「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