美國資通安全成熟度模型驗證綜覽

CMMC 實施在即 全球國防供應鏈整備以待

美國聯邦政府對於常見供應商威脅已經發展出供應鏈資安風險管理（C-SCRM），在供應鏈韌性這必要前提下，企業宜預先完成合規準備並完善資安治理與管理制度。納入 CMMC，除了符合美國國防部的國防供應鏈資安要求外，也恰好為即將進入法制化的美國聯邦採購法規 CUI 規則（FAR CUI Rule，適用所有聯邦政府機構的供應鏈廠商）預做準備。

文／梁日誠

美國國防部（DoD）於 2024 年 10 月 15 日公布了 32 CFR Part 170 CMMC Program 的最終規則（final rule），預計兩個月後正式生效，未來也將搭配 48 CFR Part 204 CMMC Acquisition 規則（2024 年 8 月進入 NPRM），進而確定美國國防供應鏈的「資通安全成熟度模型驗證」（Cybersecurity Maturity Model Certification，CMMC）要求，來強化美國國防暨國家安全。

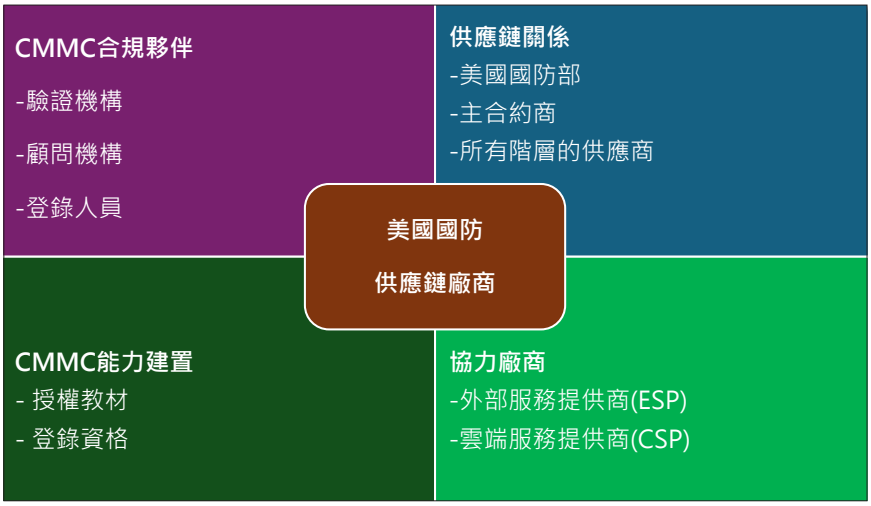
對於已經是、即將是或未來是美國國防供應鏈的供應商而言，於取得合約前必須先達成 CMMC 合規，才能擠身於美國國防供應鏈。所有階層（all tiers）的供應商也可由利害相關團體的角度，如**圖一**，綜覽 CMMC Program 規則的主要更新的概貌。

供應鏈關係

CMMC 的主管機關為美國國防部（DoD），DoD CIO（https://dodcio.defense.gov/CMMC/）提供了各項 CMMC 整備所需的資源，包含了如：

- CMMC 101 Brief、
- CMMC Program Model Overview、
- CMMC Level 1 Scoping Guidance、
- CMMC Level 1 Self-Assessment Guide、
- CMMC Level 2 Scoping Guidance、
- CMMC Level 2 Assessment Guide、
- CMMC Level 3 Scoping Guidance、
- CMMC Level 3 Assessment Guide、
- CMMC Hashing Guide 等合規指引文件（2.13 版）。

其中，CMMC Level 1（Self）更新為 15 個 FCI 的要求（與 FAR 52.204-21 校準），CMMC Level 2（Self、C3PAO）更新為 110 個 CUI 的要求（源自



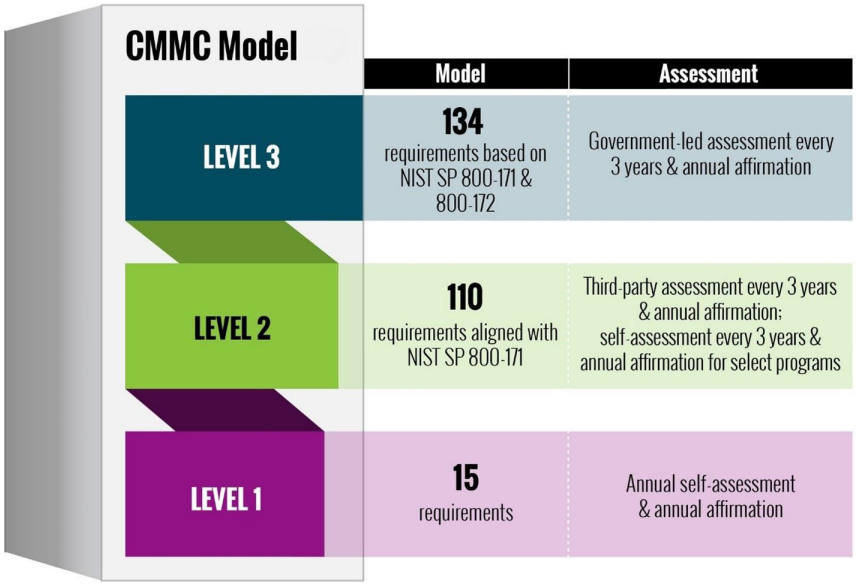
圖一、美國國防供應鏈廠商之利害相關團體示意圖。

於 NIST SP 800-171 R2），CMMC Level 3（DIBCAC）更新為 134 個 CUI 的要求（包含 Level 2 的 110 個先決要求與源自於 NIST SP 800-172 中選擇的 24 個要求）。最新的 CMMC Model 示意圖如**圖二**。

DoD 將各 CMMC Levels 均納入每年由供應商的確證官員（Affirming Official）進行年度確證（Affirmation）的要求，以確保供應商的持續合規。於 CMMC Level 2 Assessment Guide（v2.13）中指出，運作的 Plan of Action 與 32 CFR § 170.21 中所述的 CMMC 評鑑 POA&M 的不同，有助於評鑑時的判定與釐清。

於 CMMC Program 規則中，對於 NOT APPLICABLE（N/A，不適用）做出了說明，指出，在 CMMC 評鑑中，標註為不適用（N/A）的評鑑結果表示該項安全要求或評鑑目標在評鑑時不適用，對於每個被標註為不適用的安全要求或評鑑目標，經驗證的評鑑員（Certified Assessor，如：CCA，Lead CCA）須提供一份說明，解釋該要求對該供應商不適用的原因，此外，供應商應在其系統安全計劃（SSP）中記錄該安全要求不適用的原因及理由。

DoD 對於 CMMC 於合約中的要求，採取階段式實施（phased implementation），



圖二、CMMC Model 示意圖（資料來源：CMMC Model Overview - DoD CIO）

Seq. of Phase	Phase 1	Phase 2	Phase 3	Phase 4
規劃時程	自 48 CFR CMMC 規則生效日起	Phase 1 開始後1年	Phase 2 開始後1年	Phase 3 開始後1年
原則執行項目	Level 1（Self）或 Level 2（Self）	Level 2（C3PAO）	Level 3（DIBCAC）	All Levels
DoD 裁量項目	Level 2（C3PAO）	Level 2（C3PAO）、Level 3（DIBCAC）	Level 3（DIBCAC）	
提前實施可能	V	V	V	V

表一、CMMC 階段式實施時程表

主（prime）合約商要求	若供應商處理、儲存或傳送：	
	FCI	CUI
Level 1（Self）	Level 1（Self）	N/A
Level 2（Self）	Level 1（Self）	Level 2（Self）.
Level 2（C3PAO）	Level 1（Self）	Level 2（C3PAO）
Level 3（DIBCAC）	Level 1（Self）	Level 2（C3PAO）

表二、最低延伸傳遞條款要求一覽表

CMMC Level #	Level 1	Level 2	Level 3
FCI 資產	V		
CUI 資產		V	V
安全保護資產（SPA）		V	V
風險管理資產（CRMA）		V	（併入 CUI 資產）
特定資產（Specialized Assets）	V（Out-of-Scope）	V	V
範圍外資產（Out-of-Scope Assets）	V	V（VDI 條件適用）	V（VDI 條件適用）

表三、CMMC Levels 與資產類別對應表

各階段的實施內容如**表一**，包含原則執行項目與 DoD 裁量項目。若考量最早的 CMMC Level 2（C3PAO）的可能要求時程，預估將可能出現於 Phase 1 的 2025 年間。

對於國防供應鏈廠商間的延伸傳遞條款（flow-down）要求，於 CMMC Program 規則中整理於**表二**，CMMC 的延伸傳遞條款要求適用於所有階層（all tiers）的供應商。

於 CMMC 的範圍（Scoping）與資產類別（categories）領域，更新了 Level 3 的分類方式並納入虛擬桌面基礎建設（Virtual Desktop Infrastructure，VDI）成為範圍外（Out-of-Scope）資產的條件：若以 VDI 做為客戶端的端點，如果其配置不允許在該端點進行任何 CUI 的處理、儲存或傳輸，而僅限於將鍵盤／視訊／滑鼠的資料發送到 VDI Client，則該端點被視為範圍外資產（簡稱 VDI 條件）。CMMC Levels 與資產類別對應表如**表三**。

協力廠商

國防供應商在履行合約時，常需要協力廠商（如：ESP、CSP、MSP）的參與，才能順利履約並有效的使用資源，CMMC Program 規則明確的定義了協力廠商並列舉其合規的要求，整理如**表四** ESP 範圍要求。

協力廠商的定義如下，ESP：外部服務供應商（External Service Provider）、CSP：雲端服務供應商（Cloud Service Provider，依據 NIST SP800-145 Sept2011 識別）、MSP：管理服務供應商（An ESP（not a CSP）hat provides technical support services to its clients）。CMMC Program 規則中，更新定義了「安全保護資料」（Security Protection Data，SPD），SPD 是指由安全保護資產（Security Protection Assets, SPA）儲存或處理的資料，SPA 用於保護供應商的環境，SPD 屬於與安全相關的資訊，包括但不限於：營運 SPA 所需的組態資料、由 SPA 生成或接收的日誌文件、與範圍內資產的組態或漏洞狀態相關的資料、以及授予範圍內環境存取權限的密碼。若 ESP 為供應商的 CMMC 評鑑範圍之內，ESP 可選擇適當的 CMMC Level 評鑑來展現或達成或協助供應商合規。

當 ESP 處理、儲存或傳送：	當使用 ESP 做為：	
	CSP	非 CSP
CUI（有或無 SPD）	此 CSP 應符合 48 CFR 252.204-7012 中的 FedRAMP 要求	由 ESP 提供的服務為供應商的 CMMC 評鑑範圍，且應為供應商 CMMC 評鑑的一部分.
SPD（無 CUI）	由 CSP 提供的服務為供應商的 CMMC 評鑑範圍，且應為供應商 CMMC 評鑑的 SPA.	由 ESP 提供的服務為供應商的 CMMC 評鑑範圍，且應為供應商 CMMC 評鑑的 SPA.
無 CUI 亦無 SPD	不處理 CUI 或 SPD 的服務供應商並不符合 CMMC 的 ESP 定義.	不處理 CUI 或 SPD 的服務供應商並不符合 CMMC 的 ESP 定義.

表四、ESP 範圍要求

要求事項	CCP	CCA	Lead CCA
CAICO 課程&考試	ATP/APP-CCP & 考試	ATP/APP-CCP、CCA & 考試	ATP/APP-CCP、CCA & 考試
行為準則簽訂	CoPC	CoPC	CoPC
背景調查	Tier 3 或等同	Tier 3 或等同	Tier 3 或等同
資通安全經驗		3年	5年
管理經驗			5年
評鑑或稽核經驗		1年	3年
使用語言	英文	英文	英文
DoD Cyberspace Workforce Framework's Security Control Assessor（612）Work Role, from DoD Manual 8140.03		Intermediate Proficiency Level，如：CGRC/CAP or CASP+ or Cloud+ or PenTest+ or Security+ or GSEC 等證照	Advanced Proficiency Level，如：CISM or CISSO or CPTE or CySA+ or FITSP-A or GCSA or CISA or CISSP or CISSP-ISSEP or GSLC or GSNA 等證照
	註：Courses at higher proficiency levels qualify lower levels.		

表五、CMMC 評鑑人員的能力與資格要求

CMMC 合規夥伴與 CMMC 能力建置

供應商在尋求 CMMC 合規的道路上，訓練與建置內部人員能力（如 CCP 與 CCA），自行導入 CMMC 是方法之一，也可尋求具備 CMMC 專業人員或機構協助導入，於導入後尋求 C3PAO 的 CMMC Level 2 評鑑或自我評鑑（Level 1（Self）或 Level 2（Self））。C3PAO 由 CMMC 的認證機構（Accreditation Body）所認證，應保持其獨立公正的立場，避免顧問與驗證／評鑑角色的利益衝突。

CMMC Program 中的人員驗證機構 CAICO 則負責專業 CMMC 人員如，PI、CCI、CCP、CCA 等的人員驗證工作。PI 與 CCI 為專業 CMMC 講師，講師於執行工作期間不應擔任顧問角色，CCP 與 CCA 可擔任顧問或評鑑/驗證角色，但於同一供應商時，CCP/CCA 不可同時扮演顧問與評鑑／驗證角色。CMMC Program 對於 CMMC 評鑑人員的能力與資格要求綜整列於**表五**。若完成 ATP 開辦的 CCP 或 CCA 課程（使用經認可的 APP 教材）且不選擇進行 CCP/CCA 資格驗證的人員，將於 CCP/CCA 考試通過後獲得 CAICO 頒發的專業證書，以展現對應 CCP/CCA 的能力達成。

CMMC 的要求與現行的 DFARS 252.204-7012、7019、7020 同時並行於美國國防產業，供應商對於聯邦法規、國防法規與 CMMC 規則均須等同重視並持續維持合規，才能有效的確保供應商資格及合約的持續有效，近期備受重視的新興國防議題，如：無人機領域、AI 領域等，因具前瞻性，也成為各國競相爭取的專案，CMMC 逐漸成為檯面上的資通安全入場券。由近期筆者參與的 DFARS 評鑑與 CMMC 模擬（Mock）評鑑的經驗觀之，發現美方 Prime 合約商對現有及未來的國防資通安全要求等同重視，除了要求現行的 DFARS 資安合規外，也要求供應商切結將遵循即將實施的 CMMC 要求，始釋出訂單，數家台灣供應商也因此出線入選為美國國防供應鏈的廠商，適當地於合規的風險與機會中取得平衡而獲取商機，確為可喜之事。據此，台灣隨著地緣政治大環境變動，軍工產品生產的品質及後續生命週期中維運服務能力的再提升，實與 CMMC 的合規要求息息相關，也提醒國內業者能及早因應，先馳得點。

梁日誠（CISSPI CISSOI CCISMI CCISAI CCISOI PII CCPI CCAI AIMPI FIAAISI FHCA-EU AI Actl CAIEI CDEI CDAI DSFMI CBAEI FHCA-GDPRI GPM-b）現為加拿大 SCC／MC ISO／IEC JTC1／SC42、SC27、ISO／TC22／SC32、IEC／TC65 技術組成員，ISO 42001／ISO 27001／ISO 27701／ISO 22301／ISO 20000-1／IEC 62443-2-1 稽核師及講師，TCIC 環奧國際驗證公司全球營運總經理。