No Time to Lose: Promoting CMMC for Taiwan's Defense Industrial Base

Yi-Suo Tzeng
Assistant Research Fellow

Division of Cyber Security and Decision-Making Simulation
Keyword: supply chain security, CMMC, cybersecurity in the defense industry

Given the success story of foreign aid to Ukraine during the Russo-Ukrainian War, and the shock brought forth by China's military exercises surrounding Taiwan in August 2022, the democratic coalition led by the US has started discussing various preventive coping strategies. Among them military weapon assistance is one issue that has invited heated debates. As there is no D-Day, the idea of starting military weapon transportation N days before D-Day is impossible. Furthermore, proposals ranging from stockpiling weapons and ammunition by countries around Taiwan to advancing loans, to Taiwan for military defense, were met with many obstacles and suspicion.

Until recently, certain like-minded friend proposed the initiative of setting up weapons production lines in Taiwan.[1] The initiative is practical and uplifting, but it's also a mixed blessing. The good news is Taiwan would be well-equipped if the war breaks out, can become part of the U.S. military weapon supply chain, and thereby establish a large-scale military defense industry ecology. On the other hand, the U.S. military defense industry ecology has been implementing the U.S. Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC). If Taiwan wants to become part of the U.S. military weapon supply chain and keep up with the upcoming change, it is imperative to introduce and brace for the CMMC

1. "U.S. Considering Joint Weapons Production with Taiwan," *Reuters*, October 19, 2022, https://www.reuters.com/world/asia-pacific/us-government-considering-joint-production-weapons-with-taiwan-nikkei-2022-10-19/.

practices.

What is CMMC?

Cybersecurity Maturity Model Certification (CMMC) requires protection for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) in non-federal systems to ensure all contractors meet certain cybersecurity standards when they bid for military defense contracts. The U.S. Department of Defense (DoD) stressed CMMC is still a developing program. The CMMC Model is notional until rulemaking is completed. CMMC 1.0 was officially released on November 30, 2020, consisting of five levels. CMMC 2.0 was released on November 17, 2021. It trims the number of CMMC levels from five to three. As shown in the figure, since October 25, 2022, the three levels are no longer classified as Foundational, Advanced, and Expert.[2] According to the Defense Federal Acquisition Regulation Supplement (DFARS), the controls of Controlled Unclassified Information, published by the National Institute of Standards and Technology (NIST), are required to comply with NIST Special Publication 800-171 for the protection of Controlled Unclassified Information in non-federal systems and organizations, and NIST SP 800-172 if Level 3 Certification is required.[3] The CMMC revolves around the defense acquisition contract system, and the recognition of defense acquisition contract certification levels is issued by the Defense Contract Management Agency (DCMA) of the U.S. Department of Defense. Except for the defense supply chain manufacturers who define their own output information, the scope of the CUI is defined by the buyer of the procurement contract, which is the defense procurement contracting authority.[4]

Why is the U.S. promoting CMMC?

Before the SolarWinds software

2. Please refer to the official website of the Chief Information Officer U.S. Department of Defense for more information on CMMC: https://www.acq.osd.mil/cmmc/about-us.html.
3. Please refer to the official website of the CMMC Accreditation Body (Cyber AB) for more information: https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/DIB-Companies-OSCs.
4. 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/.

supply chain hacking was revealed in December 2020, the U.S. Department of Defense had already started promoting CMMC strongly since the end of November of that year. If we examine the root cause, the major contractors and subcontractors in the U.S. military supply chain have been suffering from foreign cyber-attacks and theft of business secrets for over a decade. Seeing that the Chinese Communist Party (CCP) is not shy to show off their newly-copied American-style weapons, the U.S. government has not only strengthened the protection of physical and cyber confidential information, but also the control of Controlled Unclassified Information, non-confidential information produced, handled, stored, and processed by federal organizations and defense contractors, as such information has become the high-value target of the CCP and other hostile forces, to counter CCP's piecemealapproach intelligence gathering.[5]

On November 4, 2010, the Obama administration issued *Executive Order 13556*, which requires contractors working for the federal government to strengthen physical security and cybersecurity protections for Controlled Unclassified Information per NIST SP 800-171. However, in the face of ineffective implementation, the Obama administration and the CCP reached an agreement in 2015 on not using the Internet for espionage, which was proved futile later.[6] With the complexity of NIST SP 800-171 and absence of the helping hand from significant contractors, it is quite challenging for small and medium enterprises in the defense industry supply chain to comply with the regulations. After the Trump administration embarked on a high-tech decoupling from the CCP, and continued to tighten controls over Controlled Unclassified Information of the defense industry after the Clean Network initiative, the DoD therefore launched CMMC 1.0 to strengthen the security of defense industrial networks. However, there was still a big gap between CMMC

5. "Controlled Unclassified Information," *U.S. DoD CUI Program*, https://www.dodcui.mil/.

6. Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage," *The Washington Post*, September 25, 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

1.0 and Defense Federal Acquisition Supplement and NIST SP 800-171. By the end of 2021, the Biden Administration collected feedback from all parties and continued to update and launch CMMC 2.0. The ultimate goal is to ensure that CMMC remains part of the national security strategy to keep up with the bipartisan consensus between Democrats and Republicans in countering the pacing challenge from the CCP, allowing the U.S. to maintain a leading edge in technology and warfighting capabilities.

Conclusion: What does CMMC have to do with Taiwan?

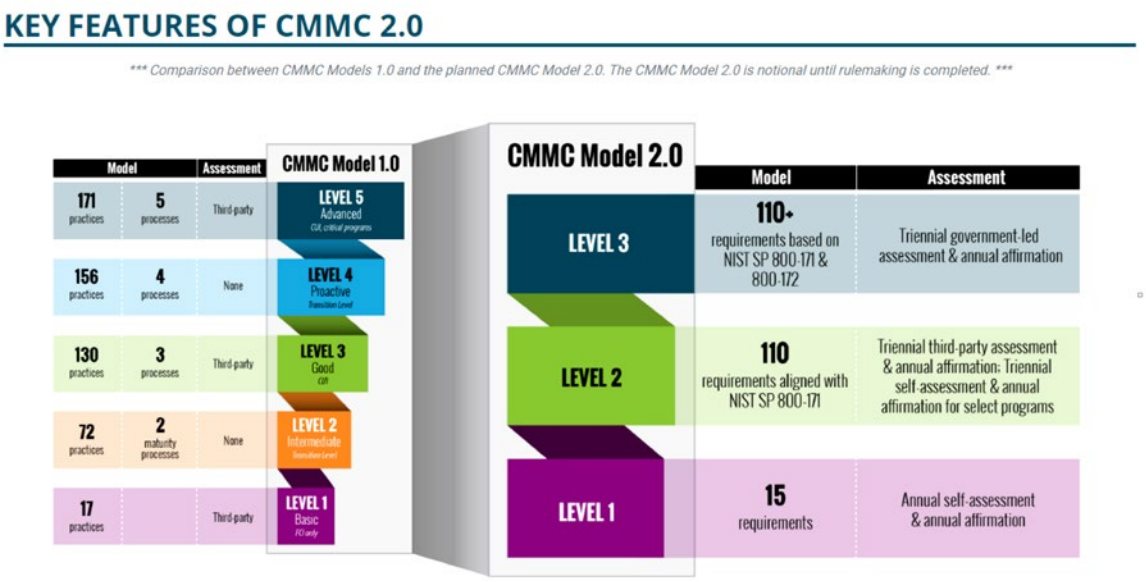
Since its launch at the end of 2020, such Five Eyes members as the UK, Canada, and Australia, together with NATO countries and non-NATO allies such as Japan and Korea, have joined the CMMC one after the other and are actively preparing to keep track with the U.S. defense industry. As the levels and scope of CMMC are decided by defense procurement projects owners, defense procurers in each country play the role of the initiator to enable the introduction and implementation of the CMMC. South Korea has done the most thorough job of copying the U.S. system per its national conditions. The kind of endeavor renders non-NATO allies to single out their position among CMMC-applicable countries and a green light for the export of military weapons embedded with U.S. supported defense technology to Poland during the Russo-Ukrainian War.[7]

Taiwan has been emphasizing "information security is national security" since 2014 and has been actively developing its information security industry. In recent years, various advanced indigenous armaments have been made and entered the test and evaluation stage. After the successful F-16 restructuring and upgrading project, something performed by Hanxiang Aerospace Industrial Development Corporation in Taiwan, Taiwan's defense industry has not only been recognized for its capability but also met the information security and counter-intelligence standards. In that light, the U.S. finally agreed to test-fire

7. 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/.

the U.S. Army's operational Patriot Pac-3 missiles in Taiwan.[8] After all, joining the U.S. defense industry supply chain can help Taiwanese defense manufacturers to expand their market scale and increase profits. Before the CMMC completes its full rulemaking process in May 2023 and full implementation in 2026, Taiwanese defense manufacturers must accelerate their pace to meet the CMMC threshold.[9] To keep in line with "information security is national security," Taiwan may consider to follow the example of South Korea under the leadership of the relevant units

Fig. Compare CMMC2.0 vs. CMMC1.0



Source: "About CMMC," *Office of the Under Secretary of Defense for Acquisition & Sustainment*, https://www.acq.osd.mil/cmmc/about-us.html.

8. Zhu Ming, "Taiwan-US Military Breakthrough: The U.S. Agrees to Test-fire Patriot Pac-3 Missiles in Taiwan for the First Time; Procurement of Extended-range MSE Missiles to be Completed in Batches in 2025 and 2026," *Up Media*, November 2, 2022, https://www.upmedia.mg/news_info.php?Type=24&SerialNo=158005.
9. Zheng-Han Luo, "U.S. Department of Defense Launched CMMC 2.0 to Establish New Cybersecurity Maturity Standard for Defense Supply Chain Networks," *iThome*, March 3, 2022, https://www.ithome.com.tw/news/149664.

of the Ministry of National Defense to work seamlessly under the framework of CMMC. Doing so will accelerate the U.S. decision-making to install weapons production lines in Taiwan, given the lesson learned from the Russo-Ukrainian war. With all the emerging thoughts and a pretty tight schedule, Taiwan should step up preparation without delaywhile taking discrete, solid steps in the right direction.

(Originally published in the "National Defense and Security Real-time Assessment," November 11, 2022, by the Institute for National Defense and Security Research.)

(The contents and views in the assessments are the personal opinions of the author, and do not represent the position of the Institute for National Defense and Security Research.)