NATO LCMG Workshop

Cybersecurity Maturity Model Certification

The US DoD cyber standard mandated on their global DIB contractors and subcontractors for contract award

26th January 2020, 17:30 – 18:00 CET.

Andy Watkin-Child CEng, CSyP, MSyI, AMAE Version 1.0, January 26th , 2020

TEAM DEFENCE INFORMATION

PARAVA SECURITY SOLUTIONS

The Cybersecurity Maturity Model Certification (CMMC) framework, oversight and assurance

Note:
The following presentation should be considered an expert opinion of the author only, not a legal opinion and not of any government, their agencies, departments or ministries

Agenda

1. Introduction
2. What's driving US DoD cyber Policy?
3. What's driving the CMMC programme?
4. The CMMC Interim Final Ruling
5. The potential impact of the CMMC programme
6. Summary

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

Chartered Security Professional, Chartered Engineer, Counsel appointed advisor

- 25 years of cyber, technology and risk experience across Financial Services, Aerospace and Media. Group VP, CISO, European head Operations Risk, head of IT.
- Group executive committee member.
- Built and grown global 1st and 2nd Lines of Defence regulated functions for cyber security and risk management.
- Chartered Security Professional (CSyP) and Chartered Engineer (CEng). Maintaining a place on the Register of Chartered Security Professionals.
- A Counsel Appointed cyber and risk expert and advisor. Practicing Associate of the Academy of Experts (TAE).
- A member of the Board of the UK Security Institute (MSyI).
- A Freeman of the Worshipful Company of Security Processionals (WCoSP), 108th City of London Livery Company. Freeman of the City of London.
- Member of the Standards Working group of the Cybersecurity Maturity Model Certification - Accreditation Body (CMMC-AB).
- A member of the Advisory Board of the CMMC – Center of Excellence (CMMC-CoE).

What's driving US DoD cyber policy?

- The US Department of Defence (DoD) has plans to invest over $1.8TRN in new weapon systems [1].
- Cyber attacks cost the US economy between $56BN and $109BN (2016 [2]).
- Increased sophistication and success of cyber attacks on the US DIB.
- The increased dependence on digital solutions for the design, manufacture and servicing of new and current defence systems.
- US Cyberspace Solarium commission recommendations [3].
- Cyber attacks and the theft of the DoD Intellectual Property (IP) puts the defence capabilities of the US under threat (GAO 2018) [4].

Cyber is a top priority. SolarWinds and FireEye Hack 2020, the GAO audit on Federal management of supply chain risk [5]

What's driving the CMMC?

- In 2019 the Inspector General of the DOD identified ineffective contractor protection of Controlled Unclassified Information (CUI) [6] using NIST (SP) 800 - 171 [7].
- DFARS 48 CFR § 252.204 - 7012 - Safeguarding covered defense information and cyber incident reporting [8] requiring NIST (SP) 800 – 171 compliance and self-attestation has been in place since December 31st 2017.
- GAO audits in 2018 and 2020 identified significant issues with cyber security. Its impact on the US economy and DIB DFARS compliance.
- A GAO Audit in 2018 [9] identified significant issues with the cyber security posture of weapon systems.

DFARS case in 2019 – <u>D041</u>

'Strategic Assessment and Cybersecurity Certification Requirements [10].

A significant impact to the global DIB, setting an international standard for cyber security compliance

Interim Final ruling – DFARS Case D041 [9]

'Strategic Assessment and Cybersecurity Certification Requirements' - The Interim Final Ruling (IFR) came into effect on the 1st December 2020 making changes to DFARS procurement clauses.

The 2 part ruling

- The IFR sets out a 2 part approach to the security Federal Contract and Controlled Unclassified Information (FCI/ CUI) using NIST (SP) 800 171 and CMMC.
  - **Part 1:** Contractors and subcontractors to assesses their 'basic' compliance to the 110 NIST (SP) 800 – 171 security practices using the DoD Assessment Methodology (DAM) [11] . Input results into the DoD Supplier Performance Risk System (SPRS). Contracting officers will confirm that results are submitted before new award.

    DoD personnel will conduct evidence based 'medium' and 'high-level' assessments, to confirm contractor and subcontractor compliance.
  - **Part 2:** CMMC levels (L1-L5) will be added by the DoD to contracts starting in 2021 [12]. All contractors and subcontractors must hold a CMMC certificate in SPRS at the appropriate 'contracted' level (min. Level 1) before a new award is made.

The potential impact of the CMMC programme - General

- Non compliance could result in no contract award.
- The NIST and CMMC framework sets a high standard for cyber security compliance.
- Compliance creates security challenges for the oversight and assurance of CUI protection across international borders.
- Dependence on US DoD spending could create economic challenges for US partner nations if the DIB fails to comply* i.e. loss of contract awards.
- The US dependency on the global DIB could create challenges for the DoD if US partner nation DIB fail to comply*.
- The lack of cyber aware and cyber skilled resources will hinder cyber compliance.

Note:
* Matter of opinion

The potential impact of the CMMC programme – DIB specific

- CMMC requires all DIB contractors and subcontractors to have a CMMC Level 1 certificate by 1st October 2025 (+250,000 companies).
- The NIST and CMMC framework sets a standard for cyber security compliance. Creating multiple tiers of cyber compliance.
- The cost of compliance is significant, costs the DIB will have to adsorb.
- From December 1st 2020 contractors and subcontractors must complete a NIST SP 800 - 171 DoD assessment and potentially a CMMC certification prior to contract award.
- Plans of Action (POA) in place at the time of the DAM assessment will result in a practice being considered unimplemented. POA are not applicable for CMMC.

Summary

Implications on Lifecycle Management and through life support

- Applies to FCI and CUI data created, stored, transmitted for products and services across the whole product lifecycle.
- Mandates compliance for the protection of FCI and CUI through procurement contracts using DFARS.
- CMMC will be applied to all DoD contracts by October 2025, applicable to contractors and subcontractors (min Level 1).
- Will require an independent assessment of compliance and a CMMC Level certificate before a contract is awarded. Repeated every 3 years.
- The cost of cyber compliance is significant. Deloitte estimated that in 2020 Financial Institutions cyber spend was 0.48% of revenue [13] ,$2,691 per employee on cyber.

CMMC is an integral component of supply chain risk and the Federal Risk Management Framework

Thank you for your interest.

Questions?

andy@parava.org

Definitions and Acronyms

- **CMMC** – Cybersecurity Maturity Model Certification – US DoD procurement cyber security framework.
- **CMMC–AB** – Cyber Security Maturity Model Certification Accreditation Body. Organisation established under MOU by the DoD to manage global CMMC compliance oversight, assurance and training.
- **Cyberspace Solarium Commission** – Established in 2019 under the National Defense Authorization Act to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks
- **DIB** – US global Defence Industry Base.
- **NIST** – National Institute of Standards and Technology - Owner and creator of the NIST suite of cyber security standards including NIST SP (Special Publication) 800 – 171.
- **POA** – Plan Of Action

References

1. https://www.gao.gov/assets/710/707359.pdf
2. https://permanent.access.gpo.gov/gpo89296/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
3. https://www.solarium.gov/
4. https://www.gao.gov/assets/700/693405.pdf
5. https://www.gao.gov/assets/720/711266.pdf
6. https://media.defense.gov/2019/Jul/25/2002162077/-1/-1/1/DODIG-2019-105.PDF
7. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
8. https://www.law.cornell.edu/cfr/text/48/252.204-7012
9. https://www.gao.gov/products/GAO-19-128
10. Interim Final Rule – D041
11. NIST SP 800 - 171 DoD Assessment Methodology
12. CMMC Pathfinder projects announced
13. https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html/#endnote-sup-2

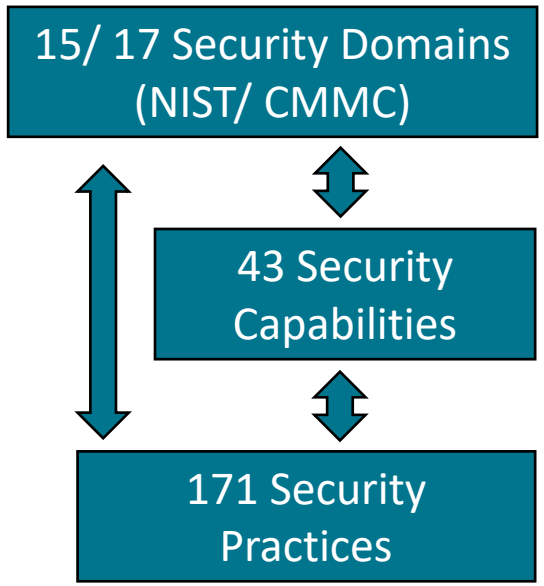
TEAM DEFENCE INFORMATION

PARAVA
SECURITY SOLUTIONS

Appendix

What is the CMMC framework

A framework to regulate the assurance and accreditation of compliance to NIST 800 – 171 for the protection of FCI and CUI for the DoD.



The domains E.g. Access Control, Asset Management, Configuration Management, Incident response, Maintenance, Media Protection, Systems Communications Protection, Systems Information Integrity.

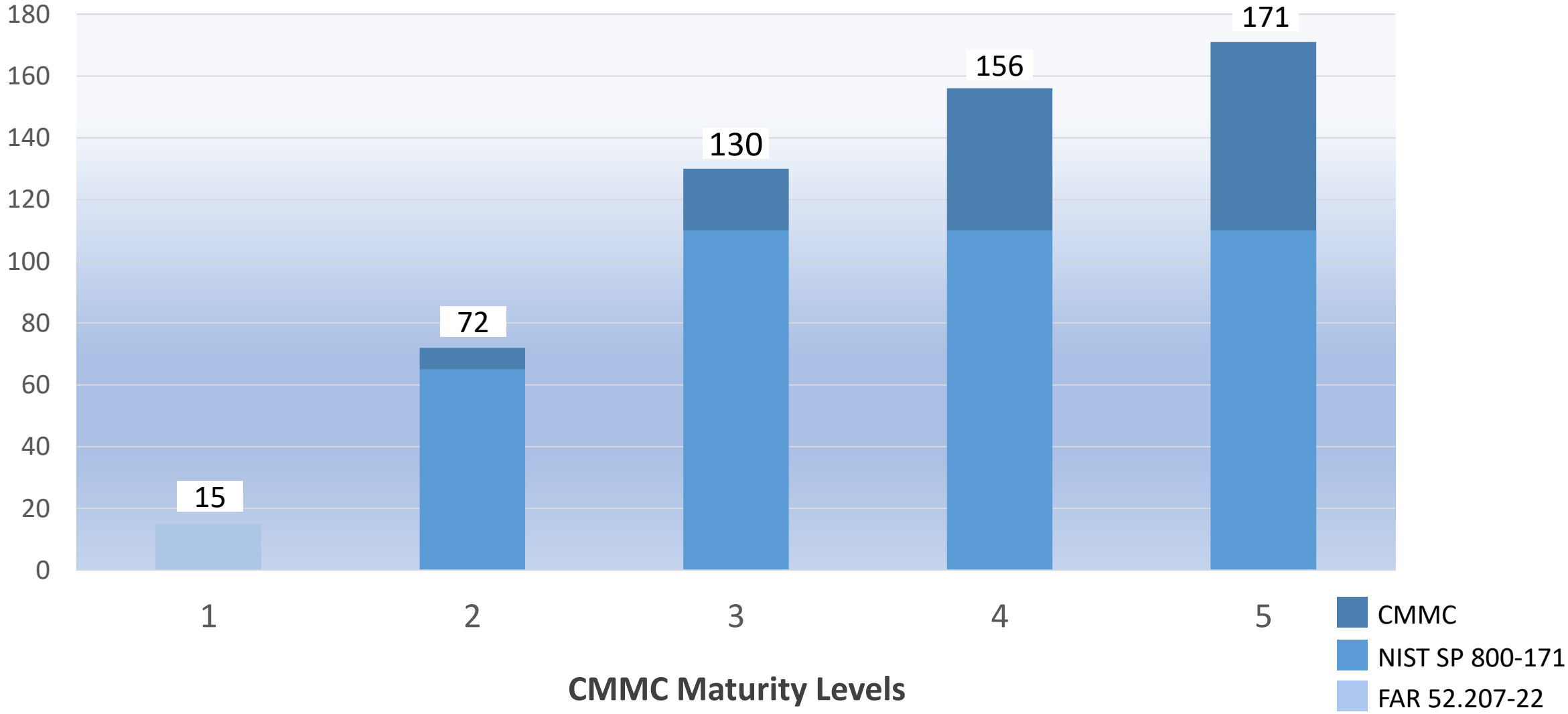
Domains comprises several capabilities to enable security within an organisation. E.g. establish systems access requirements, control internal systems access, control remote systems access and limit access to authorised users and processes for part of the Access Control Domain.

CMMC defines a total of 171 security practices taken from standards and regulations including NIST SP 800 – 171 and FAR 52.207-22. Applied across 5 levels of cyber security maturity (1 – 5). Level 1(17), Level 2(72), Level 3(130), Level 4 (156) and Level 5 (171).

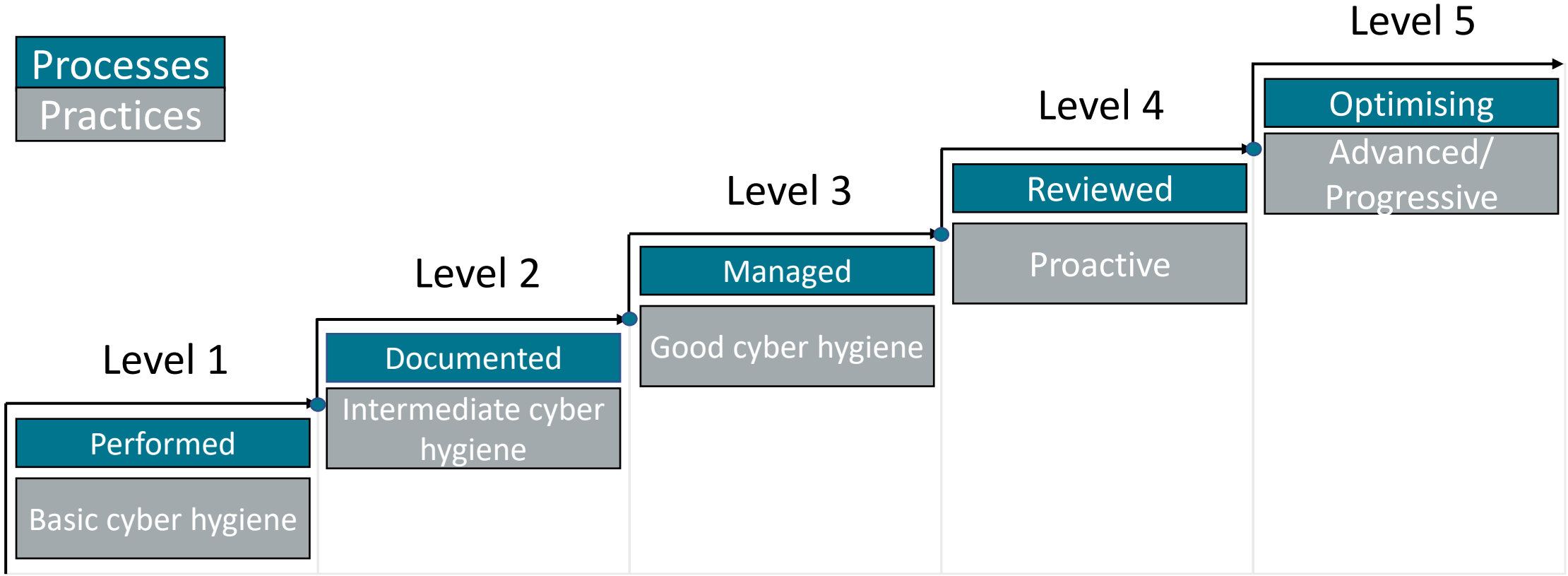
CMMC defines 5 levels of cyber security maturity. Level 1(performed, basic hygiene), 2(Documented, intermediate hygiene), 3(Managed, good hygiene), 4(reviewed, proactive) and 5 (optimising (advanced))

14

CMMC security practices



CMMC maturity processes



Basic Safeguarding of FCI

Protection of CUI and reducing the risk of complex cyber threats including Advanced Persistent Threats (APTs)

Impact of CMMC

Regulatory

- Updates to current DFARS 252.204-7012 will mandate CMMC oversight and accreditation of NIST 800 – 171 compliance to complete DoD contracts.
- Other Federal regulations are being updated to accommodate CMMC.

Procurement

- All DoD suppliers will be required to be CMMC compliant by 2024.
- The first contracts requiring CMMC maturity level certification when DFARS rules are changed.
- DoD contracts will require a valid CMMC certificate.

Legal

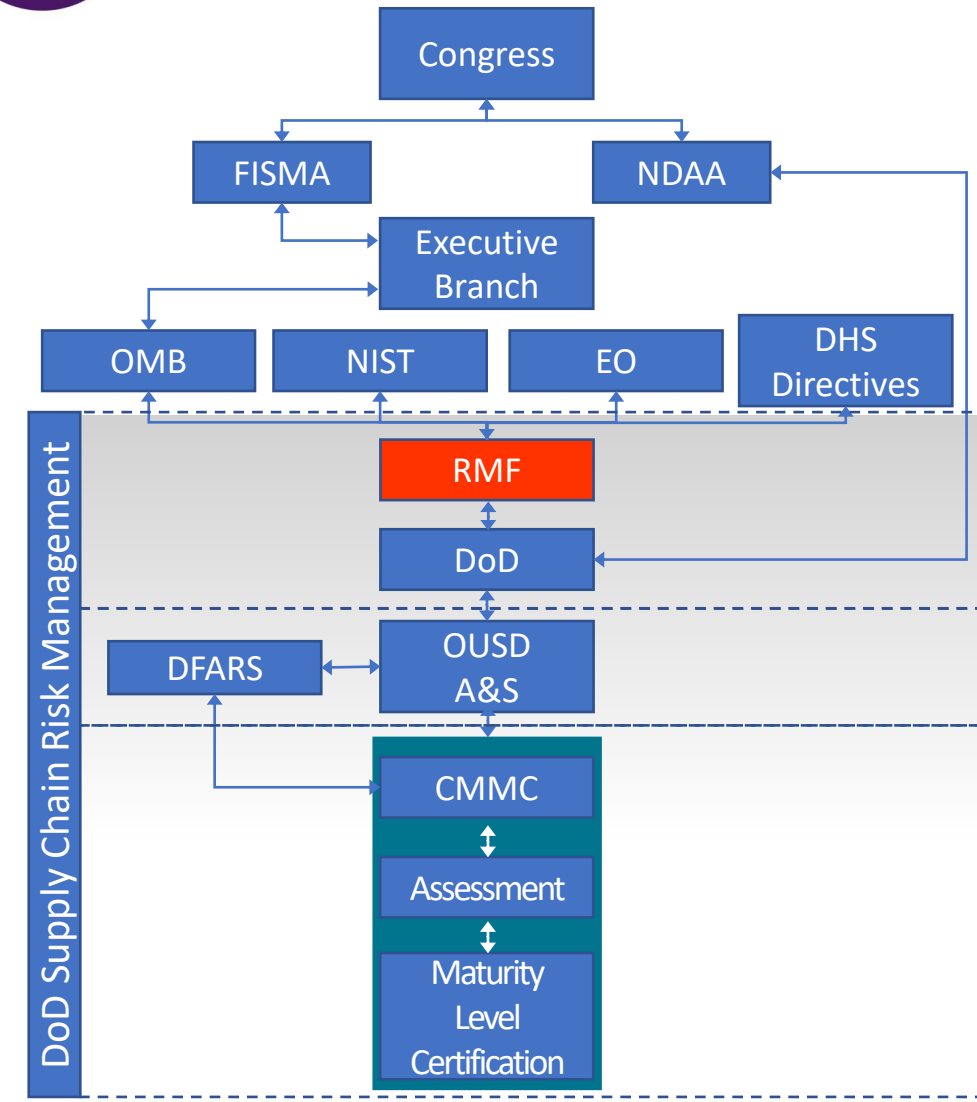
- Existing regulation requires compliance to DFARS and FAR regulation.
- Regulation requires flow down of CUI protection.
- False Claims Act (FCA)[8] – Self attestation to DFARS 252.204-7012, CMMC assessment and accreditation.

Implementation

- CMMC will require the deployment of NIST 800 – 171, as required under by DFARS 252.204-7012.
- DFARS and protection of CUI flows down the global supply chain.
- CMMC maturity levels

CMMC will be a contractual requirement with independent assessment and certification to NIST 800 – 171 and CMMC practices.

DoD Supply Chain Risk Management (SCRM)



Reducing cyber risk across the DoD supply chain through the implementation of the Risk management framework and CMMC

- The DoD is a risk owner with clearly defined responsibilities for the evaluation and management of inherent and residual risk profile under it control.
- OUSD A&S Manages supply chain risk on behalf of the DoD through the DoD procurement process & DFARS.
- OUS A&D uses the DFARS process to regulate and effect change across the US DoD DIB.
- Developing the CMMC programme to embed cyber security practices into the DIB.
- Reducing the inherent supply chain cyber risks through mandated NIST (SP) 800 – 1717 and CMMC security practices.

Inherent risk

Practices/ Controls

Residual risk

Adopting the Risk Management Framework to reduce supply chain risk

Thank you for your interest.

Questions?

andy@parava.org