GENERAL DYNAMICS
Mission Systems

small business
PARTNERSHIP
FORUM 2019

DoD Cybersecurity Maturity Model Certification (CMMC) Overview

Joanne Chabot

November, 2019

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)

Summary of DFARS Requirements for Contractors/Subcontractors

- Provide adequate security to safeguard covered defense information (CDI) that resides on or is transiting through a contractor's internal information system or network
  - **NLT 12/31/2017**, comply with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (110 requirements)
    - NIST SP 800-171, Revision 1, dated December 2016.
    - Note: This revision enables contractors to demonstrate implementation or planned implementation of the security requirements through a "System Security Plan" and associated "Plan of Action and Milestones."
  - Contractors may submit requests to vary from NIST SP 800-171 (N/A or alternatives)
  - If using a Cloud Service Provider (CSP) to store, process or transmit CDI in performance of the contract, the CSP must meet the Government's FedRAMP Moderate baseline requirements

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (OCT 2016)

Summary of DFARS Requirements for Contractors/Subcontractors

- Report cyber incidents that affect a covered contractor information system or the CDI residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support
  - 72 hours to report a cyber incident
- Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
- If requested, submit media and additional information to support damage assessment
- Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve CDI
  - "Operationally critical support" means supplies or services designated by the U.S. Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

U.S. Department of Defense Cybersecurity Maturity Model Certification (CMMC)

- As nation state adversaries continue to attack U.S. Defense Industrial Base (DIB) companies throughout the multi-tiered supply chain, the Department of Defense (DoD) is responding to cyber incidents and driving significant changes to DoD acquisition policies
- If your company handles Controlled Unclassified Information (CUI) in the performance of contracts with GDMS, it is imperative that you are aware of the impending U.S. DoD Cybersecurity Maturity Model Certification (CMMC)
- DoD is working with Johns Hopkins University Applied Physics Lab (APL) and Carnegie Mellon University Software Engineering Institute (SIE) to review/combine various cybersecurity standards into one unified standard
  - ***A new cybersecurity certification for DoD contractors named the Cybersecurity Maturity Model Certification, or CMMC, is being developed.***

What is CMMC?

- The CMMC is an assessment model that rates a company's cybersecurity maturity.
- The model, led by the Office of Under Secretary of Defense (OUSD) for Acquisition and Sustainment, is intended to have an accredited third-party assess **all** companies doing business with U.S. DoD and place them in a maturity level.
- Further, U.S. DoD contract data will be categorized for criticality and a commensurate maturity level will be assigned.
- The CMMC model is still being formulated, although we do know a significant portion of the existing framework relies on NIST 800-171 controls already required by Cyber DFARS 252.204-7012 (assessed via NIST 800-171A Assessment Guide) and the, yet to be finalized, NIST 800-171 B "enhanced controls."
- 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.

DoD Cybersecurity Maturity Model Certification (CMMC)

Securing the DoD Supply Chain

- REV 0.4 was released; comments due 9/25/19; industry associations submitted comments
- CMMC Maturity levels: Notionally 1 through 5; basic hygiene to state-of-the-art
  - Will be set forth in RFPs, sections L & M and **will be a "go/no-go decision"**
- Must be semi-automated and cost effective
- Must be agile to adapt to emerging and evolving cyber threats
- CMMC Accreditation Body - Neutral 3rd party will maintain the standard for DoD
  - RFI for CMMC Accreditation Body released; responses are due 10/21/2019
  - Government's goal is for a non-profit Accreditation Body
  - Using revenue generated through dues, fees, partner relationships, conferences, etc. "with no additional funding or resources provided by the Government"
  - Government intends to manage the relationship through a Memorandum of Understanding

How will this flow to the Supply Chain?

- This topic remains open, however the following should be anticipated:
  - At *least* every company handling CUI will need to be independently assessed and certified to cyber maturity tiers commensurate with their contract requirements;
  - DoD contracts are expected to designate maturity level requirements commensurate with the criticality of a contract's controlled unclassified data;
  - As the model is matured, assuring data criticality is assessed appropriately as it flows down, and that CUI anywhere in the multi-tier supply chain can be adequately protected are two concerns that are being addressed.

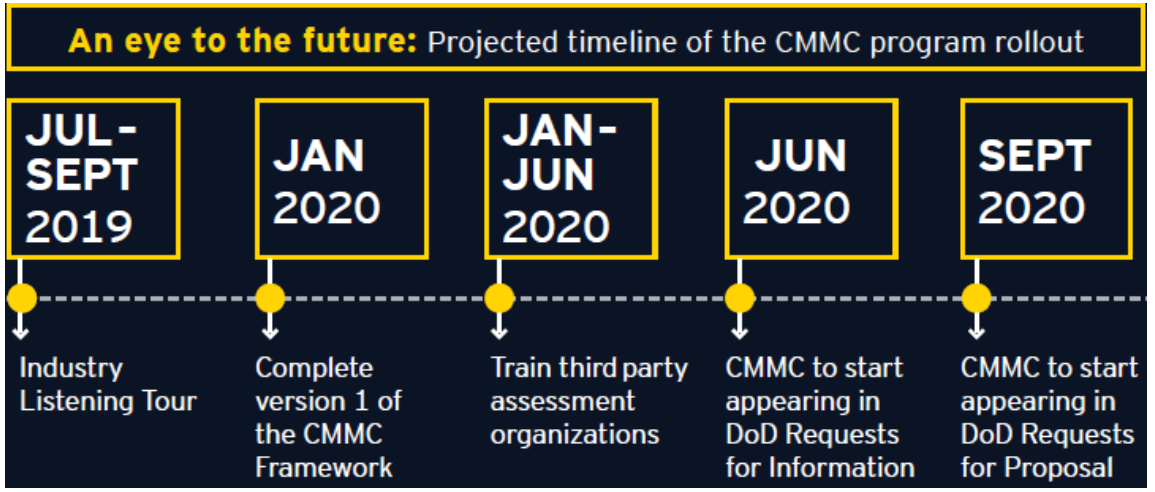
What should you be doing?

- As noted, much of the CMMC assessment model will be based on NIST SP 800-171 security controls.
  - Must have a System Security Plan (SSP) and associated Plan of Action and Milestones (POAM) to address any gaps in the security controls required
  - Work towards completing items in your POAM
- Complete and update your GDMS Representation and Certifications to keep us informed as you make improvements/progress
- Understand and keep current with the status of CMMC; OUSD CMMC website;
- Ensure your suppliers who handle CUI are informed of the CMMC and that they are also addressing any outstanding NIST SP 800-171 requirements/POAM items

DoD Cybersecurity Maturity Model Certification (CMMC)

Securing the DoD Supply Chain

- 3rd party cybersecurity certifiers will conduct the audits
  - Estimating 300,000 companies to be certified
- A tool will be developed/deployed for certifiers to use
- Schedule: Jan 2020 – Release CMMC; Jun 2020 – CMMC included in RFIs; Late 2020 – CMMC included in solicitations
  - The CMMC is on an extremely aggressive schedule and there are several important details which remain in development.
  - Intent is to begin placing CMMC requirements on a limited number of Requests for Proposal in mid-2020. The initial version of the model has been released in early draft form.



DoD Cybersecurity Maturity Model Certification (CMMC)

Securing the DoD Supply Chain

- Public meetings are on-going (see CMMC at link for schedule)
- Insights from public meetings
  - The contractor must be at the required CMMC level set forth in the RFP to qualify for doing the work.
  - Non-profits will train the certifiers.
  - Possibly annual re-certifications with CMMC
  - References to the prime being at one maturity level and the subcontractors being lower
  - New CUI guidance is expected later this year.

Find out more…

- Review GDMS site, Cybersecurity for Suppliers
  - Regulatory References
  - Reporting a Cybersecurity Incident
  - Achieving Cybersecurity Compliance
    - NIST: CUI SSP Template
    - NIST: CUI Plan of Action Template
  - Other Helpful Cybersecurity References
    - DoD Procurement Toolbox
    - DoD: Small Business Cybersecurity
    - Defense Cybersecurity Requirements: What Small Businesses Need to Know [PDF]
- Procurement Technical Assistance Centers (PTACs)
- DoD's CMMC site:
  - https://www.acq.osd.mil/cmmc/index.html

CMMC Summary

- It is envisioned that to receive the certification, a contractor will undergo a third-party audit from an accredited assessor adhering to federally developed standards.
- The intention is that the certification will provide assurance to the DoD and prime contractors that certified organizations can be trusted to utilize CDI, allowing for the validation of cybersecurity capabilities across the entire defense industrial base
- Incorporated in this envisioned CMMC, is a scoring program whereby contractor cyber capabilities are measured against cybersecurity standards. The higher a contractor's score, the more eligible they will be to bid on and be awarded contracts.
- Please continue to monitor CMMC as the requirements evolve.