aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

Cybersecurity Maturity Model Certification (CMMC) Overview

What Government Contractors Need to Know to Prepare

September 21, 2021

Is NIST 800-171 Requirement Going Away?

DFARS* clause 252.204-7012 Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting

- **Effective December 31, 2017**
- Implement NIST SP 800-171 “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” and self-attest to meeting requirements

DFARS Case 2019-D041 Assessing Contractor Compliance with Cybersecurity Requirements

- **Effective November 30, 2020 (Interim Rule)**. Final rule expected TBD pending Congressional Review
- Provides DoD with the ability to assess a contractor’s implementation of NIST SP 800-171 security requirements

DFARS clause 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements

- Requires contractors to post summary level scores of a current NIST SP 800-171 DoD Assessment (i.e. not more than 3 years old) to the Supplier Performance Risk System (SPRS)

DFARS clause 252.204-7021 Cybersecurity Maturity Model Certification (CMMC) Requirements

- Requires contractors to have a current (not older than 3 years) CMMC certificate at the CMMC level required by the contract and maintain the certificate for the duration of the contract

*DFARS - Defense Federal Acquisition Regulation Supplement

Cybersecurity Maturity Model Certification (CMMC) Overview

What is CMMC?

- CMMC is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB).
- Encompasses 5 maturity levels ranging from Level 1 - “Basic Cybersecurity Hygiene” to Level 5 - “Advanced”.

Why is it Important?

- CMMC will be a requirement for all future DOD contract awards.
- Ensures & verifies appropriate levels of cybersecurity practices and processes are in place to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) on DIB networks/systems.

Who Does It Impact?

- Department of Defense (DOD) contractors and subcontractors
- Note: Vendors that only produce Commercial-Off-The-Shelf (COTS) products are *excluded*

When Does It Take Effect?

- Rolling implementation effective FY21 (October 2020)
- By FY26 (October 2025), all DOD contracts will contain CMMC requirement (DFARS 252.204-7021 Interim Rule)

How does CMMC differ from NIST 800-171?

CMMC

- Requires 3rd Party Certification
- Pass/Fail Certification (no POAMs)
- Multi-level certification
- Process maturity expectation (ML2+)
- Recertification required every 3 years
- Includes minimum requirement to process Federal Contract Information (FCI)

NIST 800-171

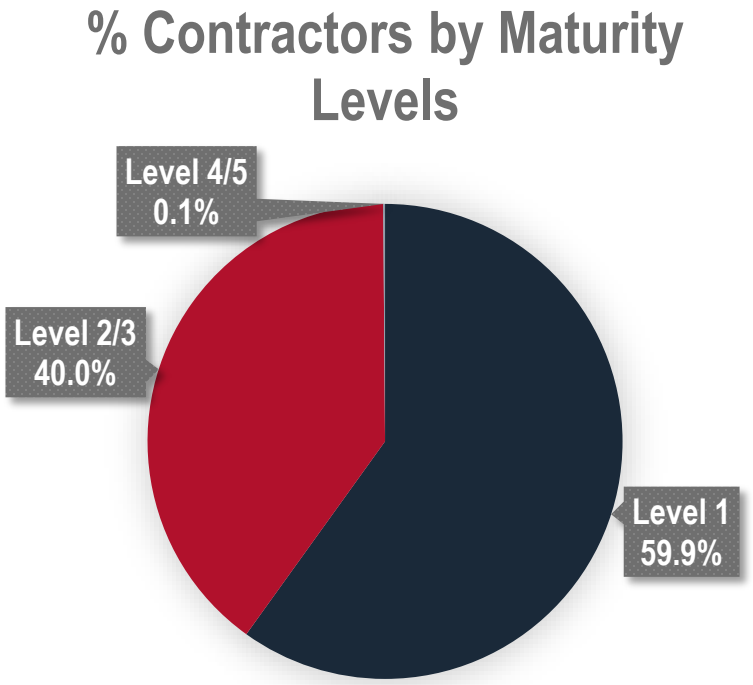
- Self-Assessment & Attestation
- Flexibility to adjust scope (tailoring) and have outstanding POAMs
- Single level certification
- No process maturity requirements
- One-time assessment
- Only applies to protection of CUI

CMMC ML 3 is equivalent to NIST 800-171 + 20 more security practices & process maturity expectations.

What Does CMMC Mean for Government Contractors?

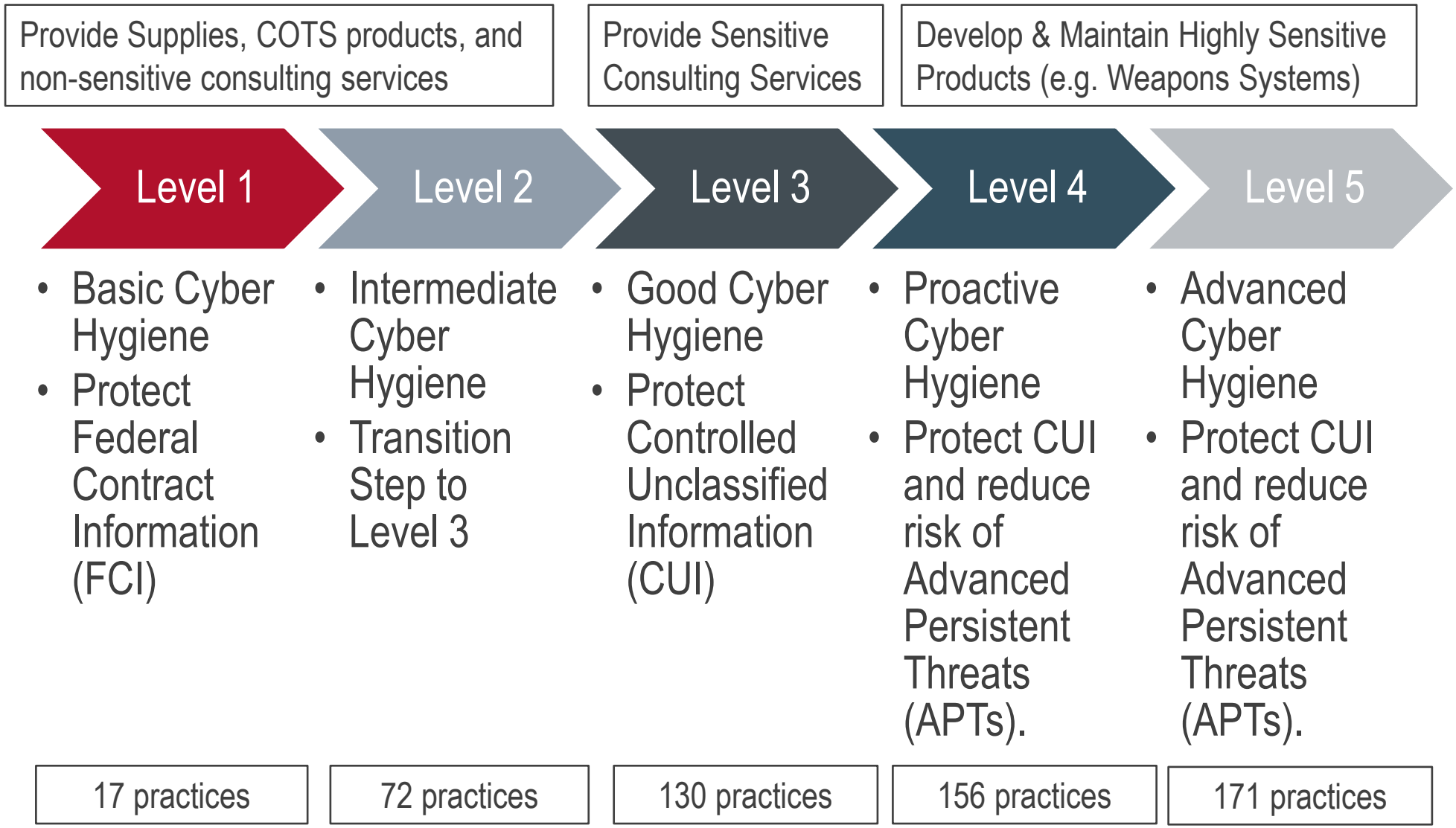
All DOD* prime and sub contractors (~300K entities) will have their IT security controls assessed by a 3rd party and certified to meet one of the 5 prescribed maturity levels.

- Maturity levels range from Level 1 (lowest) to Level 5 (highest) with majority at ML3 or lower
- 5 Year procurement cycle to get 100% of DOD contractors certified (beginning FY21)
- CMMC Certification will need to be renewed every 3 years
- Costs of achieving & obtaining certification are an allowable, reimbursable indirect cost



* Other Federal agencies are interested & planning limited implementation of this framework e.g. GSA, DHS, Treasury, etc.

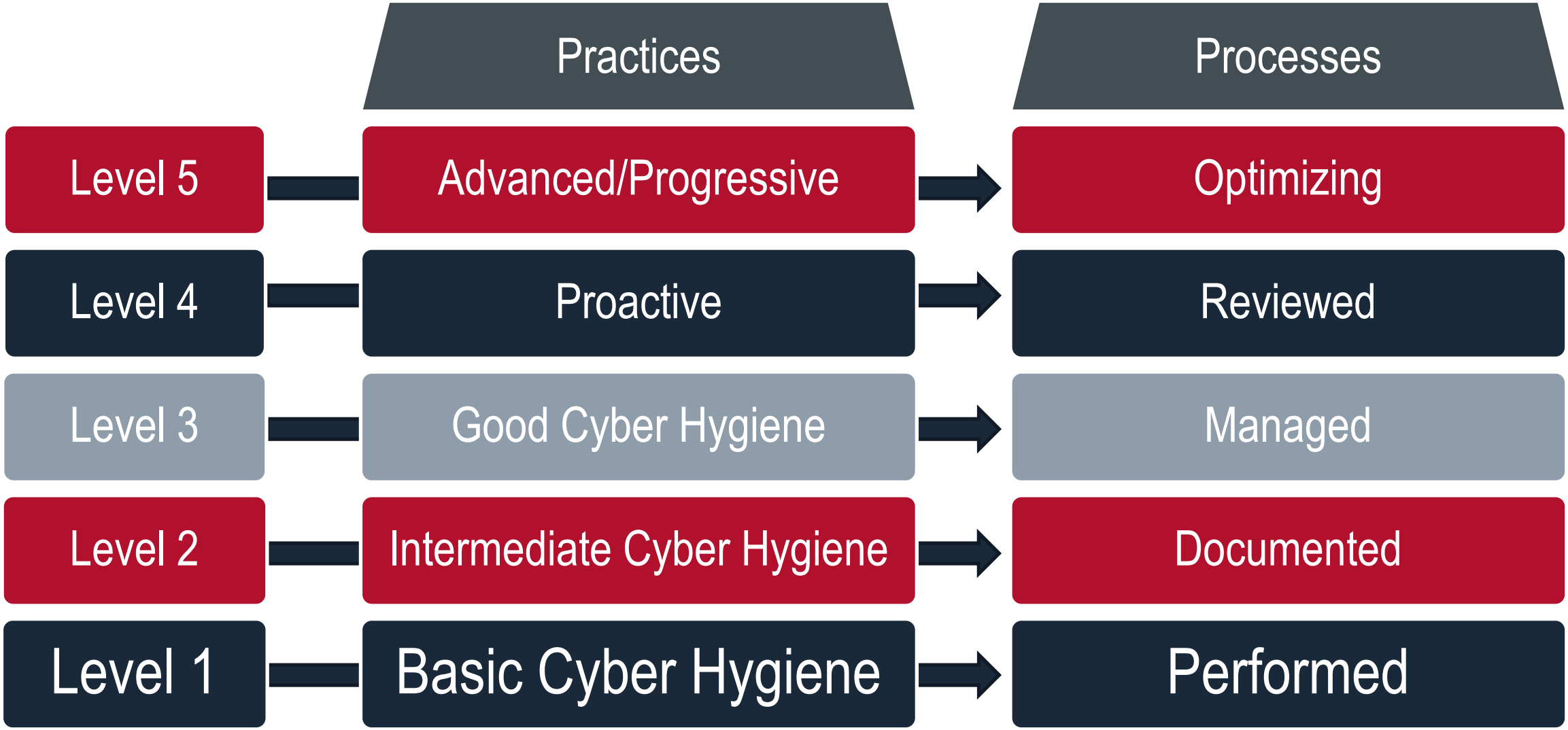
How do you determine what CMMC level applies to your company?



What are the CMMC Process Maturity Expectations?

Level 1 (Performed)	• Performs specified practices in an ad-hoc manner • Note: Process maturity is not assessed at Level 1
Level 2 (Documented)	• Establish and document practices and policies • Organization executes processes as documented
Level 3 (Managed)	• Establish, maintain and resource a management plan • Includes information on mission, goals, training, & stakeholders
Level 4 (Reviewed)	• Review and measure practices for effectiveness • Take corrective action when necessary & update management
Level 5 (Optimizing)	• Standardize and optimize process implementation

CMMC = Prescribed Security Practices + Process Maturity



Key Considerations

System Boundary Discussions

- Where does FCI or CUI exist in your environment?

Supplier Performance Risk System (SPRS)

- Have you submitted your NIST SP 800-171 Assessment Results?
- https://www.sprs.csd.disa.mil/

Subcontractor flow downs

- Prime contractors are expected to flow-down CMMC requirements to subcontractors

Challenges/Risks & Mitigations

DOD may delay or slow down projected pace of including CMMC requirements in contracts	• NIST 800-171 requirements are still in effect for many DOD contractors
Limited number of CMMC Third Party Assessment Organizations (C3PAO)	• Opportunity to prepare by getting an information assessment from a RPO or other cybersecurity firm
Firms are unaware of how much will be required to achieve compliance (time, money, people)	• Costs to achieve compliance are allowable so it is important to properly account for CMMC costs
CMMC Model will evolve over time to address new security practices and requirements	• Getting familiar with meeting existing expectations will better prepare you for future requirements
Other agencies may develop CMMC-like compliance requirements	• Watch and wait!

Common Misconceptions

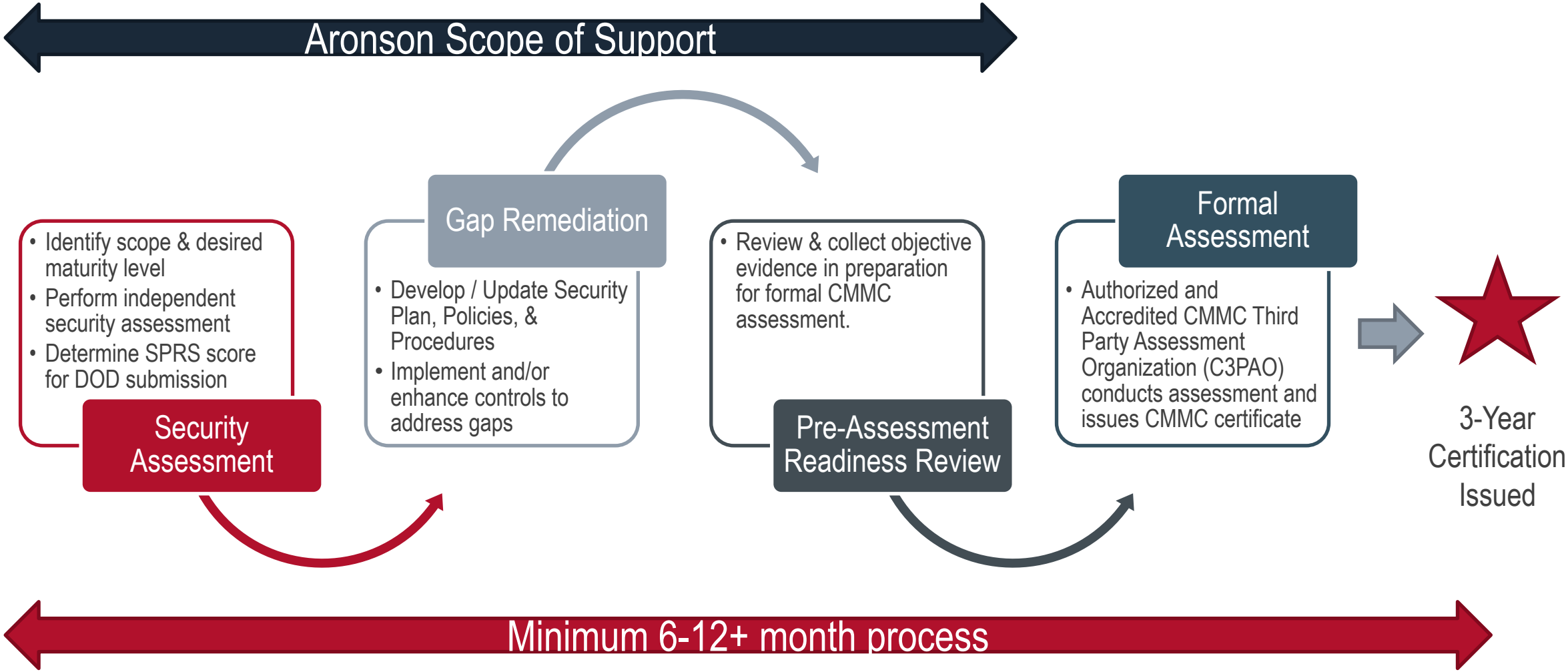
I can outsource my risk / compliance expectations

- I can buy CMMC compliance via a product or suite of products
- I can fully outsource my CMMC compliance responsibilities to a 3rd party

I can afford to wait (I have time to prepare)

- CMMC certification is required upon contract award
- There will be a backlog of C3PAOs and assessors to conduct assessments initially

What Should I Do Next (CMMC Journey Map)?



Aronson is a CMMC-AB* Registered Provider Organization (RPO)

CMMC | NIST 800-171

Quick Pre-Assessment

Provide an analysis of how organization is doing against selected standards.

CMMC | NIST 800-171

Advisory Support

Develop strategy and security roadmap to achieve compliance with selected standards.

CMMC | NIST 800-171

Remediation Support

Help address the gaps in organization security posture relevant to the standard.

AND/OR

CMMC | NIST 800-171

Develop / Update Policies

Review, create and/or update policies and map to relevant controls.

CMMC

CMMC Pre-Assessment Readiness Review

Assist with review & collection of objective evidence in preparation for formal CMMC assessment.

CMMC

Cost Allocation & Recovery Support

Provide recommendations for maximizing cost recovery within indirect rate structure.

Contact & Connect with Us

202.869.0995

cmmc@aronsonllc.com

https://aronsonllc.com/service/cmmc-advisory/

aronson LLC
ASSURANCE | TAX | CONSULTING

111 Rockville Pike, Suite 600
Rockville, MD 20815
301.231.6200 | **www.aronsonllc.com**

aronson LLC
ASSURANCE | TAX | CONSULTING
Expanding What's Possible

About Aronson

Aronson Government Contract Services Group

Government Contract Services Group

Nearly **800** government contractor clients served annually

85+ professionals dedicated to supporting government contractors

Unique insights and experiences that empower our client's success

Azunna Anyanwu

Director, CMMC Advisory & Director of Information Technology

Azunna Anyanwu leads the Technology & Security Advisory practice for Aronson. With 20 years of experience in IT operations and strategy, cybersecurity, business process reengineering, agile methodologies, and more, Azunna brings a unique and diverse technical skillset that has proven invaluable to the firm. Azunna also oversees IT operations, cybersecurity, and digital business transformation activities for Aronson. Prior to joining Aronson, Azunna served as the Director of IT at a federal government contractor as well as 12+ years in Big 4 consulting delivering solutions for state and federal government clients.

Azunna has led the implementation of security programs that addressed cybersecurity gaps to demonstrate NIST 800-171 compliance. He has also led the development of multiple federal applications and supported the certification and accreditation (C&A) process to achieve Authority to Operate (ATO). Azunna also has experience teaching graduate level courses on Information and Systems Security at the George Washington School of Engineering. He is a frequent contributor and speaker on Cybersecurity and IT Operations topics at industry and vendor-sponsored events.

Azunna graduated from Harvard University with a Bachelor of Arts in Computer Science; The John Hopkins University with a Master of Science in Computer Science; and the Quantic School of Business & Technology with an Executive Master's of Business Administration.

Azunna's CMMC-AB RP Profile is at: https://portal.cmmcab.org/marketplace/azunna-anyanwu/

301 231 6235

aanyanwu@aronsonllc.com