Presented By:

The Georgia Defense Industrial Base Task Force

In cooperation with:

TAG Technology Association of Georgia

Georgia USA

Georgia Department of Economic Development

ADAMS AND REESE LLP

Update on

CMMC

(Cybersecurity Maturity Model Certification)

A General Overview

Roy E. Hadley, Jr.

June 25, 2020

The DoD CMMC Standard

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S) is working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification (CMMC).

- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- The intent is for certified independent 3rd party organizations to conduct audits and inform risk.

What Is Cybersecurity Maturity Model Certification (CMMC)?

The Certification was developed by Carnegie Mellon and the Johns Hopkins University Applied Physics Laboratory.

CMMC marks the first step towards implementing the new cybersecurity standards into all DoD contracts.

Under previous methods: Under DFARS 252.204-7012, using NIST SP-800-171, contractors could self-certify – i.e., they could claim current compliance, or they could claim their intention to be compliant.

Under CMMC : Defense Suppliers must be inspected and certified as compliant by assessors.

The model consists of five levels of security standards, which range from Level 1 (Basic Cybersecurity Hygiene) to Level 5 (Advanced).

Where Did the CMMC Standards Come From?

- 48 CFR 52.204-21 (Contains basic cyber safeguards).
- DFARS 252.204-7012.
- NIST SP 800-171 Rev 2 (Equals Level 3 of CMMC).
- Draft NIST SP 800-171B.
- CIS Controls v7.1.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1.
- CERT Resilience Management Model (CERT RMM) v1.2 –NIST SP 800-53 Rev 4.
- Others such as CMMC Board, UK NCSC Cyber Essentials, or AU ACSC Essential Eight.

5 Levels of CMMC Certification.

Level 1: Basic Cyber Hygiene.

Level 2: Intermediate Cyber Hygiene.

Level 3: Good Cyber Hygiene.

Level 4: Proactive.

Level 5: Advanced/Progressive.

CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification

Certified Third-Party Assessment Organizations (C3PAO).

A C3PAO is an organization where licensed assessors will come together hone their skills and register their licenses.

Each C3PAO will need to be certified by the CMMC-AB prior to deploying its assessors into the field.

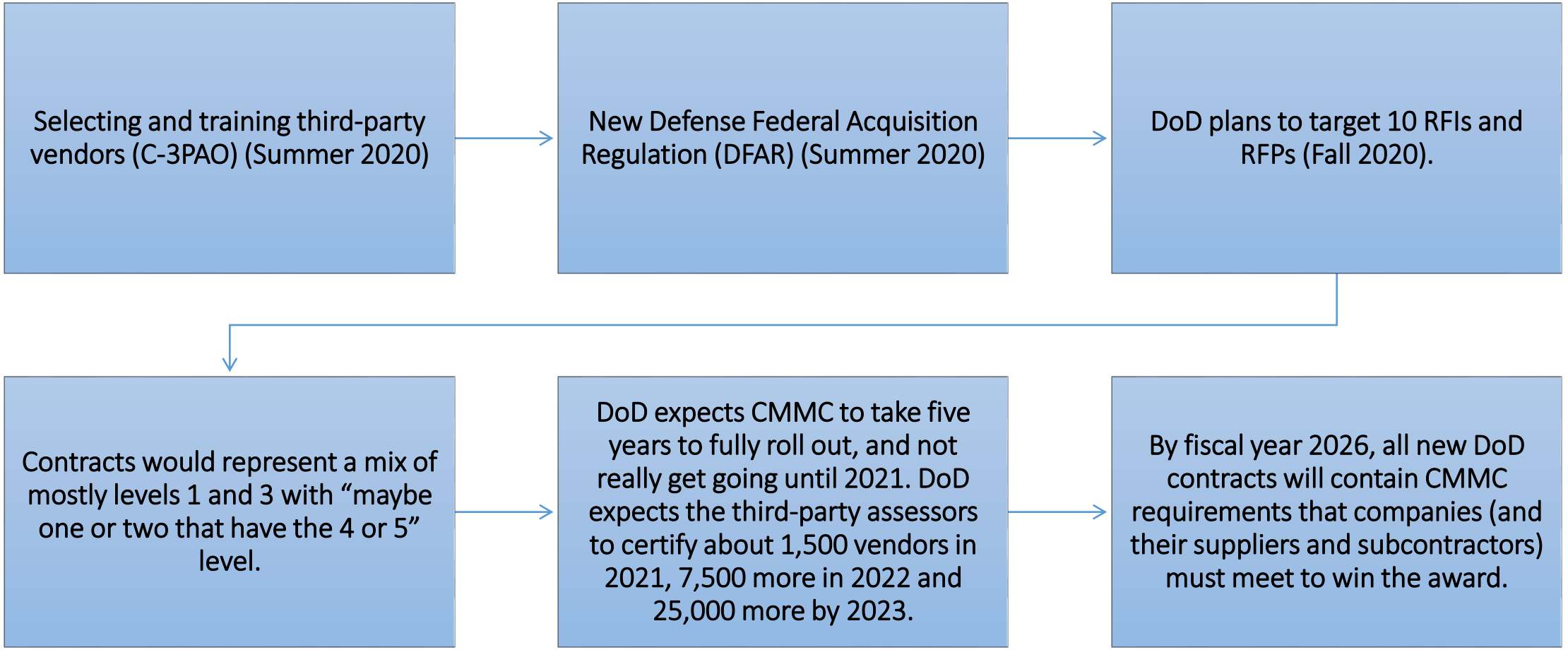
Unknowns:

- When you will be able to register to become an official C3PAO. Think Q3 2020.
- The rules for what it takes to be a C3PAO in good standing.
- The fees or details associated with the process. The CMMC-AB is a nonprofit. Fees will reflect the costs of “providing an independent, national organization with a leading-edge customer experience.”

Who are the Assessors?

- Assessors will receive a license from the CMMC-AB after completing the required training and passing an examination. Training has not been finalized, however.
- Assessors will NOT work for the CMMC-AB but will work for a C3PAO.
- Assessors will receive a license at a level(s) that matches the assessments they are permitted to conduct.
- Experience requirements for higher-level assessors are likely to be required but are not yet determined.
- Assessors are required to obtain a security clearance. The specific clearance levels are not yet determined.

What is the Current CMMC Timeline?



Where Are We Now?

Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Search

Home | Updates | FAQ's | CMMC Model | Contact Us

CMMC Third Party Assessment Organizations (C3PAOs) and CMMC Training

The Department is aware that some entities have made claims of being able to provide CMMC certifications for the purposes of contracting with the DoD. The requirements for becoming a CMMC Third Party Assessment Organization (C3PAO) are not yet established. As a result, there are no third-party entities at this time that have been credentialed to conduct a CMMC assessment which will be accepted by the CMMC Accreditation Body. Similarly, at this time, only training materials or presentations provided by the Department will reflect the Department's official position with respect to the CMMC program.

CMMC Model v1.02 Release

The Department is updating the documentation for CMMC Model v1.0 to correct administrative errors identified since January 31, 2020. The itemized list of corrected errata, as well as a more accessible version of the model (i.e. tabular format in Excel), are provided with the release of CMMC Model v1.02. The Department has made no substantive nor critical changes to the model relative to v1.0.

Where Are We Currently with CMMC?

- No Assessors or C3PAOs are formally accredited or certified by the CMMC-AB.
- The CMMC-AB is currently building the C3PAO training and accreditation process with formal adoption and approval by the CMMC AB.
- The CMMC-AB will publish a publicly available list of Assessors after the standard is complete, the training is developed, and Assessors are certified to provide CMMC certification.
- Certification requirement WILL NOT apply to current contracts.
- When implemented, all companies conducting business with the DoD must be certified.
- There are no fines for not complying – just inability to receive DoD contracts.
- The certifications are expected to be valid for three years before they must be renewed.
- Still need to meet requirements of DFARS 7012 (NIST 800-171, SSP, POA&M).

Issues and Unknowns

CMMC Is Still Unknown in Defense Industrial Base (DIB)

Tier 1 Cyber conducted a survey of 150 government contractors in November 2019.

- 27% admitted they are unprepared for a cyber breach.
- 58% were unfamiliar with CMMC -only a quarter could correctly identify the acronym.
- 12% were confident in the cybersecurity of their vendors.
- 40% said they only have between one and 10 individuals dedicated to information technology, and 10 percent didn't have a dedicated IT professional at all.
- 44% said they were still working to meet the NIST 800-171 requirements —which are expected to be part of level 3 CMMC standards.
- 41% said their cyber incident response plan was a work in progress, and only 20 percent said they have an incident response plan in place.

Unknowns.

- Cost of Third Party Assessors for DiB businesses is unknown.
- Cost of preparing for assessment is unknown.
- The Cost to obtain certification is unknown.

- Availability dates for Third Party Assessor training are not yet known. Expect late Q2 or Q3 2020.
- Training, content, structure, levels etc. are not yet determined.
- Note - Current contracts are not affected, but rebids will have the new CMMC requirements.

What Do You Need To Do

Steps to Take Now.

- Learn the Technical Requirements.
- Decide on In-House vs. Outsourcing.
- Conduct a Readiness Assessment and Gap Analysis.
- Implement Cybersecurity Monitoring (higher levels of CMMC).
- Develop a System Security Plan (SSP).

Some Advanced Considerations.

- Begin to document your practices.
- Engage with agencies now.
- Stay abreast of updated requirements. Stay informed.
- Stay flexible. The framework will likely change.

Recent Updates

Recent Updates.

- DoD believes implementation of CMMC generally is still on track in spite of the COVID-19 pandemic.
- Requests for information ("RFIs") that include the CMMC requirement are expected to come out within the next 45 days. DOD plans to release a total of 10 RFIs in 2020.
- Providers selling only Commercial-Off-The-Shelf (COTS) products will **not** be required to be CMMC-certified at this time.
- Registered Provider Organization (RPO) and Registered Practitioner (RP)details released.

The Georgia Defense Industrial Base (GDIB) Task Force is here to help!

Resources:

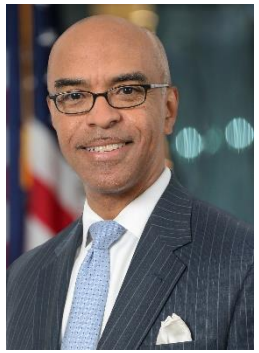
Georgia Defense Industrial Base Task Force: https://www.tagonline.org/ga-dibt/

Georgia Department of Economic Development – Cybersecurity EDGE Program: https://www.georgia.org/cybersecurityedge

CMMC-AB Website: https://www.cmmcab.org

Department of Defense: https://www.acq.osd.mil/cmmc/index.html

Thank you!



Roy E. Hadley, Jr.

Adams and Reese LLP
Office: 470.427.3730
Email: Roy.Hadley@ARLaw.com
LinkedIn Profile:
http://www.linkedin.com/in/royhadley
Twitter: @GovCyberPrep

Cassia Baker

Project Manager, OEA Grant Initiatives
Centers of Innovation
Georgia Department of Economic Development

Email: CBaker@georgia.org