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