料外洩事故，終於促成歐巴馬總統於 2010 年 11 月發布《13556 號行政命令》（*Executive Order 13556*），正式要求管理受控非機敏資訊。接續至 2021 年供應鏈資安事故不斷且愈演愈烈，美國則因應推出國家標準暨技術研究院的 NIST SP 800-171 與 172 以及建立在基礎上的 2016 年《國防聯邦採購管制補充條例》（Defense Federal Acquisition Regulation Supplement，DFARS）、2020 年國防部之「網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC），目標都鎖定在管控 CUI。

二、CUI 的安全意涵

CUI 是由政府所擁有或產出、或是由企業組織為政府而持有或產出、且需要依循既有法規政策規範之資訊安全保護之資訊。CUI 雖非機敏資訊，但其敏感性令美國政府認定，CUI 倘遭惡意外洩將對國家安全造成威脅。[3]諸如承包政府業務的廠商處理、儲放、傳輸政府資訊與自身因與其他廠商或政府之間因業務衍生而處理、儲放

[1] 江昱蓁，〈隱形的間諜活動 外媒披露陸駭客如何竊取 F-35 關鍵科技〉，《中時新聞網》，2022 年 2 月 16 日，https://www.chinatimes.com/realtimenews/20220216002107-260417?chdtv。

[2] "Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI)," *The White House*, May 7, 2008, https://www.archives.gov/files/cui/documents/2008-WH-memo-on-designation-and-sharing-of-cui.pdf.

[3] "Introduction to Controlled Unclassified Information (CUI)," *NSF*, September 2022, https://www.nsf.org/knowledge-library/introduction-controlled-unclassified-information-cui.

及傳輸的資訊，包括政府限制接觸及露出的資訊、銀行帳戶及資金流動等財務資訊、本身或其他業者之營運敏感資訊、以及相關個資，鑒於保密性（confidentiality）不足所造成之溫和（moderate）衝擊，需在 NIST SP 800-171 基礎上，對其接近取用及其他共 14 項安全要求予以管控，以達到合宜安全（adequate security）認證。

相對地，政府任職人員平日不斷處理、儲放與傳輸這些非機敏資訊，發布行政命令管控 CUI 等於是讓公職人員對於如何處置這類資訊終於有所依循。雖然本期特刊主題為 CMMC，係針對國防產業基礎所流通的 CUI，但 2010 年 11 月發布的《13556 號行政命令》將 CUI 的管理交由 NARA，將 CUI 區分 18 類型，包括關鍵基礎設施、出口管制、金融、國際協定、防務、採購、移民、自然與文化資源、專賣商業資訊、情報、執法、法律、北約、核能、隱私、條款、統計、稅務。[4]

不論是對承包政府業務業者、還是對政府公職人員而言，美國決心要管控 CUI 等於昭告世人，非具分類保密等級資訊非常敏感而相當具有價值，美國的敵手正積極蒐取這些 CUI，因此必須採取行動加以保護。基於這樣的特質，在資訊安全防護所注重的保密性、完整性與可及性中，保護 CUI 的重心在於防止外敵竊取知悉，但同時可以讓承包政府業務的業者間仍可接近使用完整未被竄改的 CUI，因此資訊安全的重心絕大部分置於保密性。基於保密考量，首先就必須區分 CUI 為業務相關單位限制於內部流通之資訊，並且嚴格確保不會對外揭露；即使在所謂的內部流通，基於敏感性／洩露所造成傷害衝擊，可以進一步區分不同等級的 CUI，在內部流通時採取管理認證措施，限制未達相對應等級認證的廠商機構或人員之接近取用。[5]

[4] "Introduction to Controlled Unclassified Information (CUI)," *NSF*.

[5] "How to Determine the Sensitivity of Information," *Spirion*, April 20, 2021, https://www.spirion.com/blog/how-to-determine-the-sensitivity-of-information/.

三、比較 CUI 與公開情報

CUI 與公開情報均為情報蒐集標的，但兩者有重疊部分，也有相大差異。首先，CUI 是屬於資料與資訊，而公開情報則是蒐集非機敏資訊並經過分析處理後的情報，在層次上有所差異。其次，CUI 主要是在內部流通且避免對外公布，而公開情報顧名思義，原則上是開放流通，但往往未必能在公開網站或者公開發表的報告或刊物上可以接近取用，所以人員情報在公開或非公開場合交換意見所蒐集到之非機敏情資，在廣義上亦屬於公開情報。智庫或諮詢顧問公司在各處蒐集發布的公開資訊或未公布的資訊之後，整理研判成為公開情報。情報機構則根據四處蒐集的公開情報與機敏情資，匯集點點滴滴勾串為線索與面向。由此可知，CUI 本就為情報機構蒐集之公開情報中，屬於非公開的資訊範疇。

再次，CUI 與公開情報既然為情報蒐集目標，自然也成為反情報目標。這也說明了美國國防反情報中心為何會將 CUI 與 CMMC 進展視為其業務關切項目。只是，除非刻意，否則 CUI 不至於出現假情報。但在公開情報部分，需要花費很大心力過濾辨識假情報，特別是敵我均會摻入假情報並刻意提供餵給對手蒐集，以其誤導對手研判。最後，基於反情報需求，CUI 的重心在於保密性，除防止人員刻意或過失之洩密，也加強網路安全以防制網路駭侵所導致外洩漏洞。相較之下，公開情報的反情報重心，反而在於辨析蒐集之公開情報是否為對手刻意釋放的假情資，特別是生成式大型語言模型（如 ChatGPT）及人工智慧分析，均可質疑所蒐集之數據會否遭下毒汙染，進而根據假訊息分析而導致研判失準偏差。

參、CUI 管控實務

一、如何劃分界定 CUI

要讓與政府有業務往來的業者在面對控管 CUI 的要求時，能夠

自願或不得不遵循，仰賴的就是採購合約裡必須法遵，將對於 CUI 的控管明列為履約要求項目（requirement）。以國防採購為例，現行 DFARS 要求得標主合約商或次合約商須通過 NIST SP 800-171 管控 CUI 認證，將來最快於 2025 年第一季施行的 CMMC 則要求合約商在參與競標之前即須通過認證。[6]

業者面臨的迫切挑戰在於，要如何確認自身在特定合約中的業務營運是否持有 CUI，又該讓那些業務範疇通過何種等級的認證？最簡單直接的方法，就是先確認該採購合約所承載業務是否屬機敏資訊，如果不是，接下來就是要確認是否為現行法規或管制條例所約束，如果是，那很自然地可以認定從政府單位傳輸過來的資料會落入 CUI 的範疇，合約商與政府或其他合約商之間將處理、儲放、傳輸 CUI，就必須依照 NIST SP 800-171 控制項要求，在軟體、硬體、韌體及人員、設施、網路通訊渠道等均達到網路安全標準。[7]

另一方面，即使不是從政府傳輸過來，主合約商或次合約商因自身合約業務所產生的資訊，也可能經自身或主合約商檢視 NARA 的 CUI 規範後，認定屬於 CUI 範疇。如果次合約商承載業務經主合約商認定屬於 CUI 範疇，那次合約商即須與主合約商通過一樣等級的認證。換句話說，保護 CUI 的等級要求，與該合約商規模大小無關，只與 CUI 資訊流究竟經過何處有關。[8]

具體而論，如果就一特定購案之主合約商下有三家次合約商，第一家次合約商涉及之業務並無須處理、儲放與傳輸 CUI，第二家次合約商涉及業務需處理、儲放與傳輸等級較低之 CUI，而第三家

---

[6] 根據數位部產業司主辦之美國國防採購管理局之國防工業基礎網路安全評估中心 DIBCAC 在 2023 年 8 月 14 日 DIBCAC 基礎訓練營授課內容。另可參閱：Derek White, “Controlling CUI: CMMC & DFARS Explained,” *Cuick Trac*, https://www.cuicktrac.com/blog/dfars-cmmc/。

[7] “Managing Controlled Unclassified Information (CUI),” *NSF*, October 2021, https://www.nsf.org/knowledge-library/managing-controlled-unclassified-information.

[8] 根據數位部產業司主辦之美國國防採購管理局之國防產業基礎網路安全評估中心 DIBCAC 在 2023 年 8 月 15 日 DIBCAC 基礎訓練營授課內容。另可參閱：“Identifying and Protecting Controlled Unclassified Information (CUI),” *NSF*, November 2021, https://www.nsf.org/knowledge-library/protect-controlled-unclassified-information。

次合約商涉及業務僅有一部份需處理、儲放與傳輸等級較高之CUI，則第一家顯然無須擔心 CUI 範疇界定，而第二家與第三家次合約商均涉及 CUI 流通，除須通過不同等級之認證，第三家次合約商業務所涉及之 CUI 將不能流經認證等級低的第一家及第二家次合約商。換句話說，CUI 的流動所經之處，必須是經過保護認證等級與該 CUI 敏感等級相對應的業者。[9]

二、管理 CUI 步驟與認證實務

要通過 DFARS 或未來 CMMC 之供應鏈網路安全認證，在確認該合約商在業務涉及產生、處理、儲放與傳輸 CUI 範疇與等級之後，接續在接受評估認證之前，還必須釐清確認 CUI 流經所有路徑，才有辦法真正界定 CUI 評估範疇，後續才能針對流經路徑之軟體、韌體、地點、硬體、通訓鏈路、操作人員自身及其手持行動裝置，按照 NIST SP 800-171 或 172 控制項要求進行網路安全認證，以確定該合約商經評估符合保護CUI的標準。[10]關於資訊流安控，可參照本期特刊作者洪嘉齡所撰文的圖 4。

根據美國國防採購管理局之國防產業基礎網路安全評估中心 DIBCAC 所分享之 DFARS 評估認證實務，近年來雲端普遍之後，還需再三確認 CUI 流經之設置、鏈路與經手之人員，一旦雲端被認定為內部網路環境，CUI 流經該雲後，其雲端服務廠商亦須通過相吻合的網路安全評估認證。反之，倘若連接雲端被視為外部雲，則除非該外部雲之主要平台業者被評估通過認證，否則 CUI 將難以傳輸至該雲。[11]

在實務上，網路安全評估專家建議可以先描繪出業務資訊流關

[9] 根據數位部產業司主辦之美國國防採購管理局之國防產業基礎網路安全評估中心 DIBCAC 在 2023 年 8 月 15 日 DIBCAC 基礎訓練營授課內容。

[10] 數位部產業司，DIBCAC 基礎訓練營授課內容，2023 年 8 月 15 日；“Identifying and Protecting Controlled Unclassified Information (CUI),” *NSF.*

[11] 數位部產業司，DIBCAC 基礎訓練營授課內容，2023 年 8 月 15 日。

係圖，並將 CUI 流經之處予以標示後，劃分接續評估認證的人員、設備、網絡、軟硬體，擬定供應商安全計畫，由滿分開始計算扣分，如也未達要求項目，可擬具「行動暨里程碑計畫」，提供給評估人作為評估依據。[12]

肆、結語

本文說明「受控非具分類保密等級資訊」在美國按照法遵階層，從總統行政命令、國家檔案紀錄管理局分類指令、國家標準暨技術研究院之標準與國防聯邦採購管制補充條例及 CMMC 要求，一路到國防工業基礎網路安全評估中心（DIBCAC）的認證實務，[13]強調根據 CUI 流經之處予以劃分範疇後，接續簡介評估認證的人員、設備、網絡等軟體、硬體及韌體。我國如有意輔導國防產業廠商介接美國 CMMC 認證，勢必需要對美國國防工業基礎之主合約商所界定之 CUI 的保護，輔導國內廠商及早規畫說明，並對於國內廠商可能產生之 CUI，在美國主合約商協助之下予以了解與掌握，冀能趕上 2025-2026 年之際 CMMC 認證正式上路之列車，開拓更廣大的海外市場。

本文作者曾怡碩為美國喬治·華盛頓大學政治學系博士，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副研究員。主要研究領域為：軍隊與網路安全、網電作戰、認知作戰、中國數位監控。

[12] 數位部產業司，DIBCAC 基礎訓練營授課內容，2023 年 8 月 14 日。

[13] 數位部產業司主辦之美國國防採購管理局之國防產業基礎網路安全評估中心 DIBCAC 在 2023 年 8 月 14 日 DIBCAC 基礎訓練營授課講義 A，頁 1-36。

Security Implications of Controlled Unclassified Information

Yisuo Tzeng

Division of Cyber Security and Decision-Making Simulation

Abstract

This article explicates that, in the US, Controlled Unclassified Information, or CUI, began with a President Executive Order, then NARA's classification guidelines, going all the way to NIST SP 800-171, DFARS and DoD's DIBCAC certification practices.

The US determination to manage CUI delivers a message to the world that CUI in and of itself is so valuable that it is worth protecting from adversaries' dot-connecting. In that sense, the prime factor for protecting CUI is confidentiality, rather than all three foci of information security, namely confidentiality, integrity, and availability.

Completion of the scoping of CUI is to identify and map CUI flow after confirming the extent to which the defense contractor is involved in generating, processing, storing and transmitting CUI. The software, firmware, hardware, locations, communication link, human operators and their own mobile device along the pathway the CUI goes through must meet NIST SP 80-171 or 172's control requirements to ensure the contractor is certified.

Keywords: Supply Chain Security, CUI, Counterintelligence, CMMC

台灣導入 CMMC 推動策略

黃希儒

網路安全與決策推演研究所

邱紹正

千附精密資訊部經理

壹、前言

若以業界導向（Business Driven）觀察現階段台灣國防產業相關企業對美國「國防供應鏈網路安全成熟度模型認證」（Cybersecurity Maturity Model Certification，CMMC）的準備與「國家標準暨技術研究院」（National Institute of Standards and Technology，NIST）資訊安全標準導入的意向，概可區分為：

一、原已是美國聯邦國防供應鏈的參與廠商（次合約商），應美國國防合約管理局（Defense Contract Management Agency，DCMA）及主合約商（prime contractor）要求，強制導入並進行認證相關前置準備工作，以期保有其持續供應的優勢；

二、對於進入美國聯邦國防採購供應鏈具高度期待，或對自身產品、核心技術相關專屬權利與企業資訊的保護具較高安全意識，主動投入資源，嘗試自評或導入規範；

三、仍處於觀望情況，期待政府政策方向及指導作法明朗化後，再考量本身的投資成本效益，始決定是否導入。

不可諱言地，就上揭實況細察，除了列屬於「項次一」為數甚少且原已由美國政府透過主合約商主動通知，要求須強制進行導入並預作 CMMC 認證準備的廠商之外（本文所列千附精密案例），事實上，國內業界有意嘗試自評但不得其門而入，或欠缺動機與利基

而處觀望者，仍占絕大多數，此均有待政府引領明確政策指導及後續推動方向。

美國推動 CMMC 機制近三年來，其國內、外約 30 萬家的國防供應鏈廠商，均將陸續受到要求進行資安認證；而隨著歐盟、加拿大、英國，以及印太地區的澳洲、日本、南韓等國家陸續加入推動行列，CMMC 機制與 NIST 的一系列標準，亦將成為現階段全球產業供應鏈最具規模的安全管控分級體制與資安基準；再進一步觀察各國政府如何看待美國的 CMMC 機制，除普遍亦是為了「接軌美國國防供應鏈商機」在作因應準備之外，實際上，各國參酌美國 CMMC 機制及 NIST 標準，亦均同步為發展建置符合本身國防產業整體環境所需的類同資安管控機制與基準在努力；以日本及加拿大為例，日本以美國的 CMMC 機制及 NIST SP 800-171 標準為參考基礎，已自行制定相當於日本版 CMMC 的「防衛產業資安基準」，[1] 並於 2023 年 4 月開始試行適用於防衛省防衛裝備廳列有相關安全條件的新購合約；至於加拿大版的 CMMC「網路安全認證計畫」（Canadian Cyber Security Certification Program，CCSCP）則甫於 2023 年 5 月 31 日公布，亦是直接引用 NIST SP 800-171 為安全基準，預劃自 2024 年冬季擇定部分列有安全需求條件的先導合約試行實施。[2]

貳、千附精密應美國要求導入 CMMC 歷程

自 1986 年，千附精密為響應國家國機國造政策，以航太零組件製造為起步，毅然投入精密金屬加工生產領域，歷經二十餘年的經

[1] 〈防衛産業サイバーセキュリティ基準の整備について〉，《防衛装備庁》*(Acquisition, Technology and Logistics Agency, ATLA)*, https://www.mod.go.jp/atla/cybersecurity.html；松本恭典，〈今後の防衛生産・技術基盤の維持・強化について〉，《防衛装備庁技術シンポジウム 2022》，2023 年 3 月，https://www.mod.go.jp/atla/research/ats2022/pdf/prog_policy_05.pdf。

[2] "Government of Canada helping defence industry protect itself from cyber security threats", *Public Services and Procurement Canada*, May 31, 2023, https://www.canada.ca/en/public-services-procurement/news/2023/05/government-of-canada-helping-defence-industry-protect-itself-from-cyber-security-threats.html.

驗累積與技術能力提升，於 2009 年，藉由漢翔航工業的引薦開始承接美國國防主合約商洛克希德馬丁（Lockheed Martin）公司（以下簡稱：洛馬公司）的訂單，在洛馬公司人員駐廠的專業技術輔導下完成各項產能建置及品質的要求，並於 2011 年首次交付產品，正式進入美國國防產業供應鏈，成為美國聯邦國防工業基礎（Defense Industrial Base，DIB）的廠商之一。2020 年 11 月，美國《聯邦採購規則－國防部增補規定》（Defense Federal Acquisition Regulation Supplement，DFARS）增修 DFRAS 252.204.7021 節有關 CMMC 運作架構及需求條件後，[3]千附精密係於 2021 年初接獲洛馬公司通知，指出其製供品項過程涉及「受控非具分類保密等級資訊」（Controlled Unclassified Information，CUI）[4]的保護，因此正式被要求改變以往僅於美國聯邦供應商風險評鑑系統（Supplier Performance Risk System，SPRS）[5]自行登錄資安管控自評成果的作業模式，而須進行取得 CMMC 第二級（Level 2）[6]的安全認證準備，以利持續保有合格次合約商的身份；千附精密的整備工作，依洛馬

[3] "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).

[4] 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。

[5] 有關美國聯邦供應商風險評鑑系統（SPRS）的法規要求及美國防部入口網站，請參閱："DFARS: Use of Supplier Performance Risk System Assessments," https://www.sprs.csd.disa.mil/nistsp.htm; https://www.federalregister.gov/documents/2023/03/22/2023-05671/defense-federal-acquisition-regulation-supplement-use-of-supplier-performance-risk-system-sprs.

[6] 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 個控制項，每年自評乙次（annual basis）；屬第二級（Level 2 進階防護）須經第三方認證機構評艦者（C3PAO assessment），須符合 NIST SP 800-171 標準要求的所有控制項目，認證效期則為三年（triennial basis）；屬第三級（Level 3 專家防護）須由政府指定機構評鑑者（Government assessment），則須符合第一、二級全部要求的標準，加上 NIST SP 800-172 部分要求（尚研議中）的控制項目，認證效期亦為三年（triennial basis）。

公司的指導必須將現行 NIST SP 800-171 標準所要求的資安控制項目，[7]規劃納入公司的系統安全計畫書（System Security Plan，SSP）與管制行動要項，隨即依計畫推展，主要步驟如次：

一、先盤整、檢視洛馬公司所指定已交付予千附精密的 CUI 相關文件資訊在組織內的確切流向，經過公司內部哪些系統？經手哪些層級、部門及員工？確認須進行標準合規的所有系統的數量及流程現況，以利優化後續所需投注的人力與資源。

二、尋求國外具標準稽核經驗顧問團隊，針對上揭 CUI 資訊流所涉系統，協助逐項審認其與 NIST SP 800-171 所要求的 14 個控制面向、110 項安全標準的全般對應關係。

三、依安全標準自行評鑑公司現有系統現況，同步重新檢討修訂組織內部相關標準作業程序，列出所有待辦行動管制要項，追蹤改善，以達到公司日常維運「說、寫、做」一致的優化目標。

導入之初，千附精密首先面臨的是公司日常處理的大量資訊，因為系統、作業流程變更及權限的重新劃分等衝擊，諸多原已習以為常的維運作業，受到新賦予的安全標準框架約束，工作效率驟降，算是組織遂行資安防護的必要之惡，無可避免；此外，將現行系統進行合規改善、優化及重新進行安全設定過程，發現原有系統於初期建置時，相關軟、硬體架構均已被限定，尤其是市售套裝系統軟體部分，幾乎完全無程式修改彈性，若有些微機會得以委託原軟體開發商進行修改優化，亦所費不貲，另若確認無優化空間，最終僅能以堆疊式架構的替代方案來達成安全標準要求，例如：公司簽核系統原套裝軟體，因無法設定較縝密的密碼原則要求，最後只能改採「一次性使用者身分驗證登入」（Single Sign-On）的解決方

[7] 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.

案涵蓋原簽核系統。

其次，依 NIST 安全標準規範，公司各個子系統間的關連性，係以資安功能為核心，整合過程涉及新、舊子系統廠商的協力配合，此與上揭提及的系統軟體修改難度一般，均將使公司面臨大幅成本投入，甚或根本無法整合改善的窘境。千附精密自接獲洛馬公司通知展開 CMMC 合規整備工作，目前執行近一年，其在既有資訊系統已具備一定完善程度的狀況下，為克服前揭所遇各項困難，人力及資源仍持續投注中，之後並須直接面對美方授權指派的第三方評鑑組織（Third Party Assessment Organization，C3PAO）的現地評鑑，距實際可取得所需安全等級的認證，尚且還有一段將備受煎熬的時日；相對地，其他國內廠商若係從零開始建置，其所要耗費的時間、人力、技術及經費，將不言可喻。

參、台灣導入 CMMC 策略

一、業界導向（Business Driven）實務層面

前已提及，若台灣係以爭取未來參與美國國防供應鏈為任務目標，國內除了少數原本即為美國防採購的次合約商且已由主合約商強制要求須預作 CMMC 認證整備者外，其他有意嘗試導入自評或尚持觀望態度的絕對多數廠商，仍殷切期盼政府能扮演指導、輔導及資源整合角色，引領業界進行接軌、導入準備。而現階段，為增加台灣國內各界對美國 CMMC 機制與 NIST 資安標準的整體認知，非常樂見政府責成數位發展部、經濟部等部門，帶動相關法人團體、工商協會，甚至私人資安訓練機構，已密集展開 CMMC 的相關訓練課程；惟此期間，亦有來自資訊專業媒體對台灣導入美國 CMMC 機制的關注焦點提出：仍偏重於輔訓廠商取得認證，或期待向美國爭取設立相關在地評鑑機構，而尚欠缺「藉由管控機制及安全標準的

引進帶動整體產業升級」思維的相關評論；[8]因此，參酌上揭千附精密為續行維持其在美國國防供應鏈次合約商資格所付出的艱困合規歷程，台灣除了現階段各界正在努力的推廣宣傳與教育訓練之外，有無更積極得以加速政府與民間專業資源整合共享、增益企業理解未來導入 CMMC 及 NIST 標準優勢的具體措施？俾使企業在進行標準合規及流程改善過程，獲得成本節約與效率提升的實質幫助；相關策略作為如次：

（一）建構官方網站、數位媒體平台及知識資料庫，提供業界有關 CMMC 機制及 NIST 安全標準的相關資訊、技術指引與實踐案例，供業界無償自主學習研究與運用，促進業界相互交流，分享經驗。

（二）整合政府部門及民間專業機構成立合規專家支援團隊，因應個別企業商機爭取及資安環境需求，提供客製化合規專業技術指導與支援，並開設技術諮詢服務窗口，協助企業針對合規自評或導入過程所遇窒礙，適時給予相關解決方案專業建議。

（三）盤點台灣企業具有成為美國國防供應鏈潛在實力廠家，優先列為輔導合規對象，並主動提供美國聯邦國防採購與國防主合約商產品項目合作商機等相關資訊。同時針對未來國內政府採購「如何將已通過 CMMC 資安認證廠家資格納為招標優先適用對象」的相關法規條件進行研議。

（四）制定輔導、補助計畫與獎（激）勵措施，對自主嘗試導入合規標準的國內企業或協助推動合規專業教育訓練機構，提供政府相關資源補助，並針對後續順利取得 CMMC 安全認證的廠家給予適切獎（激）勵。

[8] 黃彥棻，〈臺灣推 CMMC 偏重認證，明顯缺少產業升級思維〉，《*IThome*》，2023 年 1 月 16 日，https://www.ithome.com.tw/news/155124。

二、政府導向（Government Driven）策略層面

上揭案例，千附精密為滿足未來可順利取得美國防部 CMMC 機制第二級（進階防護）認證的實需，艱辛導入 NIST SP 800-171 安全標準的合規歷程，或可做為後續台灣其他有意參與美國聯邦國防供應鏈廠家的借鏡經驗，惟就現實層面而言，台灣對美國 CMMC 機制導入的認知與目標，若僅是鼓勵與輔導產業滿足資安標準的合規，甚或自我局限於寄望向美國爭取成立在地驗證機構等機會，雖然得藉以協助少部分國內廠商通過認證，而向美國及其盟友邦的國防供應鏈漸次擴展商機，惟政府及業界大費周章地為獲取 CMMC 認證及 NIST 標準合規所作的一切努力與付出，依然是在美國聯邦安全管控機制下運作，致力協助保護的「標的」對象，終究還是美國的國防採購供應鏈與國防工業基礎（DIB），對台灣本身國防產業整體安全維護，實質助益尚屬有限。

美國因戰略競爭關係，遭受中國或其他國家不斷地對其國防及高科技產業供應鏈，進行情蒐與技術資訊竊取，促使美國政府投入如此龐大規模的資源，加速 CMMC 機制的建置與推動；若以政府推動導向（Government Driven）進行策略思考，台灣著實有必要設定比「輔導業界導入 CMMC 爭取美國國防供應鏈商機」更積極的政策安全目標。因此，台灣究係是要完全比照美國推動 CMMC 的作法，或自建一套執行機制？若台灣導入的目標，亦是設定如同前揭其他各國參酌美國 CMMC 架構與 NIST 完善的資安基準，而發展符合自身區域情勢與國防產業環境所需的「台灣版 CMMC」供應鏈安全管控機制，相關推動策略如次：

（一）安全威脅與產業環境評估：

台灣因地緣政治關係與所處區域安全情勢，在面對中國日常文攻武嚇的同時，無形的網攻對國防建軍備戰、國防產業、高科技供

應鏈及國防採購相關合約廠商，所進行的情蒐、竊取，甚至具破壞性的安全威脅程度，以及政府及民間機構現階段對機敏或技術資訊保護的安全管控作為與韌性等實際情況，均有待政府各有關單位作進一步瞭解評估，以作為後續推動建置符合自身安全環境所需的國防供應鏈安全管控機制基礎參據。

（二）保護「標的」的明確定義：

美國對於國防供應鏈 CMMC 機制要保護的對象「受控非具分類保密等級資訊」（CUI）及「聯邦合約資訊」（FCI），於聯邦法令體系有非常明確且完備的定義；台灣現行《國家機密保護法》及其子法或其他如《資通安全管理法》、《政府採購法》、《國防產業發展條例》等相關法令，並未曾針對上揭須遂行保護的 CUI 或類同 FCI 的「政府採購合約資訊」（Government Contract Information，GCI）做過任何定義；此外，由於現今人民對政府相關施政資訊適時公開揭露的權利要求，更甚於以往，因此未來於法規面針對 CUI 及 GCI 的定義與範圍，須務求周延、明確，以免引發紛爭。

（三）適用法規與安全標準的審視與制定：

美國政府建立 CMMC 全新機制，是一系列由上而下、政府主導驅動的過程，從白宮發布國家策略、國會通過授權法案、國家標準暨技術研究院訂定安全標準，到國防部修訂行政規則、建制完整的運作架構；因此，除了前揭安全保護標的 CUI 及 GCI 須在後續相關法令增修訂取得法令上的周延定義與適用範圍之外，台灣現行涉及國防產業發展與安全管控的相關法律及行政規則，例如《國防產業發展條例》、〈列管軍品廠商安全查核辦法〉及〈國防科技工業合作廠商安全調查執行作法〉，甚至有關《資通安全管理法》要求不論「公務」或「特定非公務機關」，均須取得國家或國際資安認證

標準（CNS 27001 或 ISO 27001）等相關法規、基準內容，[9]其與 CMMC 認證等級與 NIST 安全標準間的差異與競合關係，均須面臨全般檢視或重新制（修）定。

（四）跨部門整合與權責分工：

就國內推動實況而言，政府現階段係以「輔導與協助業界通過 CMMC 安全認證，爭取參與美國國防供應鏈商機」的立場，責由數位發展部協同相關部會與民間企業協會進行安全標準導入；惟若以台灣整體國防產業與國防合約供應鏈為導入對象，甚而發展自己的產業供應鏈安全管控機制與制定符合本身需要的國家資安評鑑標準而言，從美國及其他國家推動歷程，因事涉國防產業供應鏈全般安全環境的變革，且 CMMC 機制本來即是以國防採購及其供應廠商為管控核心，各國主事單位概均為國防部門，但相關部會的專業分工與整合，亦至為重要。

（五）政府與民間資安專業資源與聯防機制的整合：

美國推動 CMMC 機制，除借重民間網路安全認證機構（Cyber AB）及第三方評估組織（C3PAOs）的專業協同納入整體安全認證工作之外，針對國防供應鏈安全管控過程可能衍生的威脅預警、事件回報與損害管控等問題，亦是由政府與民間業界進行技術資源整合，共同建構整體安全防護網與資安專業技術工具分享平台。事實上，無論政府或民間機構，資安專業技術與相關工具的發展，是台灣全球聞名的強項之一，尤其是近年來，台灣業界供應鏈不乏遭到惡意攻擊的案例，因而不斷強化自身資安防護作為，加上政府持續推動國家級資安戰略的「資通安全聯防與情資分享合作」等方案，[10]

[9] 媒體中心，〈資通安全管理法之衝擊與影響〉，《*SGS TAIWAN*》，2019 年 3 月 11 日，https://www.sgs.com.tw/news-media-resources-content/page?id=2。

[10] 〈第六期國家資通安全法：佈建「主動防禦」聯網，躍升亞太資安樞紐〉，《資安人》，2021 年 3 月 31 日，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=9142；羅正漢，〈NCC 揭露資安跨域聯防發展現況，主動式防禦成新焦點〉，《*iThom*》，2021 年 12 月 10 日，https://www.ithome.com.tw/news/148311。

據此，均可作為未來專業資源整合基礎，共同建構國防產業供應鏈的安全防護工作。

肆、結語

在政府「國防自主」及「資安即國安」的政策指導原則下，已經給予推動導入美國 CMMC 機制非常積極且明確的安全目標；然而，台灣國防產業與美國龐大的國防工業基礎（DIB）規模相去甚遠，無論在策略或實務層面，為防杜國防科技與其他高科技產業機敏資訊遭竊取或不當移轉，維護國防安全與國家整體利益，政府與國防產業要如何攜手整合國家有限資源，克服種種限制因素，發揮台灣引以為傲的資安專業優勢，建構符合台灣自主國防產業環境所需的 CMMC 機制，達成與美國或其他國家一致、高規格的資訊與網路安全標準，實有賴各界續予集思廣益，共同研議。

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。

本文作者邱紹正為千附精密股份有限公司資訊部經理。

Strategies for Implementing CMMC in Taiwan

Raymond H.J. Huang

Division of Cyber Security and Decision-Making Simulation

Alex Chiu

ChenFull Precision Co., Ltd.

Abstract

In this article, by observing the intentions of Taiwan's defense industry regarding the introduction and adoption of the U.S. defense industry supply chain Cybersecurity Maturity Model Certification (CMMC) and related information security standards, and using the practical example of local company Chenfull Precision's efforts to meet the requirements of the prime contractor to maintain its status as a secure supplier source for the U.S. defense industrial base, the challenges encountered in preparing for CMMC certification and NIST's standards are highlighted. On the practical level of implementation, the recommendations include establishing an official resource sharing platform, forming a compliance expert support team, identifying potential priority compliance goals, and formulating subsidy and incentive measures. It is anticipated that, with proactive governmental integration and support, Taiwan's industry CMMC-related compliance and procedural enhancement can be more cost-effective, resulting in increased implementation efficiency. Additionally, considering the progression of the U.S. CMMC initiative and similar mechanisms adopted by other nations, from a strategic perspective, Taiwan's government is urged to set a much more ambitious goal and develop a "Taiwan version of CMMC" tailored

to the specific security needs of its own defense industry environment; the aim of this is to safeguard the overall security of Taiwan's defense industry supply chain. Recommendations are also provided on matters related to security conditions and industrial environment, the definition of protected information assets, review of applicable regulations, cross-departmental division of responsibilities, and integration of government-private sector resources.

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

CMMC 相關縮寫簡字原義暨編譯對照

黃希儒

網路安全與決策推演研究所

縮寫	英文原義	中譯
C3PAOs	Certified Third-Party Assessor organizations	第三方評估組織
CCSCP	Canadian Cyber Security Certification Program	加拿大網路安全認證計畫
CDI	Covered Defense Information	涉及國防的受控非具分類保密等級資訊
CFR	Code of Federal Regulations	聯邦規則彙編（編目）
CMMC	Cybersecurity Maturity Model Certification	網路安全成熟度模型認證
CSP	Cloud Service Provider	雲端服務供應者（商）
CSaaS	Cybersecurity-as-a-Service	資安即服務（計畫）
CUI	Controlled Unclassified Information	受控非具分類保密等級資訊
Cyber AB	Cyber Accreditation Body	網路安全認證機構
DC3	DoD Cyber Crime Center	國防部網路犯罪防制中心
DCMA	Defense Contract Management Agency	國防合約管理局
DCSA	Defense Counter-intelligence and Security Agency	國防反情報暨安全局
DCISE	DoD-DIB Collaborative Information Sharing Environment	國防工業基礎資訊分享整合環境
DFARS	Defense Federal Acquisition Regulation Supplement	聯邦採購規則－國防增補規定
DIB	Defense Industrial Base	國防工業基礎
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center	國防工業基礎網路安全評鑑中心
DIB CP	Defense Industrial Base Cybersecurity Program	國防工業基礎網路安全計畫
DoD	Department of Defense	國防部
DoD CIO	DoD Chief Information Officer	國防部資訊長
DoD CISO	DoD Chief Information Security Officer	國防部資安長
DoDD/I/M	DoD Directives/Instruction/Manual	國防部 指導/指引/手冊

縮寫	英文原義	中譯
DoJ	Department of Justice	司法部
E.O.	Executive Order	執行命令（美國總統）
FAR	Federal Acquisition Regulation	聯邦採購規則
FBI	Federal Bureau of Investigations	聯邦調查局
FCI	Federal Contract Information	聯邦合約資訊
FedRAMP	Federal Risk and Authorization Management Program	聯邦風險暨權限管理計畫
FIPS	Federal Infomation Processing Standards	聯邦資訊處理標準
FOUO	For Official Use Only	限官方運用
GCI	Government Contract Information	政府採購合約資訊
ISO	International Organization for Standardization	國際標準組織
JSVA	Joint Surveillance Voluntary Assessment (program)	自願評估聯合監管（計畫）
LES	law enforcement sensitive	具法律強制執行的敏感資訊
MSP	Managed Service Provider	管理服務供應者（商）
NARA ISOO	National Archives and Records Administration / Information Security Oversight Office	國家檔案暨紀錄管理局 資訊安全監管辦公室
NCS	National Cyber Strategy	國家網路策略
NCSS	National CyberSecurity Strategy	國家網路安全策略
NDAA	National Defense Authorization Act	國防授權法案
NIST	National Institute of Standards and Technology	國家標準暨技術研究院
NSA	National Security Agency	國家安全局
NSA/CCC	NSA Cybersecurity Collaboration Center	國家安全局網路安全合作中心
PBI	proprietary business information	商業專屬權利資訊
PII	personally identifiable information	個人身份識別資訊
POA&Ms	Plan of Actions and Milestones	行動計畫暨管制時程節點
SBU	Sensitive but Unclassified	敏感但非具分類保密等級（資訊）
SCRM	Supply Chain Risk Management	供應鏈風險管理
SPRS	Supplier Performance Risk System	供應商風險評鑑系統
SSO	Single Sign-On	一次性使用者身分驗證登入
SSP	System Security Plan	系統安全計畫書

縮寫	英文原義	中譯
U/CTI	Unclassified/Controlled Technical Information	受控非具分類保密等級技術資訊
USD/A&S	Under Secretary of Defense for Acquisition and Sustainment	國防部武獲暨維持次長

資料來源：黃希儒整理及編譯。