CMMC – A CALL TO ACTION

It is time for a cyber risk reality check that includes cyber vigilance

We are at a cyber risk inflection point. As the attack surface expands, and the attack vectors increase, the defense community is searching for cyber solutions.

That means DIB businesses of all types and sizes need a solid cyber risk management plan – because it makes good business sense – not solely because it is a regulatory or contractual obligation.

Our legislatures, regulators, and institutes adopt laws, regulations, standards, and frameworks to find cyber solutions that stop the onslaught of cyberattacks and the theft of valuable intellectual property and information.

Yet, we are failing to keep cyberattacks at bay. Do you have cybersecurity measures in place? Do you have robust cyber insurance to help you respond to and mitigate a cyber incident?

It is time for a cyber risk reality check that includes cyber vigilance as part of our business DNA. That is what the CMMC is trying to accomplish.

Cybersecurity Maturity Model Certification (CMMC)

Cyberattacks on supply chains are well-documented and on the rise, especially during COVID-19. The US government is intent on minimizing supply-chain threats and cybersecurity risks.

The Cybersecurity Maturity Model Certification (CMMC) establishes cybersecurity as a foundation for future Department of Defense (DOD) acquisitions.

Protected Information

CMMC aims to protect two kinds of information:

- Federal Contract Information (FCI): FCI is information provided by or generated for the Government under

contract not intended for public release. The CMMC model uses the basic safeguarding requirements for FCI as the Federal Acquisition Regulation (FAR) Clause 52.204-21 and the security requirements for CUI as specified in NIST 800-171 / DFARS.

- Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls according to and consistent with laws, regulations, and government-wide policies, excluding classified information under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

CMMC Levels of Cybersecurity Maturity

Prime contractors and subcontractors must protect their networks and demonstrate compliance via five levels of certification of cybersecurity maturity – depending on the nature of the contract – aligning a set of processes and practices with the type and sensitivity of the information to be protected.

The Challenge for Prime Contractors

The challenge for prime contractors to be awarded DOD contracts is two-fold:

- First, they must comply with the CMMC maturity level relevant to the goods and services that they contract to sell to the DOD.
- Second, primes must confirm that their subcontractors have been certified in their appropriate CMMC maturity level.

Is the CMMC too burdensome for the DIB to follow?

Fedscoop indicates that the CMMC, applicable to 300,000 contractors in the DIB, is one of the most significant, most complicated projects in the Defense Industrial Base (DIB) – which provides everything from advanced aircraft to shoelaces in soldiers' boots.

The report adds that officials from the DOD Cyber Crime Center are concerned about expanding our attack surface when nation-states target the military via vulnerable defense contractors, some of which are ill-prepared small businesses.

Part of the cyber risk reality check may be to assure that the CMMC assessment process does not sacrifice innovation for security through the loss of participants. Finding the right balance will be a work in progress.

CMMC Accreditation Body

In June 2020, the volunteer CMMC AB opened the application process to third-party assessment organizations (C3PAOs), the umbrella organizations tasked with hiring and managing individual certified professionals and assessors, the experts who will perform the cyber assessments of DOD vendors.

CMMC Audits

As reported in National Defense Magazine, highly anticipated audits related to the Pentagon's new CMMC process are inching closer, with auditors assigned to assess companies expected to complete their training by the end of September 2020.

Katie Arrington, Chief Information Security Officer in the Office of the Undersecretary of Defense for Acquisition and Sustainment, and the DOD's point person on CMMC, presented at the Department of the Navy Gold Coast Small Business Procurement Event (i.e., webinar) on September 2, 2020. Arrington said, "We'll be starting to get some provisional assessors out into the marketplace very soon."

As a point of clarification, Arrington noted that while Requests for Proposals (RFPs) with the new cybersecurity rules inserted are expected in **November 2020**, the industry would not have to be compliant until the time of contract award.

"Your company will still have the time and the opportunity to get certified," she said. "We're hoping that industry jumps in as soon as we get these provisional assessors out there, [and that] companies start requesting to get their CMMC certification sooner rather than later to position themselves in an environment to be successful."

Additionally, Arrington said, **assessments will be good for three years and will apply to all the work a company does with the DOD.**

The Pentagon had originally planned to have assessments conducted in-person, but Arrington said some parts of that would have to be done online due to the ongoing COVID-19 crisis.

According to Arrington, in or by fiscal year:

- 2021, the Pentagon plans to have 15 contracts with CMMC rules included, involving about 1,500 companies, with 895 at Level 1, 149 at Level 2, 448 at Level 3, four at Level 4, and four at Level 5.
- 2022, the Pentagon plans to have 75 contracts with a CMMC requirement involving 7,500 additional companies.
- 2023, there will be 250 contracts involving 25,000 companies.
- 2024 and 2025, there will be 479 contracts involving 47,905 companies.
- 2026, all new DOD contracts are expected to contain the cybersecurity requirement.

DFARS Rule Change Delayed – Prerequisite to CMMC Applications

In May 2020, Arrington noted, that we will not see the CMMC in any DOD contracts or RFPs until after the rule change.

In September 2020, Arrington confirmed that the DOD would delay the changes to the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, needed before implementation of CMMC certification, with a public comment period until November 2020 -- which could push the final regulation out to 2021.

Compliance with DFARS 252.204-7012 and demonstrating implementation of security requirements in the National Institute of Standards and Technology (NIST) Special Publication 800-171 are the current regulations applicable to the DIB for storing, transmitting, and processing defense information.

Keep in mind that once CMMC requirements launch in late 2020 or early 2021, defense contractor self-attestation

of cybersecurity compliance will be gone.

In the meantime, acquiring Stand-Alone Cyber Insurance, with the cyber assessment needed to do so, could be a differentiator in the CMMC certification process.

Stand-Alone Cyber Insurance

Cybercriminals are intent on using the ever-expanding attack surface by accessing your mobile devices, computer systems, or networks as your employees work from home, remotely, in the office, or on a job site.

Hackers seek to steal critical data, such as FCI, CUI, or PII, or to shut down your operations to extort ransom, or to trick your employees into transferring funds to a fake bank account.

Have you prepared for how to respond to dynamic attack vectors, such as Maze ransomware attacks?

With the help of Stand-Alone Cyber Insurance, you can protect your balance sheet and project:

- If you suffer a data breach – you can obtain support from an incident response team. The team will implement the incident response plan, e.g., help you stop the breach, conduct a forensic investigation, notify all those impacted, recover or restore your data, use public relations to maintain your brand, and possibly defend third-party liability claims or lawsuits for damages by injured parties.
- If you suffer a ransomware attack – you can obtain support in negotiating the ransom demand and be compensated for the ransom payment (made with the prior written consent of the insurer).
- If you experience business interruption from a cyberattack – you can be compensated for lost profits, and extra expenses such as payroll, during the downtime (after a brief waiting period and during a restoration period).
- If you experience funds transfer fraud – you can obtain support in recouping some of the funds as well as compensation for the unrecovered funds.

Stand-Alone Cyber Insurance is a Win-Win – first, you win by investing in the services provided in most policies, and second, you win by investing in the coverage provided when faced with a claim or lawsuit for damages.

Takeaways

- The cyberattack surface has expanded. Are you prepared?
- The cyberattack vectors are dynamic. Are you prepared?
- A holistic cyber risk management plan is the new foundation of government contracts, including both cybersecurity and cyber insurance.
- Your business needs specialist advice from a broker and carrier dedicated to providing comprehensive cyber insurance appropriate for your specific cyber risk tolerance.
- The Cyber Armada Insurance team, in conjunction with its specialist network, is here to help you as you seek to win government contracts.

Reach out to a specialist cyber broker, such as Cyber Armada Insurance, to request cyber solutions appropriate for your needs and cyber risk tolerance. We understand the evolving demands and expectations of cyber insurance clients.

Contact Cyber Armada today to examine your company's potential financial losses from a cyberattack. Contact us at 888.727.6232.

CYBER ARMADA
INSURANCE

888.727.6232 | info@cyber-armada.com | www.cyber-armada.com