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。