REQUEST FOR INFORMATION/ PROPOSAL (RFI/RFP) CONTRACT STRATEGY CONSIDERATIONS TO IMPLEMENT THE CMMC

Chris Newborn
DAU Cybersecurity Enterprise Team

Outline

- **Current Policy - DFARS**
- **Future Process - CMMC**
- **Contracting Process /Definitions**
  - Acquisition
  - Contracting
  - Contract/Agreement
- **CMMC Certification**
- **Selection of CMMC Levels**
- **Supply Chain Graphic**
- **CMMC Certification Process**
- **Scenario-Based Discussions**
- **Contract Process**
- **Government**
  - Planning
  - RFP Considerations
  - Contract Language
  - Government Prerequisites
- **Thinking Points – RFI/RFP**
- **Prime /Subs**
  - Planning
  - Prerequisites
- **Summary**

Current Policy - DFARS Clause 252.204-7012

Requires the program office/requiring activity to:

- Mark or otherwise identify in the contract, task order, or delivery order Controlled Unclassified Information (CUI)

Requires the contractor/subcontractor to:

- Provide adequate security to safeguard CUI
- Report cyber incidents
- Flow down the clause in subcontracts

Future Policy - CMMC “Suggested”

Requires the program office/requiring activity to:

- Identify Federal Contract Information (FCI) & CUI Information /Data
- Identify CMMC Level(s)

Requires the contractor/subcontractor to:

- Develop /Update Artifacts /Deliverables per RFI /RFP
- Request CMMC assessment
- Develop Supply Chain /Tier 1 & below Contractor Support Agreements

Acquisition versus Contracting

Acquisition - is defined as “the act of acquiring.” In DoD this includes not only an item but also may include the research and development, test and evaluation, production, fielding, operating, maintenance and disposal of a system

Contracting - is the process of acquiring goods and services. It is only one function within the acquisition environment

What is a Contract?

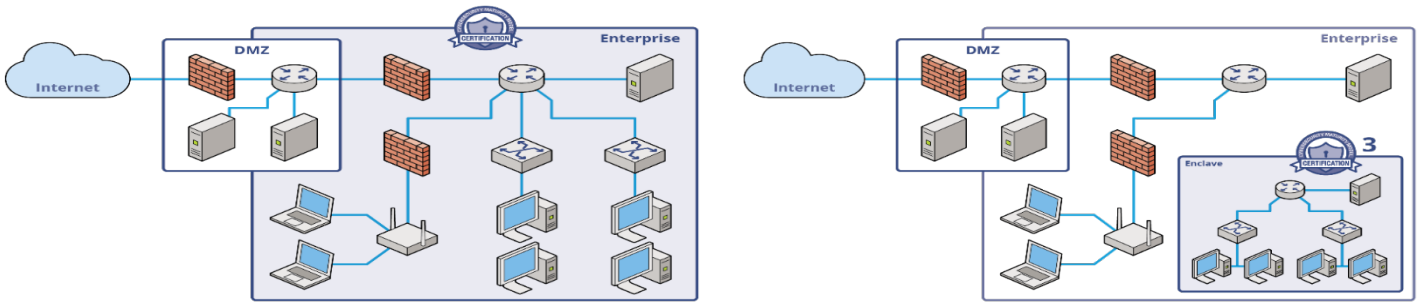
A promise for the breach of which the law provides a *remedy* or the performance of which the law recognizes as a duty and there is legal recourse.

FAR Definition: “Contract” means a mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them.

What is an agreement? Mutual assent between two or more legally competent persons, ordinarily leading to a contract.

CMMC Certification

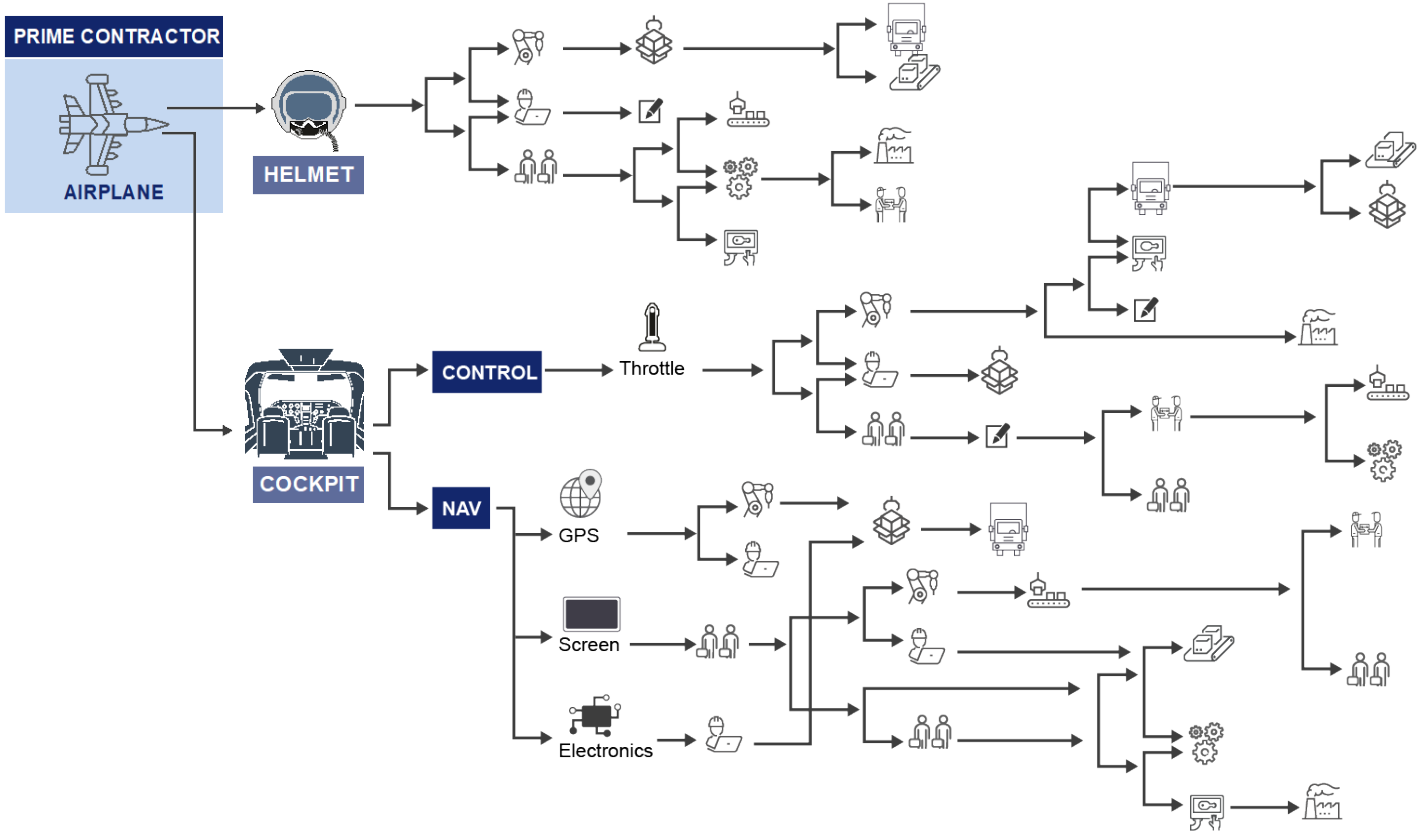
- If a contract requires CMMC certification
  - Market research conducted
  - Requirements outlined in the RFI /RFP /SOW
  - Source selection documents identified
- Companies must meet and /or exceed the CMMC Level
- CMMC certification will last 3 years
- CMMC assessment can be scoped to an entire enterprise network or enclave and defined in the System Security Plan (SSP)



Selection of CMMC Levels (I, III, & III+)

- The government (DoD and Federal) is required for each contract to stipulate the level of protection based on the sensitivity of the information and the threat
- Each Command/Procuring Activity should have the competency to identify, determine, and assess the impact levels if the information is compromised. Since CMMC is applicable to FCI and CUI, at a minimum:
  - Level 1 will be required for all contracts that involve FCI
  - Level 3 & above will be required for all contracts that involve CUI

Risk: DoD Has a Highly Complex Multi-tier Supply Chain (example only)



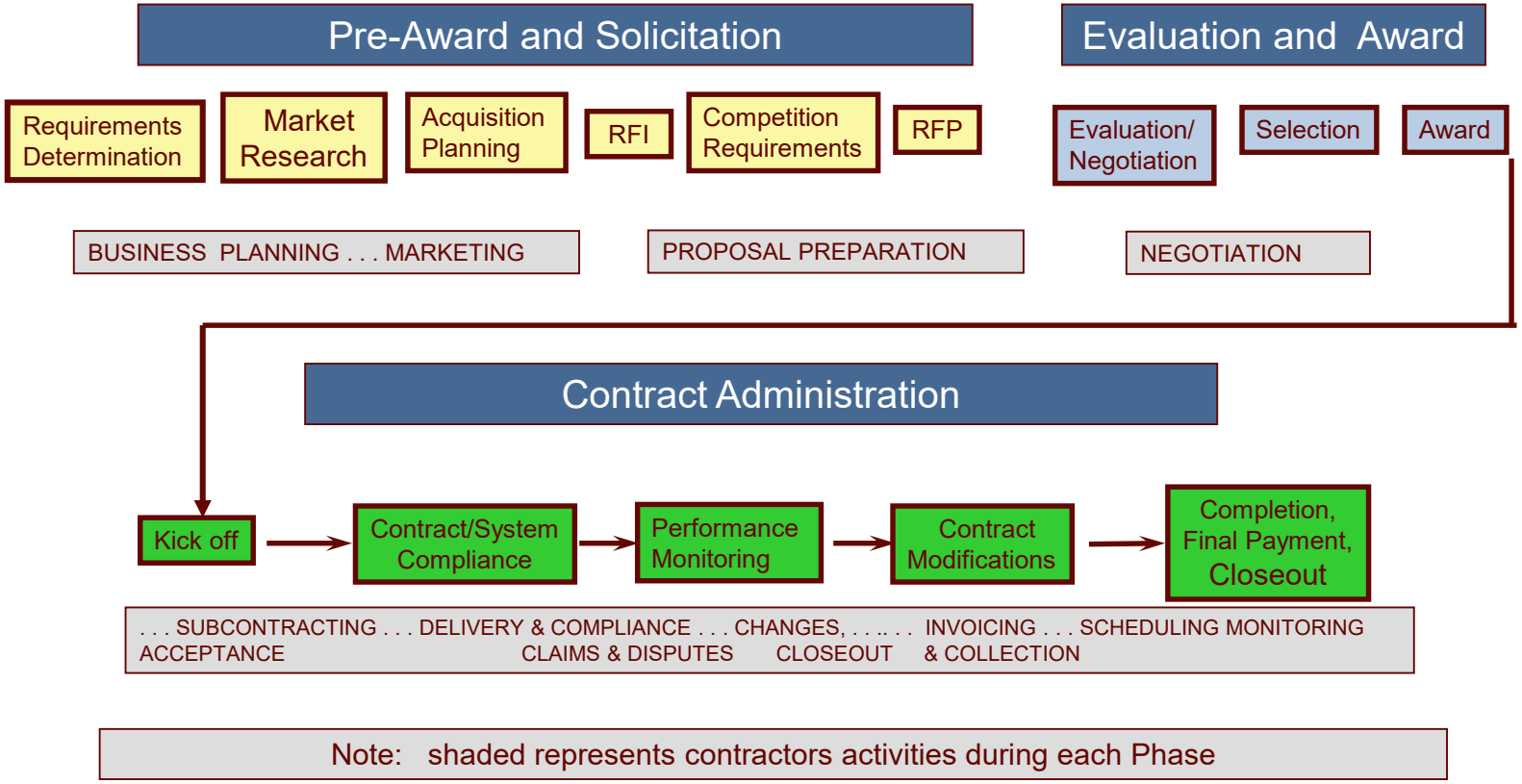
All Contractors Need to Do Their Part to Protect Information

CMMC Certification Process

Scenario-Based Discussion

“Pre-Award”

Contracting Process



“Suggested” Government Planning

Leadership /Program Management /Contracting Office

- Identify Technical and Security Requirements
- Develop Acquisition Strategy, Plan, and Contract Strategy
- Identify CMMC Level(s) (SCG and /or PPP)
- Develop Product and/or Service Work Breakdown Structure (WBS)
- Conduct Market Research to support CMMC language for RFI /RFP inclusion

“Suggested” RFP Consideration(s)

Procuring office should identify entry and exit criteria in Section L & M:

- RFI required for RFP acceptance;
- CMMC certification required before or at time of award;
- DAM Tool evaluation required for RFP acceptance;
- Go /No-Good decision for CMMC Level for RFP acceptance or at time of award;
- POA&M /waiver be allowed at time of award; and
- Artifacts be required and evaluated to validate CMMC Level.

“Suggested” Contract Language Consideration(s)

Contract Language Considerations:

- Is FAR 52.204-21 and DFARS Clause 252.204-7012 full language required (UNKNOWN BASED ON RULE MAKING PROCESS)?
- Is CMMC Level Certificate required prior to RFP submission (go/no-go decision). If not, will submission of SSP, Incident Response Plan, and Supply Chain Support Agreement be required for government evaluation?
- If contract follow-on effort /continuation, is DAM scoring required for past performance evaluation?

Unknown: Process, timeline, & cost for CMMC Certification

“Suggested” Government Prerequisites

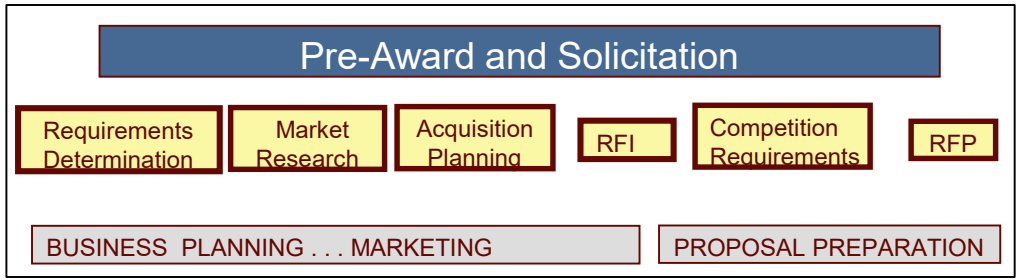
- Provide SOW /SCG /PPP/WBS
- Coordinate with Prime/ Subs and CMMC AB to ensure assessments are scheduled
- Establish CMMC evaluation criteria as pass /fail for Prime /Subs
- Insert contract language /mods to address when threat changes /incidents occur
- Establish Prime /Subs awareness /updates on imminent /changes in threat /related incidents
- Establish Technical Advisory Board

Deliverables:

- RFI, RFP, SOW, SCG, PPP, WBS

References:

- CFR 52.204-201
- DFARS 252.204-7012 Clause
- NIST SP 800-171 v1.1, DAM Tool
- NIST SP 800-171R2/171B
- NIST SP 800-171A
- DoDI 5200.48
- CMMC v1.02



Thinking Points - RFI (Level III & Above)

RESPONSE (2): Use previous DFARS contractor language and modify for RFI/market research gathering purposes. Selection should dictate RFP entry criteria.
RESPONSE (3): If security requirements are known and multiple vendors available, submit RFI package with draft SOW. If security requirements are not known but multiple vendors available, submit RFI with draft SOO. If security requirements are not known and vendors not available, conduct industry day conference, then submit RFI with draft SOO/SOW. This should be incorporated into the Contract Strategy.
RESPONSE (4): Defining what needs protection requires government to identify FCI/CUI components via specification tree (WBS) and identify who has what responsibility for each tier (prime versus sub versus vendor/ manufacturer).
RESPONSE (5): Is this procurement action only requiring the safeguarding of FCI/CUI or are there other contract services being delivered (end-item and/or services)? What related contract evaluation criteria will be used to make the final selection; what takes precedence (security of information on contractor's network/system and/or end-item)?
RESPONSE (6): Contracting office has previous contract language that identifies DFARS Clause requirements applicable to adequate security, incident reporting, and flow-down requirements. This language can easily be modified to incorporate the CMMC process.
RESPONSE (7): For RFI entry criteria, Contractor required to use DFARS Assessment Methodology (DAM) tool and upload scoring to database, to include all subs, vendors, and manufacturers (supply chain).

QUESTION (1): Is CMMC going to replace the DFARS policy or just become a standard and replace the NIST guidelines?
QUESTION (3): What additional contract or scope language is required above and beyond CMMC v1.02?

FACT (1): Creating a baseline template was a challenge for DFARS (CDI/CUI/CTI) and even more of a challenge for CMMC (FCI/CUI – Levels 1-5). Incorrect assumptions made: all contractors have a standard network configuration (stand-alone, Purdue, flat), services will be in-house (TPPs), same company size/#employees (large, medium, small), and flow-down is the same (prime, sub, vendor, manufacturer).

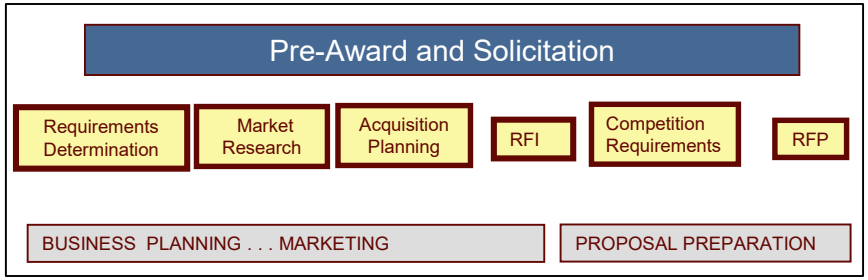
“Suggested” Prime /Subs Planning

Executives /Project Managers /Contract Managers

- Develop certification strategy and scope
  - Subnetwork /Enclaves to support Supply Chain
  - Identification of CMMC Level I (FCI) and Level III (CUI) subcontractors & associated CMMC support (Third Party Providers)
- Develop contract artifacts/deliverables per RFI /RFP to include contractual flow down requirement
- Perform self assessment to confirm CMMC Level achieved and ready for CMMC assessment
- Request C3PAO to perform CMMC assessment
- Develop draft response to RFI identifying possible CMMC compliance challenges
- Develop Supply Chain /Tier 1 Contract Support Agreements

“Suggested” Prime /Sub Prerequisites

- Ensures Subs are CMMC level certified or will be prior to awarding of contract
- Conducts periodic drills, inspections, scans, exercises, and pen test
- Prepare for PMO /Government initiated pen test and Red Team Assessment
- Develop /maintain POA&M for supply chain /Subs security network upgrades due to projected threat increase over contract PoP
- Report loss /compromise /incident wrt FCI /CUI data on Prime /Subs networks /systems
- Determine which services /capabilities performed in-house and out-sourced (TPP)



Deliverables (have available):

- SSP, SAR, POA&M, SPRS Report

References:

- CFR 52.204-201
- DFARS 252.204-7012 Clause
- NIST Handbook 162
- NIST SP 800-171 v1.1, DAM Tool
- NIST SP 800-171R2/171B
- NIST SP 800-171A
- DoDI 5200.48
- CMMC v1.02

Summary

- The government (DoD and Federal) is required for each contract to stipulate the level of protection based on the sensitivity of the information and the threat
- Each Command /Procuring Activity will have to determine the risk they are willing to accept to transition to the new CMMC process
  - DFARS Rule-Making Status
  - Maturity of CMMC support processes (certification process, C3PAO availability, pricing, etc.)
  - DFARS and CMMC training
- There are several organization(s) and program(s) available to help /aid medium to small business to implement best practices and lesson-learned to safeguard government sensitive information

The slides and question will be posted here
https://www.dau.edu/events/The%20Cybersecurity%20Maturity%20Model%20Certification%2022

And the recording will be posted
https://www.dau.edu/p/webcasts

Survey: https://survey.dau.edu/opinio/s?s=11955

For additional questions, please contact Chris Newborn at chris.newborn@dau.edu or 619-370-3076