CMMC – The DFARS balancing act

Cyber Maturity Model Certification (CMMC). The DFARS D041 balancing act and the Interim Final Rule

By:

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

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

By:

Curt Parkinson, CAP

Security Assessment and Authorization Certification (CAP), expert and Founder of Cyber CATalina.

The requirement for a Cybersecurity Maturity Model Certification (CMMC) programme was initiated through DFARS case 2019 - D041 'Strategic Assessment and Cybersecurity Certification Requirements' [1]. Implementing a standard methodology for assessing DoD contractor compliance to NIST SP 800 – 171 and the CMMC certification process. Which will ultimately be reflected in DFARS 252.204-7012 - Safeguarding covered defense information and cyber incident reporting [2]. Initiating the implementation of the CMMC Accreditation Body (CMMC AB), as the institution for managing accreditation and assurance of the CMMC standard.

An Interim final rule in response to DFARS case 2019 - D041 was published on the 17.09.2020[3,4] by the Office for Information and Regulatory Affairs, Office of Management and Budget (OIRA). It raises several interesting and pertinent questions relating to the CMMC process and oversight and assurance of Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Firstly, the rule is defined as an interim final rule. Taking a quote from the US Governments Federal Register on rule making [5] 'Interim final rules are put in place when an agency finds that it has good cause to issue a final rule without first publishing a proposed rule, it often characterizes the rule as an interim final rule , or interim rule.' The interim rule will go for public consultation, it may get modified, upon which it will be released as final. This is expected to take place before the end of 2020.

OIRAs findings. The content of the 'Interim Final Rule' needs careful consideration by contractors. (Appendix 1 - Abstract: Final rule RIN: 0750-AK81 (17.09.2020)). As a result of the rule, contractors must be prepared to address several DoD requirements, the rule sets out that contractors are currently required to provide adequate security to protect CUI, as defined in DFARS 252.204-7012 through the application of NIST SP 800 – 171. This rule requires (amongst other things) that contractors will be required to review their system security plans and provide an implementation self-assessment to DoD in accordance with the scoring methodology. With a score which reflects the net effect of security requirements not yet implemented.

Following which the DoD reserves the right to review a contractors System Security Plans (SSPs), conduct interviews and clarify the implementation of their security plans to place a level of assurance and confidence over a contractor's implementation of NIST SP 800 – 171. For very critical systems, DoD may request an on-site validation/demonstration to ensure a high level of confidence with the implementation of NIST SP 800-171 requirements, whether the assessment is conducted by the contractor or by DoD, the same scoring methodology will be used. The rule further discusses and clarifies the intention of the DoD to implement the Cybersecurity Maturity Model Certification (CMMC) programme. The assessment of CMMC maturity by an independent 3rd party assessor and the verification of NIST SP 800 – 171 practices to ensure compliance of practices prior to the awarding of a contract.

The rational for releasing the Interim Final rule so quickly is documented in their emergency justification (Appendix 2. OMB Control number 0750-0004: Emergency Justification). The DoD wants to immediately begin assessment of the compliance to NIST SP 800 – 171. It is DoDs view that contractors have not been complying with the standards, the DoD view is that contractors have not 'fully or consistently' applied NIST SP 800 – 171 security requirements on their covered information and by authorising the collection of information it will incentivise contractors to identify their current compliance to DFARS 252.204-7012, the application of NIST SP 800 – 171 and close any gaps in compliance.

Implications of the Interim Final rule? Contractors and subcontractors within the Defence Industry Base will have to assess their compliance to NIST SP 800 – 171, using a standard DoD methodology. This assessment methodology will be the existing assessment methodology applied by DCMA following their DIBCAC [6] process, which the OUSD (A&S) directed DCMA to pursue with companies for which they administer contracts.

The assessment methodology is based on three categories Basic, Medium, and High assessments. The Basic is based on a Self-Assessment of the contractor's system security plan which is conducted in accordance with the NIST 800-171A. The Medium assessment conducted by DoD personnel who are trained in accordance with DoD policy and procedures. The final level of assessment and the most intense is the High. This assessment is conducted by DoD personnel who are trained in accordance with DoD policy and procedures, this level will require an on-site or virtual verification/examination and demonstration of the contractor's system security plan and implementation of the NIT 800-171.

This is not an easy task, there will have to be an assessment to the 110 NIST controls, associated assessment criteria and an evaluation of the level of compliance, associated gaps, and remedial actions. One which should already have been made by contractors who maintain contracts covered by DFARS 252.204.7012, which the DoD believes has not been completed fully or consistently by DoD contractors. An assessment given the previous regime of self-assessment may prove challenging, especially given contractual obligations, CUI flow down and large complex defence programme with complex CUI data regimes. With the associated challenges of understanding, identifying, tracking, and marking CUI and appropriately securing covered defence systems.

The implications of compliance to DFARS 252.204-7012 compliance remains unchanged. If 7012 is contractually applicable, then compliance with NIST SP 800 – 171 and the 110 identified practices applies. The Interim Final Ruling will require contractors to evaluate their SSPs and provide a formal evaluation to the DoD as to their compliance using a DoD self-assessment methodology. With the potential for interviews and onsite visits made by the DoD to assess critical systems. It will therefore be important that the NIST compliance assessments are carried out appropriately and to an appropriate standard and be prepared for onsite visits and assurance assessments. Like any 'audit' they could be rigorous, evidential and attention will be have to be paid to compliance and remediation plans e.g. security requirements not implemented, whether a plan of action is in place or not, will be assessed as not implemented, as will the partial implementation of security requirements.

The economic challenges of compliance are self-evident and apply whether there is a NIST DoD assessment or a CMMC assessment. The final ruling unfortunately pulls these decisions to the left as the DoD will be looking for compliance data sooner rather than later. DIB contractors will need to evaluate compliance, close existing gaps in compliance across the 110 practices and ensure that their SSPs are fit for purpose across their organisations and between themselves and their subcontractors. As DFARS 252.204-7012 section (m) prescribes DFARS contractual flow down for the protection of CUI it could mean that assessments have to take place across broad and deep supply chains.

The ruling allows contractors to plan and progress with compliance for NIST SP 800 – 171 ahead of CMMC changes. Organisations can 'baseline' compliance and put in place remedial actions to improve compliance. If finalised the ruling will require the submission of compliance data, which has obvious implications in terms of quality and accuracy. Given CMMC will require an onsite assessment at a later date the baseline data submitted could be used to 'balance' the DoD assessment with a CMMC assessment and raise questions, if there are any significant differences identified incompliance between the two assessments and historical self-attestation.

Conclusion. The interim ruling as it relates to DFARS Case 2019 – D041 provides the first formal response to the request to implement CMMC. In the authors view it is a reasonable stepping-stone for the DoD to take in deploying what will be a complex cyber security programme. The interim ruling allows for the collection and assessment of DFARS 252.204-7012 compliance, specifically the implementation of NIST SP 800 – 171. Utilising an existing assessment standard, which one assumes will be the DoD Assessment Methodology (DAM) created by DCMA and the DoD CIO.

It allows the DoD to request NIST SP 800 – 171 compliance data, following a contractor assessment and allows contractors, who by the DoDs admission, may not be complying with existing regulations the chance to comply.

But there is a balancing act here and it may not be two sided. It may be more complicated, how to balance between complying the 110 NIST practices, historical self-attestation, and the economic challenges with closing the gaps which may exist in compliance. These challenges will be there under CMMC, the major difference is that the assessment process is still managed by the contractor and subcontractor, albeit the DoD reserves the right to independently review information and complete interviews. The assessment methodology if it is the DAM, DCMA and DIBCAC process is already known.

There are some complex decisions which need to be made and these maybe better discussed between legal, procurement, security, and the board today rather than waiting.

Note

1. https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf
2. https://www.law.cornell.edu/cfr/text/48/252.204-7012
3. https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202009-0750-001
4. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202004&RIN=0750-AK81
5. https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf
6. https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html

Appendix.

1. Abstract – Final rule: RIN: 0750-AK81 (17.09.20) – (https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202004&RIN=0750-AK81)

'DoD is proposing to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a standard DoD-wide standard methodology for assessing DoD contractor compliance with all security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations and a DoD certification process, known of cybersecurity practices and processes. Currently, DFARS clause 252.204-7012, Network Penetration and Safeguarding of Covered Defense Information, requires contractors to provide adequate security for controlled unclassified information for which the minimum requirement is to implement the security requirements in NIST SP 800-171. The DoD standard methodology validates contractor implementation of the security requirements in NIST SP 800-171 in a consistent and objective manner. As a result of this rule, contractors will be required to review their system security plans and provide an implementation self-assessment to DoD in accordance with the scoring methodology. The score reflects the net effect of security requirements not yet implemented. Depending on the criticality of the data, DoD may also choose to review the system security plans, get additional information from the contractor through interviews, and ask for clarification in the plan by the contractor. For very critical systems, DoD may request an on-site validation/demonstration to ensure a high level of confidence with the implementation of NIST SP 800-171 requirements. Whether the assessment is conducted by the contractor or by DoD, the same scoring methodology will be used. CMMC is a DoD certification process that is intended to serve as a mechanism to ensure appropriate cybersecurity practices and processes are in place to ensure basic cyber hygiene, as well as protect CUI residing on DoD's industry partners' networks. CMMC assessments take into consideration various cybersecurity controls/requirements/standards, including NIST SP 800-171, while also measuring the maturity of a company's institutionalization of these cybersecurity practices and processes. Information on CMMC and a copy of the draft CMMC model can be found at https://www.acq.osd.mil/cmmc/index.html. CMMC assessments will be primarily conducted by independent third parties. Upon completion of a CMMC assessment, a company is awarded certification at the appropriate CMMC level (as described in the CMMC model) and the certification level is documented in SPRS to enable the verification of an offeror's certification level prior to contract award.'

2. OMB Control number 0750-0004: Emergency Justification – (https://www.reginfo.gov/public/do/PRAViewICR?ref_nbr=202009-0750-001)

'This collection of information is needed prior to the expiration of the time periods normally associated with a routine submission for review under the provisions of the Paperwork Reduction Act, to enable the Department to immediately begin assessing the current status of contractor implementation of NIST SP 800-171 on their information systems that process CUI. Defense contractors have not fully or consistently implemented the NIST SP 800-171 security requirements on their covered information systems. Authorizing collection of this information on the effective date will motivate defense contractors and subcontractors who have not yet implemented existing NIST SP 800-171 security requirements, to take actions to implement the system security requirements on covered information systems that process controlled unclassified information. The aggregate loss of sensitive controlled unclassified information and intellectual property from the DIB sector could undermine U.S. technological advantages and increase risk to DoD missions.'