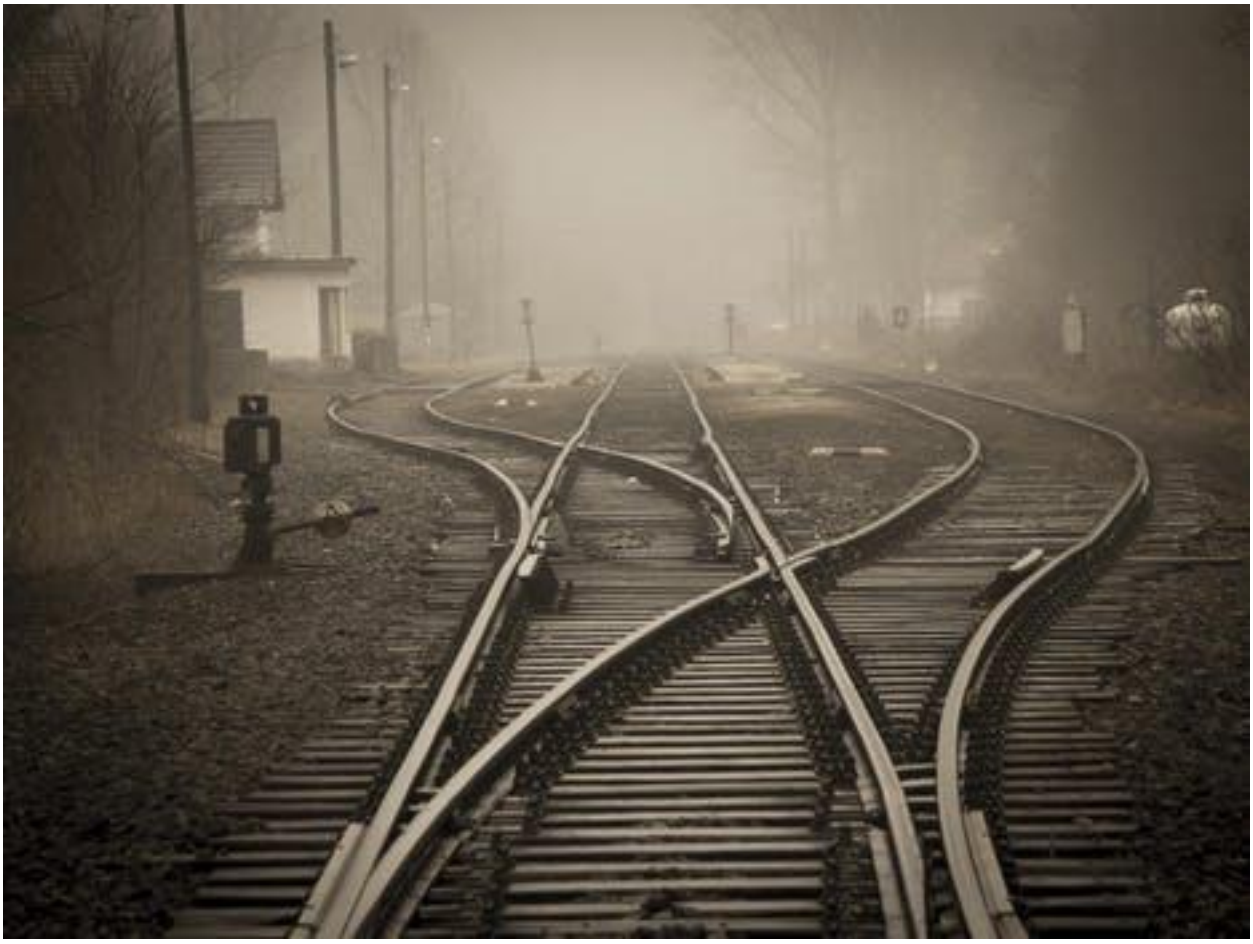
PARAVA
CYBER CONSULTING

DFARS Case D041 Interim Final Ruling (IFR)



A complex road ahead for the international DIB and the deployment, oversight, and assurance of NIST SP 800 – 171 and CMMC

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.

Note: The following is not a legal interpretation of the ruling. It is advised that General Council review both the Interim Final Ruling[1] and Associated Regulatory Impact[9]

Introduction. The US Department of Defence (DoD) spends a significant amount of money on defence innovation, the Government Audit Office (GAO) report published in June 2020 identified approximately $1.8TRN USD[1] allocated to the research development and manufacture of air, land and sea weapon systems. All Nation States rely on digital solutions for offensive and defensive capabilities and the global Defence Industry Base (DIB) to design, manufacture and service those defence systems. The digital revolution and what some call the 5th industrial revolution is playing an increasingly important role in the differentiation of weapons systems and National Defence, so much so that the protection of defence Intellectual Property (IP) from cyber-attack is a high priority for the US DoD. In an effort to prevent the leakage of IP from their supply chain, the DoD mandated implementation of NIST SP 800 – 171 security practices through DFARS Clause 252.204 – 7012. This clause and the required security practices were to have been implemented by the end of 2017 and was intended to protect the category of IP named as Controlled Unclassified Information (CUI). A requirement which did not have the desired affect at protecting defence IP at the time, which has been addressed subsequently and discussed in this paper.

On 29th of September 2020 the DoD published the much anticipated ruling on DFARS Case 2019 – D041[2]. Releasing an Interim Final Ruling (ruling) to enhance the protection, oversight, and assurance of DoD data. The ruling has a 60-day window for public consultation with an effective date of the 30th November 2020. It is an important ruling for the US DoD Defence Industry Base (DIB), cyber security, legal and procurement professionals. Setting a precedence for cyber security, implementing a standard which has global reach and direct economic influence on the DIB and the countries in which they are located. The ruling addresses the failings to secure critical defence information including defence IP, which is managed through Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). In this paper we explore the requirements and implications which the ruling sets out from a cyber security perspective, and the potential impact to the international DIB.

In 2016[3] the final rule was published to update DFARS 252.204-7012 which included the requirement for the protection of CUI in Nonfederal systems. Adopting at a minimum the NIST SP 800 – 171 standard, to be applied no later than the 31st December 2017. This rule required all contractors and subcontractors to apply appropriate security practices to protect Controlled Unclassified Information (CUI) residing in contractor information systems and report cyber incidents that affect those systems to the DoD. Also included was the mandatory flow down of NIST SP 800 – 171 from contractors to subcontractors at all appropriate levels where CUI was created, consumed, and managed in the supply chain. The premise of which was not in the main followed and did not achieve its stated goals of protecting CUI. Initiating the DFARS case D041, which the ruling released on the 29th of September 2020 addresses.

DoD assessment methodology and CMMC. The ruling sets out a 2-part approach, which work in parallel to address the oversight and assurance of contractor and subcontractor compliance for the protection of CUI and FCI data across the DIB. It introduces both the DoD Assessment Methodology[4] and CMMC framework[5].

- DoD Assessment Methodology. In February 2019, the Office of the Under Secretary of Defence for Acquisitions and Sustainment (OUSD A&S) directed the Defence Contract Management Agency (DCMA) to develop a standard methodology to assess contractor implementation of the requirements in NIST SP 800 – 171. This methodology produces a consistent measure scoring model which is intended to be used and accepted by multiple US government agencies. A methodology, as described in DoD Assessment Methodology version 1.2.1, which contractors may use to assess the implementation status of NIST SP 800 – 171 of their subcontractors.
- CMMC Framework. Section 1648 of the National Defense Authorisation Action for Fiscal year (FY) 2020 (Pub L. 116-92)[6] directed the Secretary of Defence to develop a cybersecurity framework for the DIB sector Resulting in the CMMC as the basis for a mandatory DoD standard. The aim of the CMMC framework is to build upon the NIST SP 800 - 171 DoD Assessment Methodology through independent assurance and oversight. Adding scalability and certification to verify that contractors have implemented NIST SP 800 – 171 to a level appropriate to the data and information which they process, the size and complexity of their business and that of the contracts which they process on behalf of the DoD and contractors in their supply chain.

Part 1. NIST SP 800 – 171. The ruling amends DFARS subpart 204.73 'Safeguarding Covered Defence Information and Cyber Incident Reporting' to implement the DoD assessment methodology. It directs contracting officers to verify that if an offeror is required to implement NIST SP 800 – 171 (pursuant of DFARS 252.204-7012), that they must have a DoD assessment on record in the Supplier Performance Risk System (SPRS)[7]. This requires contractors to apply the DoD assessment methodology for the oversight and assurance of compliance to the existing DFARS clause 252.204 – 7012, when

it has been applied to solicitations and contracts. Additional DFARS clauses have been created by the ruling to be included by a contracting officer in solicitations and contracts. Clause 252.204 - 7019 sets out the requirement for those contractors who are required to implement NIST SP 800 – 171 to have a DoD assessment on record in SPRS (which is no more than 3 years old) to be considered for an award. Clause 252.204 - 7020 requires contractors to ensure that applicable subcontractors have the results of a current DoD assessment posted in the SPRS system, prior to the awarding of a subcontract or 'other contractual instrument'. Clause 252.204 – 7020 will require contractors to provide the Government access to their facilities, systems and personal when necessary for the DoD to conduct or renew medium or high-level DoD assessment, defined below.

The DoD assessment methodology is to be used by contractors, subcontractors, and DoD personnel to assess NIST SP 800 – 171 compliance, basic, medium, and high. Calculating the net effect of compliance to the 110 practices documented within NIST SP 800 – 171. These levels are:

- Basic – Contractors are required to complete a self-assessment of their compliance to the 110 security practices in NIST SP 800-171. Based on a review of the system security plan(s) associated with covered contractor information system(s), conducted in accordance with NIST SP 800-171 DoD Assessment Methodology (current version 1.2.1). It calculates a net impact score of practice compliance.
- Medium – A NIST SP 800-171 assessment will be conducted by DoD personnel and consist of a review of the System Security Plan(s) and how the 110 defined requirements have been met. Identifying descriptions which may not properly address the security requirements. It is anticipated that the assessment is conducted as part of a separately scheduled visit.
- High – An assessment will be conducted by DoD personal and involve a thorough onsite visit or virtual assessment. It will involve a verification/ examination/ demonstration of the System Security Plan and implementation of the 110 NIST 800 – 171 security requirements.

The results of the basic, medium and high-level DoD assessment are to be documented in SPRS and available to all of Government for use in their procurement actions. Once posted, these scores are visible to the assessed organization and their existence is to be confirmed prior to awarding a contract.

The DoD assumes that the burden of the basic level self-assessment will be low for contractors and subcontractors. Their positioning is that the requirements for compliance have been in place and tested through self-attestation since the DFARS 252.204 - 7012 clause was to have been fully implemented by the end of 2017. However, the reality is likely that many organizations are still working to complete the 110 security practices. Where requirements have not yet been implemented, they are to be documented in their System Security Plans and Plans of Action (POAs).

Medium and high - level assessments will be intrusive. A medium assessment will review the company's System Security Plan and descriptions of how each requirement is met to evaluate compliance to the 110 security requirements and may require an onsite visit. For both medium and high - level assessments contractors and subcontractors will be required to substantiate their basic assessments, provide evidence of compliance and system testing in line with their System Security Plan(s) and Plans of Action. With the results of both medium and high-level assessments being input into SPRS by the DoD

Basic, medium and high - level assessment are conducted using NIST SP 800 - 171A 'Assessing Security requirements for CUI' and will review appropriate evidence and/or demonstration of compliance (e.g. recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication).

Part 2. CMMC – CUI and FCI. The CMMC framework builds upon the DoD Assessment Methodology deployed in Part 1. It structures CUI and FCI protection into 5 levels of security maturity. Oversight and assurance of FCI data protection is defined at CMMC level 1, in line with FAR 52.204 – 21. CMMC level 2 is an intermediate compliance level for contractors and subcontractors who process FCI and wish to bid for contracts containing CUI, progressing to level 3. CMMC level 3, 4 and 5 are applied to contractors and subcontractors processing CUI, utilising the 110 NIST SP 800 – 171 security practices as a foundation from level 3. CMMC requires security practices to be institutionalised by the contractor and subcontractor with 5 levels of maturity compliance (ML 1, 2, 3, 4 and 5) applied at corresponding CMMC levels. Evaluating that practices are performed (level 1), documented (level 2), managed (level 3), reviewed (level 4), and optimised (level 5).

The ruling creates a new DFARS subpart 204.75 Cybersecurity Maturity Model Certification (CMMC), directing contracting officers to verify in SPRS that a contractors or subcontractors CMMC certification is current and meets the appropriate level prior to making the award.

Incrementally each CMMC level (1, 2, 3, 4 and 5) requires compliance to an increasing number of practices and an increase in associated maturity. To achieve compliance a company must demonstrate both institutionalisation of maturity and deployment of the practices to achieve the appropriate CMMC level certification.

CMMC Level	Security Practices	CMMC Practices	Maturity Processes	Regulation/ Standard
1	15	-	1	FAR 52.204–21
2	65	7	2	NIST SP 800–171
3	110	20	3	NIST SP 800–171
4	110	46	4	NIST SP 800–171
5	110	61	5	NIST SP 800–171

Table 1: Security practices and maturity processes applied at each CMMC level

A new DFARS clause 252.204-7021, 'Cybersecurity Maturity Model Certification Requirements' is prescribed for use in all solicitations and contracts or task orders or delivery orders but phased in over the next five years. It requires contractors to obtain a CMMC certification at the level defined in the solicitation prior to contract award. They must also maintain that CMMC level for the duration of the contract and ensure that its subcontractors have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments. Similar to the other clauses, this clause includes the requirement of flow down of the clause in all subcontracts or other contractual instruments.

DoD also notes in the ruling that they do not expect to award any contracts at Level 2. They expect the majority of the DIB to be either Level 1 (FCI) or Level 3 (CUI).

CMMC assessments will be conducted by Certified 3rd Party Assessor Organisations (C3PAO), accredited by the CMMC Accreditation Body (CMMC - AB). The CMMC - AB will maintain accreditation assessments, reports, issue CMMC certificates and distribute these to the DIB contractors ~~for~~ and input into SPRS. Contractors will be required to flow down appropriate CMMC certification requirements to subcontractors through contractual arrangement, albeit further clarity will be required on FCI flow down (if applicable) and the implication on micro purchases. DIB contractors that do not process, store, or transmit CUI must obtain a minimum level 1 CMMC certification. CMMC level 1 practices are mapped with clause FAR 52.204-21 requiring the Basic Safeguarding of Covered Contractor Information Systems by all government contractors. DIB contractors and subcontractors who process, store, or transmit CUI must achieve CMMC level 3 or higher. From 1st October 2025, the DoD expects that CMMC will be fully implemented and will apply to all business entities that are awarded a DoD contract (other than Commercial of The Shelf products (CoTS) and those below the micro purchase threshold).

As stated previously, the ruling assumes that contractors should have already implemented the security requirements documented within both FAR 52.204 - 21 and DFARS 252.204 – 7012 and contractors and subcontractors have deployed the appropriate security requirements. Therefore the 15 basic FAR and 110 NIST SP 800 - 171 practices have been implemented or where there are identified gaps an appropriate remediation plan is in place via the POA. It is worth noting, however, that CMMC certification requires that all items within the POA be completed.

The ruling makes changes to existing DFARS sections and creates new provisions and contract clauses. The original DFARS clause 252.204-7012 sets out clearly the requirement to protect CUI and flow down the clause to subcontractors. The addition of the DoD NIST SP 800 – 171 assessment methodology and CMMC within the ruling require amendments to:

- DFARS 212-301 - Solicitation provisions and contract clauses for the acquisition of commercial items. To document changes in the DFARS clauses associated with the DOD assessment methodology and CMMC.
- DFARS 217.207 - Exercise of options. To advise contracting officers that an option may only be executed after verifying the contractors have a summary level score of a current NIST 800-171 DoD assessment or the appropriate CMMC level, when CMMC is in the contract.

Creating new DFARS rules

- DFARS clause 252.204-7019. Notice of DoD assessment requirements.
- DFARS clause 252.204-7020. Granting DoD permission to conduct medium/high assessments.
- DFARS clause 252.204-7021. Cybersecurity Maturity Model Certification requirements

These amendments and new rules are aimed at enabling the DoD to assess contractor compliance of the security requirements in DFARS 252.204 - 7012 and NIST SP 800 – 171. The DoD is also proposing to apply the new provisions and clauses to contracts and subcontracts valued at or below the simplified acquisition threshold[8] (SAT), but greater than the micro purchase threshold and will not apply the rule to CoTS products. Which the author believes will increase the scope of applicability of implementation and required oversight and assurance.

The DoD assessment methodology and CMMC deployment schedule is outlined for cost purposes within the IFR Regulatory Impact Analysis (RIA)[9]. Whilst one must accept is used for costing purposes only, it provides an indication of the deployment plans for both the DoD assessment methodology and the CMMC framework. In case of the application of the DoD Assessment Methodology it is estimated that contracts and orders which contain DFARS 252.204 – 7012 are awarded to 39,204 unique awardees and as such will fall under the DoD Assessment Methodology (Basic, Medium and High). Contracting officers will have to verify that an up to date assessment is on records within SPRS. The DoD has assumed that each year for the next 3 years 13,358 contractors will have to submit a basis NIST SP 800 – 171 assessment to SPRS.

Assessment	Impacted Entities	Year 1	Year 2	Year 3
Basic	Small	8,823	8,823	8,823
	Other than Small	4,245	4,245	4,245
Medium	Small	148	148	148
	Other than Small	52	52	52
High	Small	81	81	81
	Other than Small	29	29	29

Table 2: Expected rollout of DoD assessments over a three-year period

The DoD expects to have fully implemented CMMC by 1st October 2025 following which it will apply to all business entities that are awarded a new DoD contract. Prior to the 1st of October 2025 the DoD plans to add CMMC requirements into selected contracts and phase the deployment of CMMC over 7 years. For costs purposes the DoD has identified the total number of unique prime contractors and subcontractors which will be impacted by CMMC to be 220,966 and the average number of new contracts for unique contractors is 47,905 for any given year. The DoD will identify up to 15 prime contracts which require CMMC in year 1. (For costing purposes, the DoD has assumed that for program there are 100 unique subcontractors).

Prior to the 1st of October 2025 it expects that 129,810 unique entities will be required to have a CMMC certification.

CMMC Level	Total Number of Unique DoD contractors and subcontractors						
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
1	899	4,490	14,981	28,714	**28,709**	28,709	25,919
2	149	749	2,497	4,786	**4,785**	4,785	4,320
3	452	2,245	7,490	14,357	**14,355**	14,355	12,960
4	0	8	16	24	**28**	28	26
5	0	8	16	24	**28**	28	26
Totals	1,500	7,500	25,000	47,905	**47,905**	47,905	43,251
Cumulative to year 5 (2021 – 2025)					**129,810**		

Table 3: CMMC part rollout plan year 1,2, 3 and 4 – prior to 1st October 2025

Although the DoD figures are indicative, the CMMC programme will be deployed across 7 years and will run alongside the DoD Assessment Methodology.

The impact of the ruling on the DIB. The ruling has set a train in motion. Prior to the 30th November 2020 oversight and assurance of FAR 52.204 - 21, DFARS 252.204 – 7012 and compliance to their associated security requirements has been on a self-attestation basis. This has been redressed through the oversight and assurance mechanisms defined in the ruling, impacting contractors and subcontractors which are bound by the contractual requirements of DFARS 252.204-7012 and FAR 52.204-21, and will be bound by the additions of the new DFARS subparts and clauses.

The ruling will have a significant impact on the DoD supply chain. Following a review by the DoD using NAICS codes and awards that included the DFARS clause 252.204 – 7012, there is an expectation that the top 5 industries impacted by the rule will be Research and Development in the Physical, Engineering, and Life Sciences, Engineering Services, Commercial and Institutional Building Construction, Other Computer Related Services and Facilities Support Services. Sectors which are serviced by international contractors and subcontractors and the ruling is explicit in its reference of the role of contractors and subcontractors in providing adequate protection to the storage, processing, and transmission of CUI.

The ruling is complex, the most salient points of consideration from the ruling[1, 9] are that it:

- Assumes that contractors and subcontractors who are required to comply with DFARS 252.204 - 7012 have either implemented the 110 NIST SP 800 – 171 security practices or identified gaps in compliance, assessed against their System Security Plan(s) and covered these by a Plan of Actions..
- Assumes that the cost of CMMC compliance will be minimal and based upon the incremental costs of compliance above the existing requirements mapped to the relevant CMMC maturity level. There will be additional cost element to comply with additional CMMC practices at level 2,3, 4 and 5 as additional CMMC practices are applied.
- Contractors are required to flow down DFARS Claus 252.204 - 7012 to subcontractors through contractual agreements. The result of which is the flow down of CUI related information, the application and oversight of NIST SP 800 – 171 and the appropriate security requirements.
- On formal release of the ruling, contractors and subcontractors processing CUI will be required to submit a current 'basic' assessment of their compliance to NIST SP 800 - 171 (following the DoD assessment methodology) into SPRS, before a new contract is awarded. Contractors will be expected to ensure that applicable subcontractors have submitted their assessments of NIST SP 800 - 171 compliance into SPRS prior to the awarding of a subcontract or other contractual instrument. 'Medium' and 'high' level assessments will be carried out by the DoD personnel, including a relevant programme office and the DCMA.
- The new DFARS clause 252.204 – 7020 will require contractors to provide US government access to their facilities, systems, and personnel when it is necessary for the DoD to conduct or renew a higher-level DoD assessment. DFARS clause 252.204 - 7020 will require contractors to ensure that applicable subcontractors have the results of a current NIST SP 800 - 171 assessment posted in SPRS.
- Upon formal release of the ruling and prior to CMMC programme completion (1st October 2025). If a contract award includes CMMC requirements, a certificate of CMMC compliance for the specified level will be required before the contract is awarded. From the 1st of October 2025, all contractors and subcontractors will require a CMMC certificate of compliance before they are awarded a DoD contract.
- The new DFARS Clause 252.204 - 7021 requires contractors to have a CMMC certification at the level required in the solicitation or contract award and maintain the required CMMC level for the duration of the contract. Including the clause in all subcontracts and ensure that its subcontractors have the appropriate CMMC level prior to awarding a subcontract and include the requirements of the clause in all subcontracts or other contractual instruments.
- In the case where the DoD assessment methodology is used, if a POA is in place for unimplemented security requirements (partial or otherwise) it will result in the security requirement being considered as unimplemented. POAs are not accepted to achieve CMMC compliance.
- Assessments using the DoD assessment methodology and CMMC certifications are valid for 3 years.

Ruling considerations for the International DIB. The US DoD relies on the international DIB for the supply of products and services for research & development, the design and manufacture and servicing of its weapon systems, provision of IT systems and facilities. The international DIB is also dependent upon DoD contracts to provide these products and services. The relationship is symbiotic, economically important and critical for sustaining a robust offensive and defence capability for partner nations, who procure defence systems from the US.

The DIB is international in scope and whilst there are no figures available on the number of international contractors or subcontractors. The nature of global procurement requires the creation, transmission, and storage of CUI data across international boundaries. Data by contractual agreement which must be protected appropriately is contractually defined through several DFARS clauses. These clauses designed to protect data using appropriate security controls and require the oversight and assurance by contractors, subcontractors, government agencies and independent auditors.

In the authors opinion the ruling raises several questions for the international DIB and the DoD, namely:

Regulatory and compliance – International DIB. The regulation will come into force on the 30th November 2020. It may change through public consultation but is unlikely to be substantive. It is important that contractors and subcontractors work together and put a focus on the IFR and compliance, namely:

- Have a clear understanding of the regulation from the contractors and subcontractors General Council, commercial, procurement, technology, and security teams.
- Governance and oversight: DFARS compliance, cyber assessment and CMMC should be a board conversation. It will impact commercial decisions and financial statements, regionally and internationally. The DoD assumes that contractors and subcontractors already comply with NIST SP 800 – 171. That costs to comply have largely already been factored into pricing and therefore not 'new costs' with the exception of CMMC Maturity Levels 4 and 5.
- Start a regulatory review with legal, commercial, procurement, technical and security. Compliance to NIST SP 800 – 171 and CMMC is an enterprise wide issue. Review the implications of compliance to the business strategy and operating model.
- A programme office should be established to facilitate compliance to NIST SP 800 – 171 and CMMC. The DoD assume that contractors and subcontractors already comply with NIST SP 800 – 171.
- DFARS 252.204-7012 requires the flow down, oversight and assurance of the protection of CUI from contractors to subcontractors, through the supply chain. Contractors and subcontractors should be aware of the CUI they create and share, the contractual relationships with subcontractors, and the provisions made in line with NIST SP 800 – 171 to secure that CUI.
- Contractors are responsible for ensuring that their subcontractors recognise their obligations for the protection of CUI using NIST SP 800 – 171 practices and CMMC. Contractor and subcontractor compliance to NIST SP 800 – 171 and CMMC will be assessed for contract award.

Operational – International DIB. There is an assumption running through the ruling that contractors and subcontractors who are required to comply with DFARS 252.204 – 7012 prior to the ruling have deployed NIST SP 800 – 171 practices.

- Contractual arrangements with contractors should clearly recognise and action the appropriate DFARS clauses when dealing with subcontractors.
- CUI flow down is a requirement in DFARS 252.204 – 7012. Contractors and subcontractors should clearly document the CUI which is passed contractually to the subcontractors. Contractors and subcontractors should have appropriate processes and procedures in place to identify, document, mark and secure their FCI and CUI. Both for their own use and for transmitting CUI to their supply chain.
- CUI oversight and assurance. The protection of FCI and CUI is provided by the application of security practices required in FAR 52.204–21, DFARS 204.52-7012, with addition practices added by CMMC. From November 30th 2020, contractors and subcontractors must complete a NIST SP 800 - 171 DoD assessment and potentially a CMMC certification prior to contract award. Requiring an evaluation of the 110 NIST SP 800 – 171 practices (unless the contractor only processes FCI (15 practices))
- Compliance to the ruling will create challenges for the international community namely how to provide oversight and assure CUI protection across international boundaries and jurisdictions. How will a contractor or a CMMC assessor be able to assess compliance?
- Contractors are expected to oversee subcontractors who may be international in location.
- CMMC assessment can only be carried out by US citizens and C3PAOs can only be owned by US Citizens. How will oversight and assurance of DoD assessments and CMMC take place?
- The NIST and CMMC framework sets a standard for cyber security compliance. A benchmark which maybe significantly higher than that set within partner nations and the DIB.
- The medium and high confidence DOD assessments require significant sharing and access to information by DoD personnel. How will international organizations respond to the requirement of US DoD requiring information or access?

References

1. GAO Defence acquisition annual assessment – June 2020
2. Interim Final rule – D041
3. https://www.federalregister.gov/d/2016-25315/p-190
4. DoD NIST SP 800 – 171 assessment methodology
5. https://www.acq.osd.mil/cmmc/
6. https://www.govinfo.gov/content/pkg/PLAW-116publ92/pdf/PLAW-116publ92.pdf
7. https://www.sprs.csd.disa.mil/
8. https://www.law.cornell.edu/cfr/text/2/200.88#:~:text=Simplified%20acquisition%20threshold%20means%20the,than%20the%20simplified%20acquisition%20threshold.
9. Interim Final Ruling D041 Regulatory Impact Assessment (RIA)

About the author. Andy Watkin-Child is a 20-year veteran of cyber security, risk management and technology. He has held international leadership positions in 1st and 2nd Lines of Defence (LoD) for cyber security, cyber risk management, operational risk, and technology. For companies across Engineering and Manufacturing, Financial Services and Publishing and Media. Working with leadership teams of companies with balance sheets over €1TRN. He has been a member of management boards, global risk leadership teams, cyber security, operational risk and GDPR committees. He holds Royal Charters in Security (CSyP), recognised by the UKs , he holds a place on the UKs Register of Chartered Security Professionals and has a Royal Charter in Engineering (CEng) gained whilst working for Rolls-Royce plc. He is am a member of the Board of the Security Institute (MSyI), a Freeman of the Worshipful Company of Security Professionals (WCoSP) and a Freeman of the City of London. He is a counsel appointment expert witness who specialises in risk management and cyber and an Associate of the Academy of Experts (AMAE) a UK register of experts recognised by the UK Legal profession, providing expert advice to companies and support to General Counsel. He is a member of the board of the Security Institute, the UKS largest members only security trade body. He is a member of the CMMC Accreditation Body (CMMC-AB) Standards working group and he is a member of the advisory board of the CMMC Center of Excellence (CMMC-CoE). He if the Founding Partner of Parava Security Solutions, an independent Cyber Risk Management advisory firm, supporting organisations deliver cyber risk management and cyber regulatory programmes. https://www.linkedin.com/in/andywatkinchild/

About the contributor. Matthew Titcome is the founder of Peak InfoSec, Mr. Titcombe left the Department of Defense to reapply his 25+ years of Information Security & Technology experience to the commercial sector. Mr. Titcombe now leads an organization that specializes in Information Security Turn Around efforts supporting federal and commercial sectors. Mr. Titcombe has been brought into consult with organizations across the globe like United Launch Alliance, Sony, ConocoPhillips, Munich Re-Insurance, Nutanix, Toyota Research Institute, and Uber. He also supports contractors in the Defense Industrial Base fulfil their compliance requirements form the Department of Defense. He is also a volunteer for the Cybersecurity Maturity Model Certification (CMMC) Advisory Board (CMMC-AB) and was certified as CMMC Provisional Assessor #17 form the first class oof assessors. Mr. Titcombe also supports two Licensed Partner publishers developing CMMC curriculum. https://www.linkedin.com/in/matthewtitcombe/

About the contributor. Jason Spezzano is an experienced cybersecurity services delivery leader and cybersecurity consultant with expertise in risk management, compliance, and cyber security operations supporting DoD, Federal and Intelligence Agencies. He is skilled in using information security frameworks established by the National Institute of Standards and Technology (NIST) and the DoD Cybersecurity Maturity Model Certification (CMMC). Jason specializes in DoD CMMC, NIST 800-171, and NIST 800-53, and defensive cybersecurity. Jason is a former Major in the United States Marine Corps where he managed the design, installation, maintenance and operation of communication networks and information systems. Jason is the Senior Director of Cybersecurity at Grammatech, as well as a Senior Cyber Security Consultant supporting NIST and CMMC initiatives. Jason is also a Fellow with the Cyber Security Forum Initiative (CSFI). https://www.linkedin.com/in/jason-spezzano-aaa862b/

About the contributor. Kris Carter is VP and CISO at Verify, Inc. (www.verifyglobal.com) where he also oversees the quality and compliance teams. Verify provides supply chain performance management solutions to a majority of the global aerospace & defense industry. His previous roles have included providing technology consulting and management services to a number of small and mid-market companies and their investment teams. Kris earned his Masters of Business Administration from Pepperdine University. He is active with several cybersecurity committees for AIA & NDIA, government/industry working groups, and law enforcement/industry cooperative efforts. More locally, Kris volunteers with emergency response and father-daughter community programs. https://www.linkedin.com/in/kriscarter/