CMMC UPDATE IN CYBERSPACE

The Cybersecurity Maturation Model Certification is on schedule

The 300,000 companies in the Defense Industrial Base (DIB) need to be mindful that implementation of the Cybersecurity Maturity Model Certification (CMMC) is on schedule despite the COVID-19 public health crisis.

The Department of Defense (DOD) is moving forward with the implementation of CMMC.

Prime contractors and subcontractors in the supply chain must remain vigilant during these troubled times because hackers have increased their cyberattacks:

- Phishing emails attacks have increased.
- Ransomware attacks have increased.
- Data breaches while ransom payments are pending have increased.
- Social engineering resulting in funds transfer fraud has increased.

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), taking effect in fall 2020, establishes cybersecurity as a foundation for future DOD acquisitions. Government suppliers must go through a third-party audit to become certified to work at progressively higher levels of DOD contracts. The auditors are known as CMMC Third Party Assessment Organizations or C3PAOs.

CMMC Protection of FCI and CUI

CMMC aims to protect two kinds of information:

THE US GOVERNMENT IS INTENT ON MINIMIZING SUPPLY-CHAIN THREATS AND CYBERSECURITY RISKS

- **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.

The Five Levels of CMMC

In late 2020, the DOD is scheduled to assign levels of cybersecurity maturity for DIB contractors to obtain Cybersecurity Maturity Model Certification (CMMC) and win specific government contracts.

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

- **Level 1:** Safeguard Federal Contract Information (FCI)
- **Level 2:** Serve as a transition step in cybersecurity maturity progression to protect CUI.
- **Level 3:** Protect Controlled Unclassified Information
- **Level 4-5:** Protect CUI and reduce risk of Advanced Persistent Threats

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.

These obligations will require due diligence, with the help of legal counsel, to decrease the risk of losing the DOD contract bid.

CMMC Updates & Timeline

Since our recent article on CMMC, Katie Arrington Chief Information Security Officer (CISO) for the Office of the Under Secretary of Defense for Acquisition (OUSDA) for the Department of Defense (DOD), served as a keynote speaker during Potomac Officers Club's CMMC Virtual Forum on June 24, 2020.

Following the release of the CMMC guidance, Arrington has announced her support for the regulation and commented on how the **shift from the National Institute of Standards and Technology (NIST) standards** will affect both the public and private sectors.

Arrington noted that the certification has been in progress for 18 months. She reassured the audience that COVID-19 would not have drastic changes in the implementation process. “We do not have another day to wait,” she said.

In preparation for the certification implementation, Arrington discussed the various ways the DOD has prepared for integration, including pathfinders, requests for information (RFI), and training the **CMMC accreditation body (AB).**

“Pathfinders are current contracts from the DOD that we are working through to map from the primes to the subs. We are doing that with contracts with NDA. We’ve gone in to look at the contractors and their level of security to complete these contracts,” Arrington said.

As she discussed the RFIs, she noted that a level **3 certification would require an in-person audit.** Arrington elaborated on the ways COVID-19 has presented new issues with the auditing process due to social distancing and the new regulations that have become the “new normal.” However, once the auditors graduate in approximately a month, DoD will release RFIs.

After addressing the auditing process, Arrington dissected how DOD plans to allocate pricing for CMMC. She noted that if companies participate in pilot programs, then the government will cover the costs of the auditing process. She did also note that it will not be attributional.

The non-attributional audit means that the company cannot own the level of certification that it has attained through the pilot audit process. They can only use it for the one contract they had audited. While the audit will not have long term effects, Arrington said that it would provide companies with a test run for the official CMMC implementation and audit process.

“The pilot audits can be used as a tool for preparation and modification, but when it comes to the RFP, you will have to get an audit that your company pays for that you will own for three years,” Arrington specifically mentioned.

Also, Arrington discussed the role that the AB will play in business and acquisitions. At the same time, there have been concerns revolving around the auditors (C3PAOs) creating challenges, and, as a result, creating a loss of revenue. Arrington confirmed that the AB would work with industry to create “a model that works equally.”

“We have worked so hard to ensure that the system treats organizations equally and fairly and that the process has an adjudication baseline. Two auditors should be able to look at the same information and get the same conclusions,” Arrington expanded. “You absolutely have the right to have a different auditor come in if you disagree with the conclusions from the initial audit.”

Arrington noted that you do not have to have a CMMC certification until the time of a particular contract award. However, she added that it is imperative to prepare for CMMC ahead of time.

“Do not wait on CMMC. If you have the DFAR rule on your contract, then you are self-attesting that you are doing 110 of those controls, so do not wait,” she emphasized.

In May 2020, Arrington noted that changes to the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 are being carried out and could be finalized in October. “You will not see the CMMC in any Department of Defense contracts or RFPs until the rule change is completed,” Arrington said.

Thus, the completion of the pending DFARS rule change is a prerequisite to CMMC application.

Currently, DOD contractors use the self-attestation of adherence to requisite cybersecurity practices.

Cyberspace Solarium Commission Report

The Solarium Report establishes the need for cyber insurance.

The bipartisan Cyberspace Solarium Commission (CSC) was established in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyberattacks of significant consequences." The well-written finished report entitled “A Warning From Tomorrow” was presented to the public on March 11, 2020.

The CSC proposes a strategy of layered cyber deterrence. The CSC report consists of over 80 recommendations for implementation, including several relating to insurance:

- A federally-funded center to develop cybersecurity insurance certifications
- A public-private partnership on cyber risk models and
- A government reinsurance program to cover catastrophic cyber events.

The insurance recommendations suggest that the US government needs to step in because the insurance industry is failing on its own to provide financial incentives for better cyber risk management:

Can Modern Insurance Improve Cybersecurity?

Insurance can provide financial incentives for individuals and organizations to manage their risk better. From incentivizing the use of seatbelts and airbags in the automotive industry to pushing for fire suppression systems as a part of building codes, the insurance industry has played an essential role in identifying risk management standards

for individual consumers and large corporations alike. A robust and functioning market for cyber insurance could play a similar role in determining and regulating behavior to improve cyber risk management."

The report goes on to say, that cyber insurance is failing to deliver on this potential -- due to a lack of underwriting and claims talent, insufficient risk models, and silent cyber risk in other insurance offerings -- all leading to hesitancy on the part of insurers to assume meaningful amounts of cyber risk.

Indeed, this idea of cyber risk management and the yin and yang between cybersecurity and cyber insurance is an ongoing discussion in the markets that will not likely be resolved in the short term. It is encouraging to see this high-level report tackle the crux of the matter.

Nevertheless, we advise primes and subs to tackle the need for dedicated Stand-Alone Cyber Insurance now, without delay, as you move forward in the CMMC process.

Stand-Alone Cyber Insurance

Your company can survive disruption caused by cybercriminals attacking or accessing your mobile devices, computer systems, or networks to steal critical data or to shut down your operations.

With the help of Stand-Alone Cyber Insurance to protect your balance sheet and project budget, you should be aware:

- If you suffer a data breach, your business will need to:
    - Stop the breach
    - Conduct a forensic investigation
    - Notify all those impacted
    - Recover or restore your data
    - Use public relations to maintain your brand
    - 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 funds that are not recovered

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

Cyberattack vectors are ever-evolving, dynamic, and varied – which may allow hackers to bypass current cybersecurity defenses.

- A holistic cyber risk management plan is the new foundation of government contracts, including both cybersecurity and cyber insurance
- Since we have no immediate guarantee of a government cyber insurance solution, your company 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