TOPICS

• Changes in Department of Defense cybersecurity
  • CMMC
  • Language / Terminology
  • Contracts

• What can be done to prepare
BRIEF HISTORY
2013
DFARS 252.204-7012
Safeguarding Unclassified Controlled Technical Information (UCTI)

2015/2016
Inclusion of NIST SP 800-171
Final Ruling

2017
Dec 31, 2017
DFARS compliance deadline
CHANGES SINCE DEADLINE - ASSESSMENT

DoD Assessment Methodology

The NIST SP 800-171 DoD Assessment Methodology enables DoD to strategically assess a contractor’s implementation of NIST SP 800-171 on existing contracts which include DFARS clause 252.204-7012, and to provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to the contract-by-contract approach.

Supplier Performance Risk System

Supplier Performance Risk System for National Institute of Standards and Technology Special Publication 800-171 Department of Defense Assessment

https://www.acq.osd.mil/dpap/pdi/cyber

Cybersecurity Maturity Model Certification

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.

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.

https://www.acq.osd.mil/cmmc
“The CMMC model which measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats.

The model consists of maturity processes and cybersecurity best practices.”
# CERTIFICATION

<table>
<thead>
<tr>
<th>DFARS 252.204-7012</th>
<th>CMMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contractors who receive, transmit, produce “CDI”</td>
<td>Applies to all contractors conducting business with the DoD who possess “CUI” or “FCI”</td>
</tr>
<tr>
<td>Single Level (Compliant or Not Compliant)</td>
<td>Multiple Levels from “Basic Cyber protection” to “Mature Cybersecurity Practices”</td>
</tr>
<tr>
<td>Requires Self Attestation to Compliancy</td>
<td>Requires Certification from Third Party</td>
</tr>
<tr>
<td>Contractual Requirement</td>
<td>RFP/RFQ Requirement (Section L&amp;M)</td>
</tr>
<tr>
<td>“Covered Defense Information” (CDI)</td>
<td>“Controlled Unclassified Information” (CUI) “Federal Contract Information” (FCI)</td>
</tr>
<tr>
<td>Allows for “Plan of Action” for currently not implemented requirements</td>
<td>Requires full implementation of requirements</td>
</tr>
</tbody>
</table>
CMMC – TRUE / FALSE

• CMMC is the new version of DFARS
  FALSE – Currently, CMMC is a separate entity from DFARS with CMMC applying to the RFP/RFQ while DFARS is a contractual requirement.

• CMMC is the next NIST SP 800-171
  FALSE – The CMMC is a separate model that includes components of NIST SP 800-171, NIST 800-172 (171B), and “Other.”

• I can obtain my certification now
  FALSE – While the CMMC model has been released, the actual certification process has not been completed. As of today, there is NO method to be certified and NO company can offer CMMC certifications.
**CMMC – TRUE / FALSE**

• I received a letter from my customer saying I need to be certified at CMMC Level {X}.

**POTENTIALLY TRUE** – While the CMMC model currently does not specify exact supply chain requirements a contractor can choose to require certification of their supply chain. It is important to remember the following regarding this:

1. There is currently no method to become certified and no current date when this will become available.
2. While your customer can require additional security requirements there are currently no requirements from the DoD that require you to have a certain CMMC level.
3. CMMC is not a substitute for DFARS requirements. If you have DFARS 252.204-7012 flowed down to your contracts, this still needs to be met.
CMMC / CONTRACTING FACTS

• As of today, DFARS 252.204-7012 has not changed and it still outlines current contractual requirements. The primary focus of a contractor should be to continue implementing unmet requirements on their POAM and improving their policy/procedure maturity.

• Working toward full NIST SP 800-171 implementation is the best path to prepare for CMMC.

• While a contractor cannot currently become CMMC certified, the model has been released which specifies the required practices. Contractors should be familiar with these and plan any needed modifications to their current implementation.

• What is true today may not be tomorrow. CMMC is still in the process of development and will be updated as that occurs. DoD contractual requirements also will very likely change in the future.
CHANGES OCCURRING

Terminology and Contracts
CDI

Controlled Defense Information (CDI)

“unclassified controlled technical information or other information.... that requires safeguarding or dissemination controls....”
CUI

Controlled Unclassified Information (CUI)

“... unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.”
CDI

Controlled Defense Information (CDI)

DoD Instruction 5200.48 - establishes policies, responsibilities, and procedures for controlled unclassified information (CUI), as well as a DOD CUI repository.
CDI

• Is this the same as the CUI registry?
  • No - The “CUI Registry”, maintained by the National Archives and Records Administration (NARA) is not the same as the DoD CUI repository.
CDI

- Is this the same as the CUI registry?
  - No - The “CUI Registry”, maintained by the National Archives and Records Administration (NARA) is not the same as the DoD CUI repository.

- How do I access the repository?
  - Currently the repository is not available to the general public. However, the “DoD” category on the NARA CUI Registry contains similar information.

| Defense                  | • Controlled Technical Information  
|                        | • DoD Critical Infrastructure Security Information  
|                        | • Naval Nuclear Propulsion Information  
|                        | • Unclassified Controlled Nuclear Information - Defense |

https://www.archives.gov/cui/registry/category-list
Federal Contract Information (FCI)

- Information provided by or generated for the Government under contract not intended for public release.

Controlled Unclassified Information (CUI):

- Information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies....
Why should I be concerned with this change?

- “FCI” will more than likely require only a Level 1 CMMC certification.
- “CUI” requires a Level 3 CMMC certification.
FCI

• Why should I be concerned with this change?
  • “FCI” will more than likely require only a Level 1 CMMC certification.
  • “CUI” requires a Level 3 CMMC certification.

• Weren’t “FCI” and “CUI” both part of “CDI”? Which information is classified as each? - Pending Review
RFI / RFQ (BID)

- Section (L/M)
- CMMC
- FCI / CUI
- Certified at Level 1-5

CONTRACT

- CDI
- Self Attest

CONTRACT

- DFARS 252.204-7012
- NIST SP 800-171 Implementation
CONTRACT

RFI / RFQ (BID)

Section (L/M)
CMMC
FCI / CUI
Certified at Level 1-5

CONTRACT

DFARS 252.204-7012
NIST SP 800-171 Implementation
CDI
Self Attest

- 252.204-701x – revised or new?
- NIST SP 800-171 or CMMC?
- DoD CUI?
- Inclusion of FCI?
- When?
WHY BE PREPARED?

• Estimated six (6) to eighteen (18) month preparation for CMMC Certification.
• 90 days corrective action (after assessment).
INFORMATION

- Information you have.
- Why it needs to be protected.
- How you are protecting it.
- How to validate that protection.
SYSTEMS

- Physical
- Technical
- External
“CONTROLS”

- KNOW your policies and practices.
  - Document
  - Review
- KNOW what risks they reduce.
- KNOW that they are effective.
  - Validate
  - Revise
- KNOW they are complete.
- KNOW employees are trained.
WHO IS INVOLVED

• Decision makers (Owners, Presidents, Executive Management).
• Employees.
• External resources.
REVIEW

- Current Policies.
- NIST 800-171 Implementation.
- Address outstanding Plan items.

- Evaluation Methods.
THANKS TO:

Jeff Williams
Michigan Manufacturing Technology Center
jwilliams@the-center.org
QUESTIONS?
Let CONNSTEP help you grow your business, increase profitability, improve efficiencies, and create a sustainable competitive advantage in the marketplace.

Jeff Orszak
Director, Strategic Growth and Technology
jorszak@connstep.org
860 539-4905
SUPPLEMENTAL SLIDES
CMMC STRUCTURE

CMMC Model Structure

17 Capability Domains (v1.0)

- 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 cybersecurity maturity

- Level 5: Optimizing
- Level 4: Advanced/Progressive
- Level 3: Reviewed
- Level 2: Proactive
- Level 1: Managed

DISTRIBUTION A. Approved for public release
CMMC MATURITY 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 800-171r1
- 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 800-171r1
- 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 800-171r1
- Includes a select subset of 11 practices from Draft NIST SP 800-171B
- Includes an additional 15 practices to demonstrate a proactive cybersecurity program

**LEVEL 5**
Advanced / Progressive
- 171 practices
- Comply with the FAR
- Encompasses all practices from NIST SP 800-171r1
- Includes a select subset of 4 practices from Draft NIST SP 800-171B
- Includes an additional 11 practices to demonstrate an advanced cybersecurity program
## CMMC LEVEL 3
### ADDITIONAL PRACTICES BEYOND NIST SP 800-171

<table>
<thead>
<tr>
<th>Practice Number</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU.2.044</td>
<td>Review audit logs.</td>
</tr>
<tr>
<td>IR.2.093</td>
<td>Detect and report events.</td>
</tr>
<tr>
<td>IR.2.094</td>
<td>Analyze and triage events to support event resolution and incident declaration.</td>
</tr>
<tr>
<td>IR.2.095</td>
<td>Develop and implement responses to declared incidents according to pre-defined procedures.</td>
</tr>
<tr>
<td>IR.2.097</td>
<td>Perform root cause analysis on incidents to determine underlying causes.</td>
</tr>
<tr>
<td>RE.2.137</td>
<td>Regularly perform and test data back-ups.</td>
</tr>
<tr>
<td>RE.3.139</td>
<td>Regularly perform complete, comprehensive and resilient data backups as organizationally-defined.</td>
</tr>
<tr>
<td>RM.3.144</td>
<td>Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources and risk measurement criteria.</td>
</tr>
<tr>
<td>RM.3.146</td>
<td>Develop and implement risk mitigation plans.</td>
</tr>
<tr>
<td>RM.3.147</td>
<td>Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.</td>
</tr>
<tr>
<td>CA.3.162</td>
<td>Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally-defined as an area of risk.</td>
</tr>
<tr>
<td>SA.3.169</td>
<td>Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.</td>
</tr>
<tr>
<td>SC.2.179</td>
<td>Use encrypted sessions for the management of network devices.</td>
</tr>
<tr>
<td>SC.3.192</td>
<td>Implement Domain Name System (DNS) filtering services.</td>
</tr>
<tr>
<td>SC.3.193</td>
<td>Implement a policy restricting the publication of CUI on externally-owned, publicly-accessible websites (e.g., forums, LinkedIn, Facebook, Twitter, etc.).</td>
</tr>
<tr>
<td>SI.3.218</td>
<td>Employ spam protection mechanisms at information system access entry and exit points.</td>
</tr>
<tr>
<td>SI.3.219</td>
<td>Implement email forgery protections</td>
</tr>
<tr>
<td>SI.3.220</td>
<td>Utilize email sandboxing to detect or block potentially malicious email.</td>
</tr>
</tbody>
</table>