CMMC – An international perspective

Positioning Paper:

Cyber Maturity Model Certification (CMMC). The challenges and opportunities for contractors in complying with US DoDs requirements

By:

Andy Watkin-Child CSyP, CEng, MSyI, MIMechE, AMAE

Chartered Security Professional (CSyP) and Chartered Engineer (CEng), Advisory Board Member CMMC Center of Excellence (CMMC CoE), Board Member of the Security Institute, counsel appointed expert and Founding Partner Parava Security Solutions.

Why CMMC?

According to the US Government Accountability Office's(GAO) Defence Acquisition Annual Assessment report[1] (June 2020). The US Government plans to invest $1.8Trn in new and current weapon systems such as aircraft, ships, and satellites. Activities which create, modify, and manufacture new and existing technologies and Intellectual Property (IP) across many diverse digital platforms. Platforms which are exposed to cyber threats.

In 2016 the DoDs Office of the Undersecretary of Defence for Acquisition & Sustainment (OUSD A&S) modified DFARS 48 CFR § 252.204-7012[2] (Safeguarding covered defense information and cyber incident reporting) regulations. To regulate the protection of systems and networks that process, store, or transmit "covered defence information" and Controlled Unclassified Information (CUI). Compliance with DFARS 48 CFR § 252.204-7012 requires a company to identify and protect the CUI data it creates, processes and stores. Assess and apply security controls to the NIST (SP) 800 – 171 standard and self-attest their effectiveness. Visible losses of Intellectual Property (IP) through cyber-attacks, data breaches and reports of IP stolen by Nation States compounded the view that IP created across the US Defence Industry Base (DIB) supply chain needed stronger protection. It is no surprise that concerns were raised over compliance to DFARS 252.204.7012 regulations, the application of NIST (SP) 800 – 171 and self-attestation.

To address these issues the DoD raised a formal DFARS case 2019 - D041 'Strategic Assessment and Cybersecurity Certification Requirements'[3]. Initiating the CMMC process for implementing a methodology to assure and accredit DoD contractor compliance, against NIST (SP) 800 – 171 and the protection of Controlled Unclassified Information (CUI) in Non-federal systems and organisations. It is expected that DFARS will be modified in Qtr. 4 2020 to include the appropriate CMMC amendments, with regulatory approval being sort shortly after. For the independent oversight and assurance of compliance to NIST (SP) 800 – 171 cyber security standards.

Cyber-attacks have tangible and intangible effects on the DIB, government agencies and society. They impact a contractor's financial statements and competitive advantage. A GAO National cyber study[4] in 2018 identified the challenges cybersecurity had on the US in 2017 and the actions required to address them. By way of example the economic impact of cyber-attacks on the US was estimated by the Council of Economic Advisers in their 2018 report[5], published by the Office of the President of the United States. That the cost of malicious cyber activity on the US economy in 2016 was between $57Bn and $109Bn.

CMMC, applicability and scope?

For companies across the DIB NIST (SP) 800 – 171 compliance will be on the corporate radar. Compliance to NIST (SP) 800 – 171 has been a requirement for 3 years but unlike its predecessor the CMMC will be extended to include both Federal Contract Information (FCI), covered by 48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems[6] and CUI. CMMC proposes to remove the current self-attestation process and formalise the independent and accredited assessment of cyber security compliance and assurance by accredited and certified 3rd party assessment organisations (C3PAOs) and assessors. Companies who contract with the DoD will be required to be certified to a CMMC maturity level (level 1 – 5) set by DoD procurement.

The CMMC programme is a data led initiative focusing on the security of IP as defined by FCI and CUI. As the US DoD DIB is global, from primes through flow down to subcontractors. CMMC will have a global reach and impact DoD contractors outside of the US.

Note

1. https://www.gao.gov/assets/710/707359.pdf
2. https://www.law.cornell.edu/cfr/text/48/252.204-7012
3. https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf
4. https://www.gao.gov/assets/700/693405.pdf
5. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
6. https://www.law.cornell.edu/cfr/text/48/52.204-21

Whilst the total number of companies impacted by CMMC is not known exactly, estimates of 300,000 – 350,000 are discussed. If the DFARS regulation is amended as expected to include CMMC, maturity level requirements will be included in new RFPs quickly and will impact all DIB contractors by 2024. E.g. The US General Services Administration(GSA) STARS III programme has reserved the right to request CMMC certification for their $50Bn government wide IT contract for disadvantaged small businesses (July 2020).

CMMC implications for consideration by the international DIB?

The defence supply chain is complex, comprising many tiers of contractors. Including organisations which manufacture complex weapon systems, provide maintenance services for DoD facilities, maintenance services for equipment sold to partner nations and R&D contracts within academic and corporate research environments. In all cases creating, processing, storing, and/ or consuming FCI and/ or CUI related data and information. Current DFARS 252.204 – 7012 requirements and the proposed changes have cyber security implications and opportunities for the DIB.

Regulation and oversight

- DFARS 48 CFR § 252.204 - 7012 (CUI flow down). Irrespective of the implementation timelines for CMMC, contractors and subcontractors are obliged to apply the CUI security requirements as laid out in NIST (SP) 800 - 171 under DFARS 252.204 – 7012 (paragraph m). Contractors are required to ensure that their subcontractors are securing covered defence information, maintaining assurance over the security of CUI and incident reporting.

  Current DFARS regulations present several challenges for global primes and for US regulatory oversight.
  - CUI can reside in multiple geographic locations on different systems. Making it difficult to track and trace.
  - The NIST (SP) 800 - 171 security standard maybe different to existing cyber security standards applied to secure data belonging to other clients. Creating security tiers.
  - Contractors may produce products or deliver services for multiple nation states. Who often have different security requirements regarding privacy and security?
  - At present only US citizens are being trained to assess CMMC. Subcontractors outside of the US will have local security controls which may prevent US citizens from performing security assessments. Reciprocity between countries will be required.

- Federal Acquisition Regulation (FAR) Clause 48 CFR § 52.204-21. The proposed CMMC Changes will bring FCI into CMMC scope, requiring the implementation of a security programme to identify and secure FCI appropriately.

Legal

- Contractual obligations. DFARS 252.204 - 7012 is an existing requirement, which can be assessed under applicable contracts. For an organisation which suffers from a cyber-attack and data breach within its contractual timeframe, it could bring into consideration whether they have failed their contractual obligations, to secure CUI and FCI.
- False Claim Act (FCA). Current DFARS regulation for NIST compliance requires organisation to self-attest their compliance to NIST (SP) 800 – 171. CMMC will require an independent assessment and accreditation. For organisation which do not meet the appropriate maturity level, it could raise questions related to self-attestation and whether the organisation met the standards expected at the time of self-attestation. Two recent legal cases have tested cybersecurity compliance relating to DFARS 252.204 - 7012 and the False Claims Act (FCA).

See *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., et. Al*[7], and United States ex rel. Glenn v. Cisco Systems, Inc., No. 1:11-cv-00400- RJA (W.D.N.Y. July 31, 2019)[8] have started to test the application of DFARS 252.204 – 701 in court.

Implementation

- CMMC as a competitive differentiator. CMMC provides an opportunity for an organisation to differentiate itself and create competitive advantage. E.g. a company who has attained ML 3 CMMC may in the eyes of the DoD to be more secure and a more appropriate contract partner?
- Brand and reputational damage. When CMMC is documented within DFARS, an organisation which fails to meet the necessary CMMC standards will not be awarded applicable DoD contracts. An organisation which suffers a cyber-attack will be judged by its shareholders and customer against its CMMC compliance.
- Other contracting opportunities. Successful compliance with DoD CMMC may be seen favourably by other agencies?
- Cost of compliance, contract value and shareholder value. Cybersecurity and managing cyber risk is a cost of doing business and securing financial statements requires the adoption of appropriate security standards**.** Cybersecurity is expensive, companies who wish to achieve and maintain CMMC will initially have to balance the cost of compliance, against contract value.

Conclusion.

The CMMC programme should be of no surprise to companies within the US DIB. Its forerunner defined the cyber security requirements to protect CUI. The real and significant difference between what is currently in place and the proposed CMMC, is one of assurance and accreditation. For those companies who already comply with DFARS 252.204 – 7012 and NIST SP 800 – 171, CMMC compliance will be straightforward. For those which currently do not comply or do not know if they will comply, then the process for CMMC, cybersecurity and cyber risk management will be more challenging. CMMC sets 5 levels of cybersecurity maturity, detailing a cumulative number of security practices and maturity capabilities, to be applied to both FCI and CUI. For a level 3 certification applied to an international organisation, a robust and compliant cyber risk management programme can take more than 18 months to design and deliver.

Cyber risk is a complex global[9] and expensive non - financial risk to manage. A risk which is well documented to impact both the top and bottom line with high implementation, legal, compliance, revenue, sales, brand, reputation, and incident costs. Cyber implementation programmes and cyber incidents impact P&L, balance sheet, cashflow as well as share price and market perception. There are examples of listed organisations being downgraded following cyber-attacks (Equifax[10]) and the costs attributed to attacks, in some cases more than $10Mn[11] and others $100Mn[12].

But rather than looking at CMMC as a compliance programme. CMMC should be considered as a standard which an organisation adheres to secure its financial statements, protects its IP and that of the DoD, albeit the appropriate level of compliance must be met.

Note

7. https://www.govinfo.gov/app/details/USCOURTS-caed-2_15-cv-02245
8. https://thewhistleblower.com/wp-content/uploads/2019/08/James-Glenn-Cisco-Video-Surveillance-FCA-Complaint.pdf
9. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
10. https://www.forbes.com/sites/kateoflahertyuk/2019/05/28/equifax-becomes-first-firm-to-see-its-outlook-downgraded-due-to-a-cyber-attack/#7210abe45671
11. https://www.insurancejournal.com/news/international/2019/07/24/533763.htm
12. https://www.forbes.com/sites/leemathews/2017/08/16/notpetya-ransomware-attack-cost-shipping-giant-maersk-over-200-million/#67f7e3d44f9a