2024 SRAI SO/NE
SECTION MEETING
HILTON HEAD, SC
MAY 7 - 10

Attain Partners

Cybersecurity Maturity Model Certification (CMMC) 2.0

Andrea Deaton, MHR, CRA
Attain Partners, LLC
addeaton.ctr@attainpartners.com
405.613.1417

Objectives

Understand CMMC 2.0 as it relates to your specific situation

Identify when it is appropriate for CMMC language to be included in contracts

Background

2010, EO 13556

CMMC model seeks to provide a standard for the protection, storage, and transmission of CUI

- EO defined what constitutes CUI and how it is defined.

2017, defense contractors had to self-assess against the NIST 800-171 standard.

- CMMC was founded on these standards and was created as a way to better enforce NIST 800-171 requirements.

2019, DoD Defense actually announced the development of CMMC in order to move away from the current "self attestation" model of security.

2020 CMMC 1.0 was implemented as an interim rule in all DoD contracts requiring to upload a SPRS score in compliance with NIST 800-171 and various DFARS requirements.

2021 CMMC 2.0 was announced and attempted to streamline the expectations of the previous models by downsizing the transitionary levels of 2 and 4.

Why CMMC?

Cybersecurity is a top priority for the Department of Defense.

The Defense Industrial Base (DIB) is the target of more frequent and complex cyberattacks. To protect American ingenuity and national security information, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) 2.0 program to reinforce the importance of DIB cybersecurity for safeguarding the information that supports and enables our warfighters.

Currently under Proposed Rule

Streamlining model from five levels to three levels

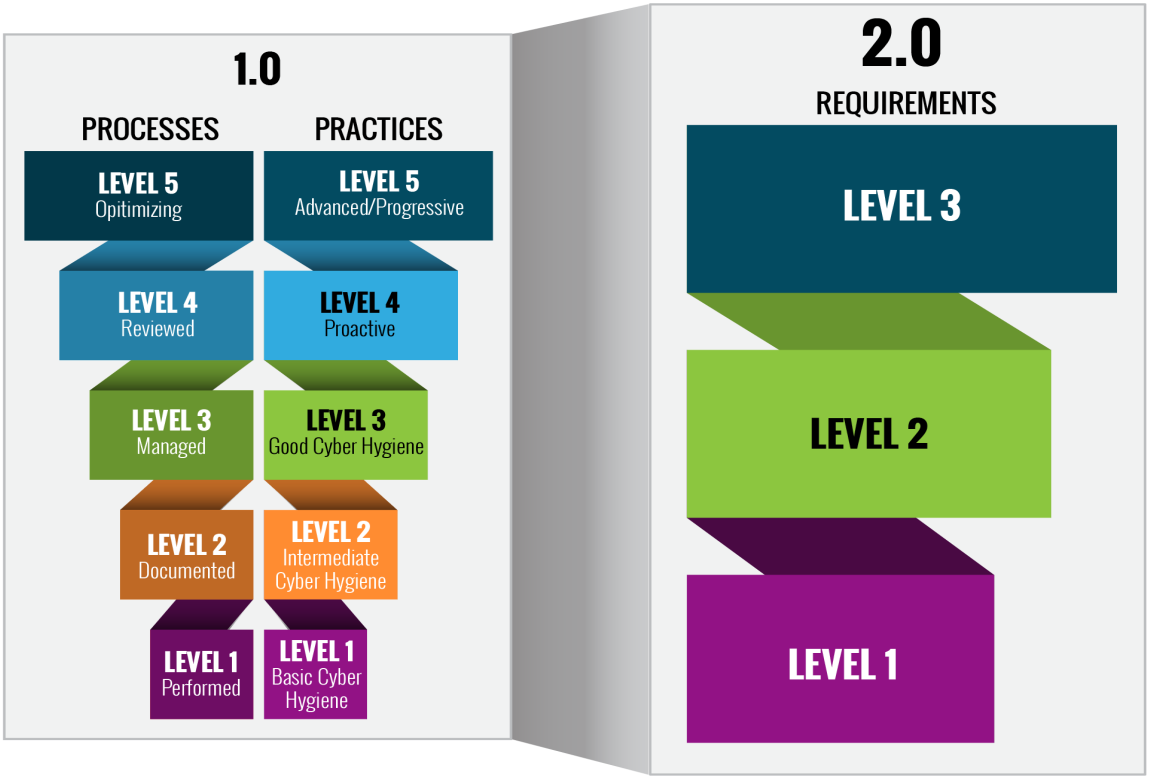
Exclusively implementing National Institute of Standards and Technology (NIST) cybersecurity guidelines

Allowing all companies at Level 1 and a subset of companies at Level 2 to demonstrate compliance through self-assessments

Increased oversight of professional and ethical standards of third-party assessors

Allowing companies, under limited circumstances, to make Plan of Action & Milestones (POA&M) to achieve certification

CMMC Model Structure



How does this apply to Universities

- Prime Government Contractor
- Lower tier Government Contractor
- RFQ
- Solicitations

What to watch for

FAR clause 52.204–21, *Basic Safeguarding of Covered Contractor Information Systems*

- requires compliance with 15 security requirements, FAR 52.204–21(b)(1), items (i) through (xv).
- These requirements are elementary for any entity wishing to achieve basic cybersecurity

DFARS clause 252.204–7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

- requires defense contractors to provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in the **National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.***
- The DFARS clause 252.204–7012 also requires defense contractors to flow down all the requirements to their subcontractors.

What to watch for (cont'd)

DFARS clause 252.204–7019, NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS

- strengthens DFARS clause 252.204–7012 by requiring contractors to conduct a NIST SP 800–171 self-assessment according to NIST SP 800–171 DoD Assessment Methodology.

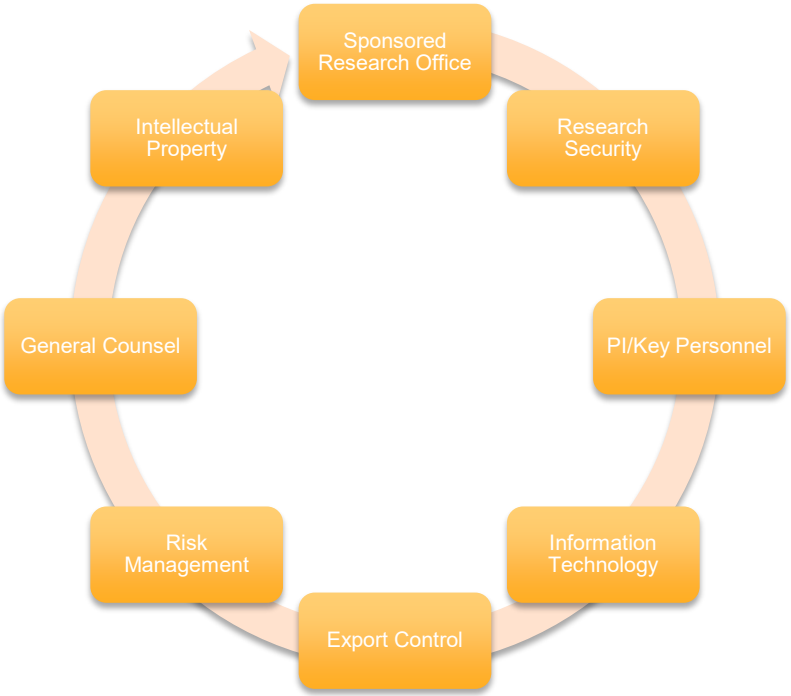
DFARS clause 252.204–7020, NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

- notifies contractors that DoD reserves the right to conduct a higher-level assessment of contractors' cybersecurity compliance, and contractors must give DoD assessors full access to their facilities, systems, and personnel.

DFARS clause 252.204–7021, CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS

- paves the way for rollout of the CMMC Program. Once CMMC is implemented, DFARS clause 252.204–7021 requires contractors to achieve the CMMC level required in the DoD contract.

University stakeholders



Burning Questions

How does your University handle this?

- What does this cost?
  - Varies significantly
    - University research portfolio
      - Project specific
- Who Pays?
  - Varies significantly
    - University/F&A
      - Service Center model
        - Project Specific

Resources

- Federal Register :: Cybersecurity Maturity Model Certification (CMMC) Program
- About CMMC (defense.gov)
- DVIDS - Video - Cybersecurity Maturity Model Certification (CMMC) Proposed Rule Overview (dvidshub.net)

2024 SRAI SO/NE
SECTION MEETING
HILTON HEAD, SC
MAY 7 - 10

Attain Partners

Questions? Concerns? Comments? Thank you!

Andrea Deaton, MHR, CRA
Attain Partners, LLC
addeaton.ctr@attainpartners.com
405.613.1417