Department of Defense’s Cybersecurity Maturity Model Certification (CMMC) and the CMMC Accreditation Body
What is CMMC?

Third-party assessment of a contractor’s cybersecurity maturity based on the CMMC model.

Targeted to be in 10 initial “pathfinder” contracts in September 2020.

Will be integrated into additional contracts over a 5-year period.

By 2026, CMMC requirements will be in all DoD contracts.
How did CMMC Begin?

“If we were doing all the necessary security controls, we wouldn’t be getting exfiltrated to the level that we are.”

Katie Arrington, CISO for Assistant Sec. Def. for Def. Acquisition, June 20, 2019
Why is CMMC Necessary?

Cybersecurity incidents negatively impact US business

- Cybersecurity incidents increase contract delivery costs, lengthen delivery timelines, and jeopardize business integrity:

  - Malicious cyber activity cost the US economy between $57 billion and $109 billion in 2016 (The Council of Economic Advisors)
  
  - $3 trillion in annual cybercrime losses in 2015, estimated to grow to $6 Trillion by 2021 (Cybersecurity Ventures)

  - The average data breach costs $3.9 Million worldwide, $8.9 Million in USA (Ponemon Institute)
Why is CMMC Necessary?

Cybersecurity is national security
- US electrical grid nearly taken offline
- Office of Personnel Management breached
- Military and industrial intellectual property stolen
What is the CMMC Model?

- The CMMC Model defines a framework for measuring cybersecurity maturity with five maturity levels and aligns a set of policies and practices with the type and sensitivity of information to be protected and the associated range of threats.
- Based on best practices from multiple cybersecurity standards, frameworks, and other references.
- Focuses on protecting FCI and CUI.
....with a number of Processes and Practices....
...to increase overall Cybersecurity Maturity

- There are Five Maturity Levels in CMMC (balances process, technology and maturity)
- Movement between levels require documented processes; these must be in place and verified
  - The documentation process frequently identifies areas where costs can be saved, and efficiencies realized.
  - This can take significant time to implement and, although CMMC requirements may not apply to them now, organizations should begin creating appropriate documentation now.
- Each level builds on the prior level
- CMMC Level 3 is required for contracts which include Controlled Unclassified Information

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Maturity Level Description</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML 1</td>
<td>Performed</td>
<td>There are no maturity processes assessed at Maturity Level 1. An organization performs Level 1 practices but does not have process institutionalization requirements.</td>
</tr>
<tr>
<td>ML 2</td>
<td>Documented</td>
<td>Establish a policy that includes [DOMAIN NAME].</td>
</tr>
<tr>
<td>ML 3</td>
<td>Managed</td>
<td>Document the CMMC practices to implement the [DOMAIN NAME] policy.</td>
</tr>
<tr>
<td>ML 4</td>
<td>Reviewed</td>
<td>Establish, maintain, and resource a plan that includes [DOMAIN NAME].</td>
</tr>
<tr>
<td>ML 5</td>
<td>Optimizing</td>
<td>Review and measure [DOMAIN NAME] activities for effectiveness.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.</td>
</tr>
</tbody>
</table>
Why Install the Accreditation Body?

- DoD asked industry to create a nonprofit, corporation-agnostic organization and the CMMC-AB was formed in January 2020.
- CMMC-AB is responsible for creating the CMMC Ecosystem, including:
  - Clarify the CMMC Standard (implementing the CMMC Model created by DoD)
  - Developing CMMC-related Testing and Accreditation Requirements
  - Licensing Training Organizations and Curriculum
  - Licensing Trainers
  - Licensing Certified 3rd Party Assessment Organizations (“C3PAOs”)
  - Licensing Assessors
  - Issuing Certificates to Organizations Seeking Certification

https://www.cmmcab.org/
What is the CMMC Accreditation Body?

- Registered as a non-stock corporation in Maryland
- Consists of an all-volunteer Board Directors
- Directors are diverse (small business to large, some with govt experience)
- Directors serve as individuals and not representatives of their parent organizations

CMMC-AB Main Focus: Operationalize the training, accreditation and certification aspects of the CMMC model and standard

- Board founded on strong ethics and mission-focus
  - Directors cannot be individual assessors nor affiliated with a C3PAO
  - All Directors are subject to a strict Conflict of Interest Policy
Organizations Seeking Certification (OSC)