Cybersecurity Maturity Model Certification (CMMC)

Panelists:
David Furman, JD, University of South Alabama
Russ Ward, MBA, University of Alabama in Huntsville
Moderator:
Andrea Deaton, CRA, Attain Partners, LLC

Cybersecurity Maturity Model Certification (CMMC) is a critical topic that impacts the security and integrity of our nation's research endeavors. The role of the research administrator is pivotal to CMMC compliance.

As we all navigate the complexities of cybersecurity compliance, the CMMC framework provides a structured approach to safeguarding our data and research assets. This presentation will explore the key components of CMMC, its relevance to your institution, and how research administrators can effectively manage and support compliance efforts.

Objectives

- Understand key components of CMMC
- Identify ways to support CMMC requirements and compliance at your institution

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.

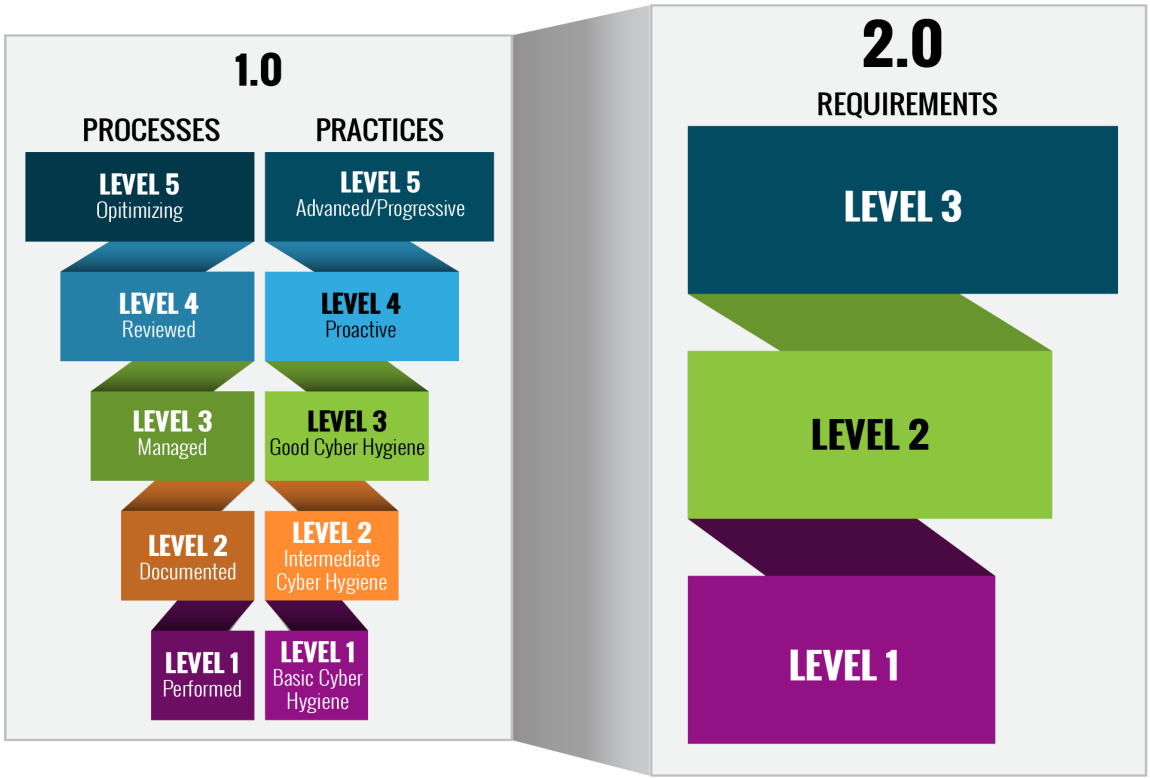
2021 CMMC 2.0 was announced and attempted to streamline the expectations of the previous models by downsizing the transitionary levels of 2 and 4.

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.

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.

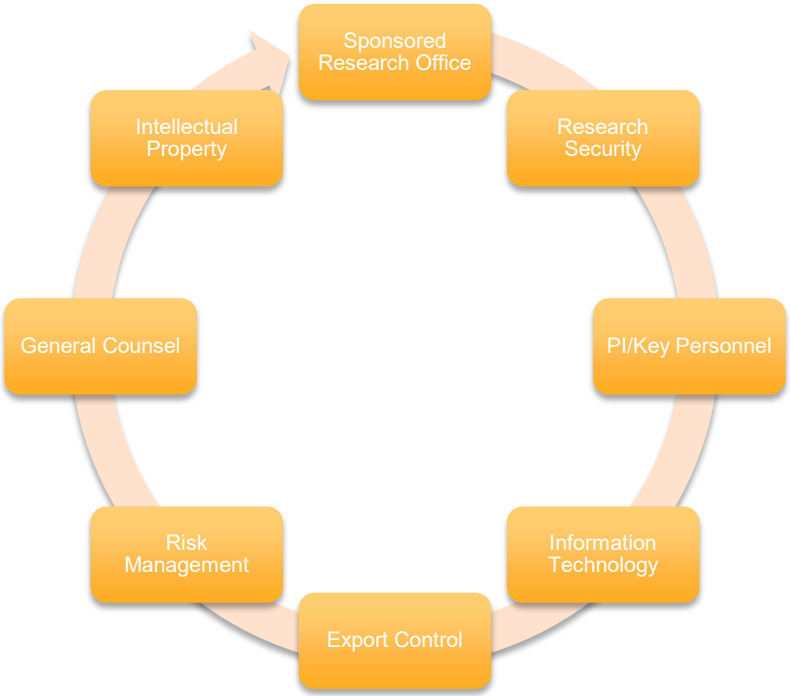
DFARS clause 252.204–7020, NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS

- 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



Questions for Panelists

- Background
- Evolution
- Cost
- Role of Research Administrator
- Deadlines
- Award Language
- Other Federal Agencies
- Deadlines
- Assessments
- Penalties
- Levels

SRA INTERNATIONAL

SOCIETY OF RESEARCH ADMINISTRATORS INTERNATIONAL

Wrap up!

Thank you!