William Blair

CMMC 2.0 Set to Materially Expand Cyber and Regulatory Compliance Market

The U.S. government is preparing new cybersecurity rules that will drive most of the 220,000-plus companies that contract with the Department of Defense (DoD) to seek compliance help from third parties, bolstering a nascent and fragmented ecosystem of service and software providers that are primed for investment.

Industry Commentary

Josh Ollek
+1 704 969 1583
jollek@williamblair.com

Gordie Vap
+1 704 969 1581
gvap@williamblair.com

B.T. Remmert
+1 470 351 6927
bremmert@williamblair.com

Cooper Bradley
+1 704 969 1789
cbradley@williamblair.com

Peer and near-peer adversaries continue to invest heavily in next-generation technologies, prompting the federal government to heighten its regulatory focus on securing the Defense Industrial Base (DIB)[1]—particularly related to intellectual property (IP), advanced technology, and information security. This focus has manifested itself as a set of rules, known collectively as Cybersecurity Maturity Model Certification (CMMC) 2.0, which are expected to go into effect in 2025 and rapidly scale the market for third parties that provide CMMC assessments from $56 million to $3.5 billion by 2031.[2]

The reworked federal standards will go beyond classified programs to also include Controlled Unclassified Information (CUI)[3] in an effort to safeguard information that may not be classified but is, nonetheless, sensitive, including certain trade data. Defense contractors and subcontractors will need to demonstrate the "maturity" of their cybersecurity programs in compliance with the new standards, based on their level of CUI access.[4] As a result, prime contractors will not only be held responsible for ensuring their own compliance but that of their sub-contractors.

The growing need for third parties to perform CMMC assessments is likely to spur investment in the expanding ecosystem of CMMC consultancies that service DoD contractors. That presents an opportunity for financial sponsors to execute either a buy-and-build or roll-up strategy given the current size and fragmentation of the existing consultancies landscape.

In the following report, William Blair's aerospace, defense, and government services team in collaboration with Arnovia, a premier provider of transaction and growth strategy services to the Aerospace, Defense, and Government Services markets, outline the evolving threat landscape, the new regulatory reality for contractors, the rise of third parties that support compliance, and investment opportunities in the third-party universe.

The Next-Generation Threat Landscape

America's biggest rivals are actively stealing its IP and national security secrets as they attempt to close the capability gap between nations. In 2016, a Chinese citizen was found guilty in the U.S. of being involved in a "conspiracy originating in China, to illegally access sensitive military data, including data relating to military aircraft" during the same time China was developing two stealth fighters—the J-20 (which resembles the American F-22) and the FC-31 Gyrfalcon (which resembles the

1. A vast network of contractors, suppliers, and service providers that work with the Department of Defense and handle sensitive information.
2. Source: Detail from Federal Register, DoD, and Arnovia analysis.
3. Information the government shares with contractors as part of the work process.
4. Source: Federal Register, "Cybersecurity Maturity Model Certification (CMMC) Program, A Proposed Rule by the Department of Defense," December 26, 2023.

American F-35).[5] In 2021, a federal jury convicted a Chinese intelligence officer of "attempting to steal industry-leading aviation trade secrets … related to GE Aviation's exclusive composite aircraft engine fan."[6] According to the DoD, China "uses its cyberspace capabilities, not only to support intelligence collection against U.S. academic, economic, military, and political targets, but also to exfiltrate sensitive information … to gain economic and military advantage."[7]

In 2022, FBI Director Christopher Wray said that China's sophisticated hacking program was "bigger than those of every other major nation combined" with the U.S. being its chief target.[8] But China is far from the only threat. Russia is utilizing a variety of cyber tactics to identify security weaknesses and access the DIB supply chain at the contractor level. In recent years, the FBI, NSA, and CISA have all "observed regular targeting of U.S. cleared defense contractors … and subcontractors."[9]

To implement a uniform cybersecurity standard across its vast supply chain, the DoD announced the development of CMMC in 2019, preceding the 2020 launch of CMMC 1.0. As the latest standard update, CMMC 2.0 is far more expansive and will greatly impact companies trying to access DoD business opportunities.

A New Reality for Contractors

CMMC broadly aligns with the DoD's Zero Trust Strategy, which aims to "reduce the attack surface, enable risk management and effective data-sharing in partnership environments, and quickly contain and remediate adversary activities" by 2027.[10] As a result, defense contractors will need to adopt and are, in fact, moving toward a "Zero Trust" posture to thwart accidental insider threat exposure. Given the recent regulatory trend lines, many contractors are becoming increasingly comfortable turning to third-party experts for compliance assistance, the installation and management of access and identity controls designed to satisfy Zero Trust requirements, and on matters related to the Federal Risk and Authorization Management Program (FedRAMP) and the National Institute of Standards and Technology (NIST).

Put another way, there is greater understanding among DoD contractors that spending money is increasingly necessary to stay compliant. This will certainly be true when CMMC 2.0 begins to take effect, but it is likely to happen sooner, as preparing for the new rules will require significant organizational effort, especially with the compliance processes that can take about a year.

While the risk of non-compliance is high, the cost to mitigate risk and comply with regulation is certainly material. Some contractors likely do not realize just how vulnerable they are to cyber threats, or non-compliance with regulations, given inconsistent adoption of commercial technologies and "Shadow IT"—i.e., the employment of third-party IT services providers who may or may not use compromised technology or protocols without the knowledge of a company's IT or security staff. To understand the pervasive nature of the threats, and the extent to which CMMC 2.0 will address them, consider this: Showing documentation considered "Not Releasable to Foreign Nationals" to someone on an overseas support desk would violate the new requirements.

Under CMMC 2.0, contractors will be required to submit compliance affirmations at least once a year.[11] This presents potential liability under the False Claims Act, particularly for prime contractors managing the contracts of greatest scale as well as various sub-contractor relationships. That provides additional incentives for businesses to employ third parties to assist with compliance and mitigate risk in their attestations. For smaller companies not affected by CMMC 2.0's more stringent requirements, accreditation could still serve as a competitive advantage in working with DIB businesses that might traffic in sensitive or classified information.

CMMC 2.0 categorizes contractors into three levels (down from five under CMMC 1.0). For the new Level 1 category—i.e., companies that handle comparatively less-sensitive information—self-assessments will be allowed. Still, CMMC-accredited providers can help companies in Level 1 avoid inaccurate self-certifications.

Those in Levels 2 and 3, however, will be required to use certified third-party assessor organizations (C3PAO)[12] to perform audits. Level 2 covers nearly 77,000 DIB companies and must meet 110 requirements in those assessments. Level 3, which covers about 1,400 companies, must meet Level 2 requirements and others from the NIST in government-led assessments. These processes will involve utilizing a qualified third-party to conduct a CMMC audit that precedes the preparation of documents necessary for CMMC assessments.

The Three Levels of CMMC 2.0[13]

	Model	Frequency / Assessor
Level 3 Expert	**110+ security requirements** based on NIST SP 800-172	Triennial Government-Led Assessment
Level 2 Advanced	**110 security requirements** aligned with NIST SP 800-171	Triennial C3PAO Assessment
Level 1 Foundational	**17 security requirements**	Annual Self-Assessment

5. Source: U.S. Department of Justice, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information," March 23, 2016.
6. Source: U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China," October 19, 2023.
7. Source: Ibid.
8. Source: Remarks by FBI Director Christopher Wray, "Countering Threats Posed by the Chinese Government Inside the U.S.," January 31, 2022.
9. Source: CISA, "Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology," February 16, 2022.
10. Source: U.S. Department of Defense, "Department of Defense Releases Zero Trust Strategy and Roadmap," November 22, 2022.
11. Source: Federal Register, "Cybersecurity Maturity Model Certification (CMMC) Program, A Proposed Rule by the Department of Defense," December 26, 2023.
12. An independent entity authorized and certified by the Cybersecurity Maturity Model Certification Accreditation Body (CMMC-AB) to conduct assessments and audits of organizations seeking CMMC compliance.
13. Source: Federal Register, "Cybersecurity Maturity Model Certification (CMMC) Program, A Proposed Rule by the Department of Defense," December 26, 2023.

The Rise of Third-Party Support for CMMC 2.0

The increase in the market for assessors—from $56 million in year one to $3.5 billion by 2031, as noted above—represents a compound annual growth rate of almost 100%.[14] That increase stems from the planned phased rollout of the assessments—not all contractors will be assessed in year one—and the required triennial reassessments thereafter for some contractors. These projected costs only cover assessment, planning, and reporting, as the actual implementation of security requirements is covered under other federal regulations.

The universe of CMMC assessment providers has many smaller providers that have already begun preparing to scale in parallel with the new regulations. But there will also be a boom in highly specialized small businesses—focusing on CMMC compliance—creating a dynamic, evolving market with significant rollup opportunities. As of November 2023, there were approximately 50 authorized C3PAOs with more than 450 applications pending from additional companies seeking certification.[15]

With additional regulation beyond CMMC 2.0 highly likely in the years ahead given the evolving threat landscape, the strong demand for third-party support shows no signs of abating. Other opportunities for third parties that serve DIB contractors are clear as well, including providing gap assessments and ongoing maintenance to support maintaining CMMC compliance and commercial application beyond CMMC, notably non-DIB companies and institutions interested in applying similar cybersecurity standards. Third parties can further improve their chances of success by acquiring appropriate scale through customer acquisition and drive cost savings by investing in automation tools, particularly differentiated software solutions. This will present opportunities in the form of capital and transaction experience for strategic partnerships with financial sponsors.

CMMC 2.0 Overview[17]

Goal
Expand protections of sensitive information shared by the Department of Defense (DoD) with its contractors and subcontractors

Timeline
Proposed rule published in December 2023 and public comment period closed in February 2024; phased rollout to begin in early 2025, with full integration by 2028

Companies Affected
More than 220,000 companies in the Defense Industrial Base (DIB)

Companies Most Affected
Nearly 77,000 companies that handle more sensitive information (Levels 2 and 3)

CMMC Compliance Addressable Market Expansion
$56 million, growing to $3.5 billion by 2031

Investment Opportunities

There also are several areas investors can explore for opportunities related to the CMMC changes: the C3PAO space, adjacent services providers capable of implementing C3PAO audit findings, and developers producing SaaS tools to assess and monitor compliance. All of these opportunities will scale alongside the seven-year phased rollout of CMMC 2.0. The number of DIB contractors being assessed will peak in year seven as the rollout of the requirements is complete across companies and triennial assessments come due again.

Importantly, providers of CMMC services and solutions principally interface with government contractors, not the government itself. This reduces exposure to the risks associated with compliance requirements, the requirement to interface with multiple authorities to consummate a sale, and other quirks specific to government contracting, like delayed payments or the risk of contract protests. C3PAOs also do not need to create government-focused business development functions, which are typically staffed by expensive mid- to late-career professionals.

Thus, purchasing a CMMC-focused services provider effectively enables the buyer to create a "synthetic long" on federal digital modernization that captures the benefit of selling to the government, an evergreen customer with a large budget for IT modernization, while reducing many of the common disadvantages of government contracting including working with actual government.

Threats, Regulations, and Recurring Revenue

CMMC 2.0's triennial reviews and assessments will present a constant compliance burden on DIB contractors. Other macro factors contribute to the evolving threat landscape, another reason contractors will likely rely on third parties for ongoing management of internal systems and necessary updates to remain in compliance.

The demand for third-party services appears stable, given bipartisan federal support for spending on IT modernization—as well as the overwhelming likelihood that regulations will increase given the ever-increasing cyber threats directed at the U.S. To provide some perspective, the number of those threats is already quite high, as China alone prompts the FBI to open new cases prompted by intelligence operations from that country every 12 hours.[16]

Importantly, the defense industry is—to a certain extent—acyclical, which means that qualified third parties that assist with CMMC compliance may not be subject to the same macro trends that impact other cybersecurity or technology-oriented enterprises. These companies support customers that perform mission-critical work for the national defense, thus ensuring consistent demand for their services.

This is the third article in our series on National Security Technology and the first written in conjunction with the transaction and growth strategy advisors at Arnovia. To learn more about CMMC opportunities, please do not hesitate to contact William Blair or Arnovia.

14. Source: Detail from the Federal Register and Arnovia analysis. These totals do not include the cost of implementing Level 2 requirements.
15. Source: Cyber AB, "CMMC November Town Hall," November 28, 2023.
16. Source: Remarks by FBI Director Christopher Wray, "Countering Threats Posed by the Chinese Government Inside the U.S.," January 31, 2022.
17. Source: Detail from the Federal Register and Arnovia analysis. Addressable market expansion totals do not include the cost of implementing Level 2 requirements.