AustCyber
Australian Cyber Security Growth Network

UNITED STATES GOVERNMENT'S Cyber Security Maturity Model Certification

In January 2020, the US Office of the Under Secretary of Defense for Acquisition and Sustainment introduced the Cyber Maturity Model Certification (CMMC). It is the next evolutionary step for the US Department of Defense (DoD), from the previous Defense Federal Acquisition Regulation (DFAR) requirements.

The CMMC will become the standard requirement for suppliers to operate within the US DoD acquisition and procurement process. All companies supplying to DoD projects, sustainment and operations must become certified and it will be a 'go, no-go' process where suppliers need to be certified before commencing supply.

What's involved?

The CMMC is a unified cyber security standard for suppliers that are part of the United States Defense Industry Base (DIB). It is designed to support efforts across the DoD to better manage cyber risk in its supply chains, currently involving over 300,000 companies globally.

The standard is assessed across five levels of maturity, with level 1 requiring the most basic cyber security and level 5 requiring the most advanced with 171 embedded practices and processes to ensure security and compliance with suppliers who hold Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Requirements will be cumulative, so requirements at level 1 are also required at every other level and so on (See Figure 1).

17 Capability Domains (v1.0)

Figure 1 – Cyber security Maturity Model Certification Capability Domains and Levels

- Access Control (AC)
- Incident Response (IR)
- Risk Management (RM)
- Asset Management (AM)
- Maintenance (MA)
- Security Assessment (CA)
- Awareness and Training (AT)
- Media Protection (MP)
- Situational Awareness (SA)
- Audit and Accountability (AU)
- Personnel Security (PS)
- System and Communications Protection (SC)
- Configuration Management (CM)
- Physical Protection (PE)
- System and Information Integrity (SI)
- Identification and Authentication (IA)
- Recovery (RE)

CMMC Model with 5 levels measures cyber security maturity

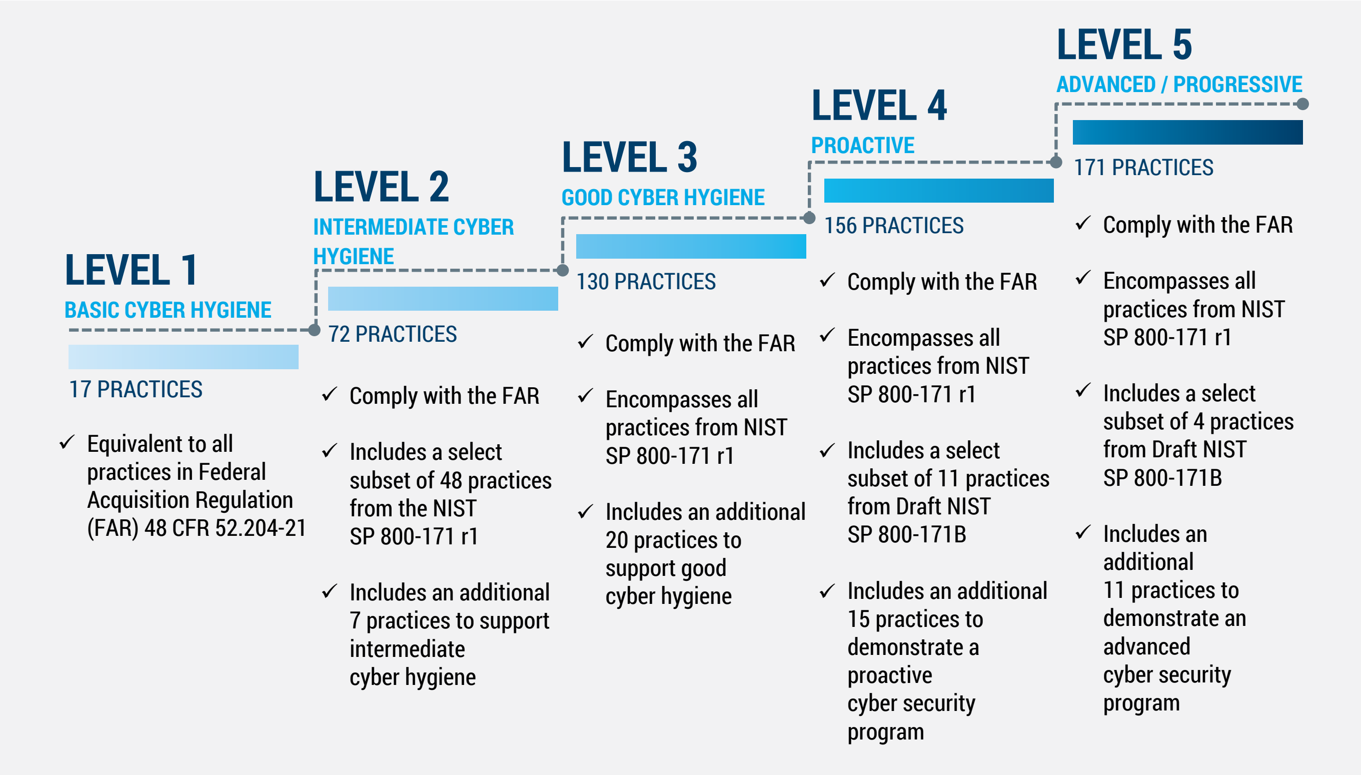
Level 1	Level 2	Level 3	Level 4	Level 5	
Performed	Documented	Managed	Reviewed	Optimizing	PROCESSES
Basic Cyber Hygiene	Intermediate Cyber Hygiene	Good Cyber Hygiene	Proactive	Advanced/ Progressive	PRACTICES

What does it cover?

The matrix at Figure 2 outlines the number of practices required to achieve the level and cross-references to existing certifications. The certification requires compliance with the DFAR/NIST 800-171 requirements and is harmonised with the Australian Cyber Security Centre's Essential 8 and the United Kingdom's Cyber Essentials. CMMC will not replace other compliance requirements but is required in addition to other requirements.

Companies already using NIST 800-171 are well on the way to meeting requirements set out under the CMMC. The major difference between NIST800-171 and CMMC is the new maturity model outlines the practical implementation of requirements. The CMMC will also indicate where requirements map to NIST 800-171 as well as other compliance requirements like FedRAMP.

Figure 2 – Cyber security Maturity Model Certification Levels



LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE
156 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cyber security program

LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cyber security program

How has it been developed?

The CMMC Advisory Board (CMMC-AB) has initiated working groups who are developing the individual processes required for broad implementation. These include:

- CMMC Standards Management
- Standards Management Committee and Industry Working Group
- Credentialling Committee
- Accelerating Initial Assessment Working Group
- Assessment Quality Assurance Working Group
- CMMC Assessment Methodology Working Group
- Training Committee
- Review of CMMC-AB Training and Certification Framework
- Structure of Learning Objectives of Provisional Certification Assessor – Level 3 examination
- Development of pool of exam questions for Provisional Certification Assessor Level 3 examination.

This also includes what will be classified as controlled unclassified information (CUI), training of DoD acquisition employees on the CMMC requirements and certification of companies endorsed as certifiers for CMMC.

The CMMC-AB will also work with partners in Australia, Canada, New Zealand the United Kingdom to build strategic relationships with local accreditation bodies or certify allied foreign nationals to assess local companies.

What is the timing on implementation?

The CMMC will apply to contractors, sub-contractors and third-party suppliers/providers. It is likely to be a five to six-year transition to full implementation of CMMC and NIST 800-171 will continue to be utilised until then.

From 3 May 2020, the certification of qualified certifying organisations will commence, followed by an indication of providers and associated/expected levels of CMMC in June 2020. It is expected that by October 2020, the CMMC will start to appear in RFP paperwork. Note the COVID-19 pandemic may impact these timeframes.

What does this mean for Australian cyber security companies?

The adoption of the CMMC across the DIB will create both opportunities and pressures for Australian companies looking to enter the market to work with US DoD.

Australian companies should consider the level of CMMC that may be required in order to operate with US DoD. All companies within the US acquisition and procurement cycle will be required to be fully compliant by 2025.

More information on the CMMC can be found at **https://www.acq.osd.mil/cmmc/faq.html** and updates will be provided by our Special Projects and US Ecosystem Development Lead Michelle Mosey (**michellem@austcyber.com**) over the coming months on the initial uplift.