Accelerating DIB Supply Chain Security

Standards, Practices, Solutions

http://cmmc-coe.org

JOHN WEILER, CO-FOUNDER/EXEC DIRECTOR

RAVINDRA GARG, CHIEF OPERATING OFFICER

BOB DIX, SVP POLICY & STRATEGY

GARY WANG, FORMER NAVY CTO, OUSD(I) CIO, ARMY DCIO

SUMMER 2020

What is CMMC…

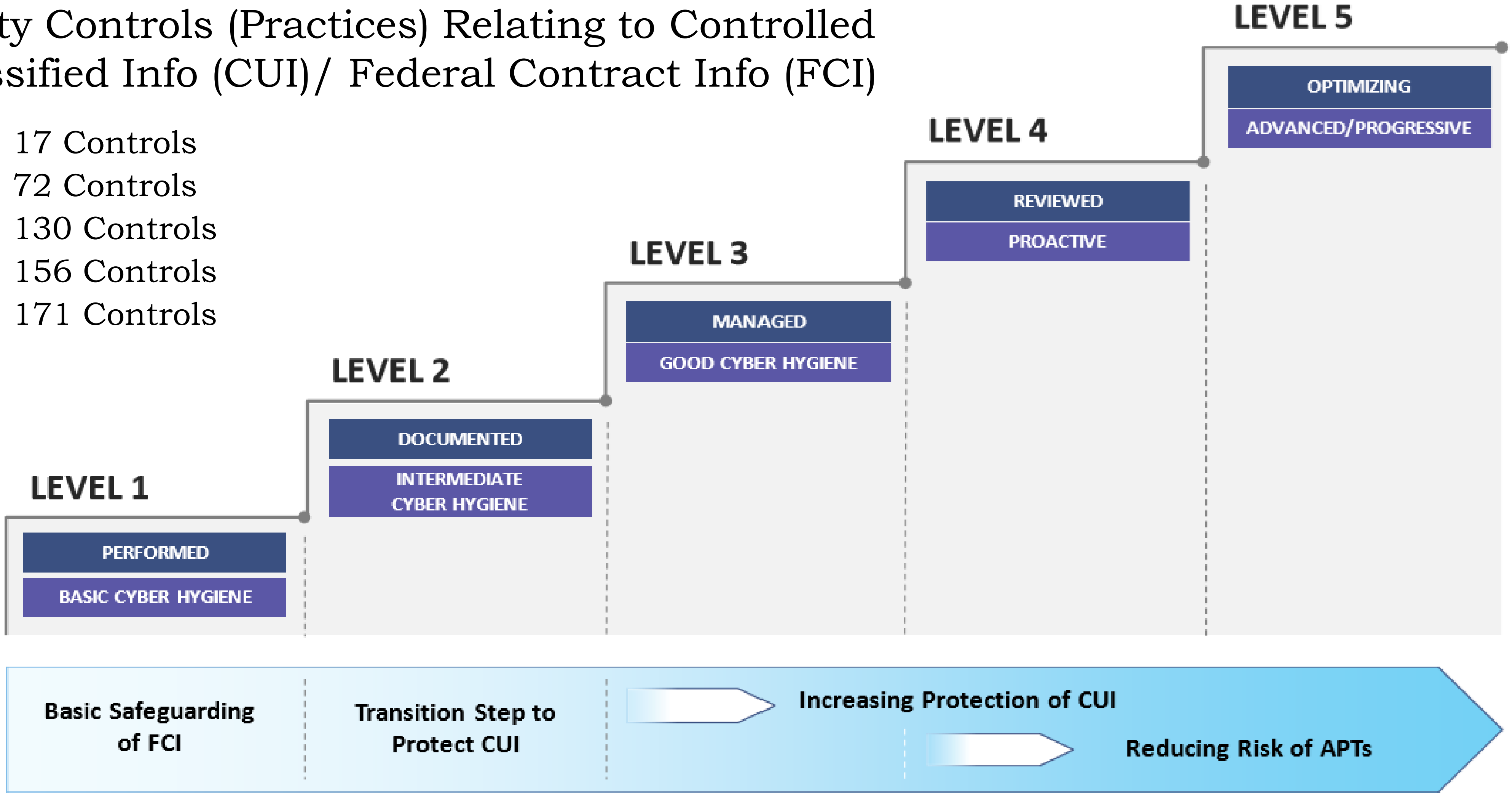
- Cybersecurity Maturity Model (CMM) is primarily a build out of NIST 800-171 Security Standard that allows Cybersecurity compliance Level 1-5, with 3-4-5 being necessary for most DIB Primes. Focuses on protecting CUI & FCI.
- Targeted to be in 10 initial "pathfinder" Contracts in September 2020.
- Will be integrated into additional contracts over a 5-year period.
- By 2026, CMMC requirements will be in all DoD contracts.
- Third-party Assessment of DIB Contractors for cybersecurity maturity based on the CMMC model. www.CMMCab.org

CMMC-AB has established a Strategic Relations Group that will forge partnerships with leading non-profits, DIB Trade Groups and Cyber Communities of Practice to accelerate adoption and implementation.

Cybersecurity Maturity Levels…

Security Controls (Practices) Relating to Controlled Unclassified Info (CUI)/ Federal Contract Info (FCI)

Level 1 - 17 Controls
Level 2 - 72 Controls
Level 3 - 130 Controls
Level 4 - 156 Controls
Level 5 - 171 Controls

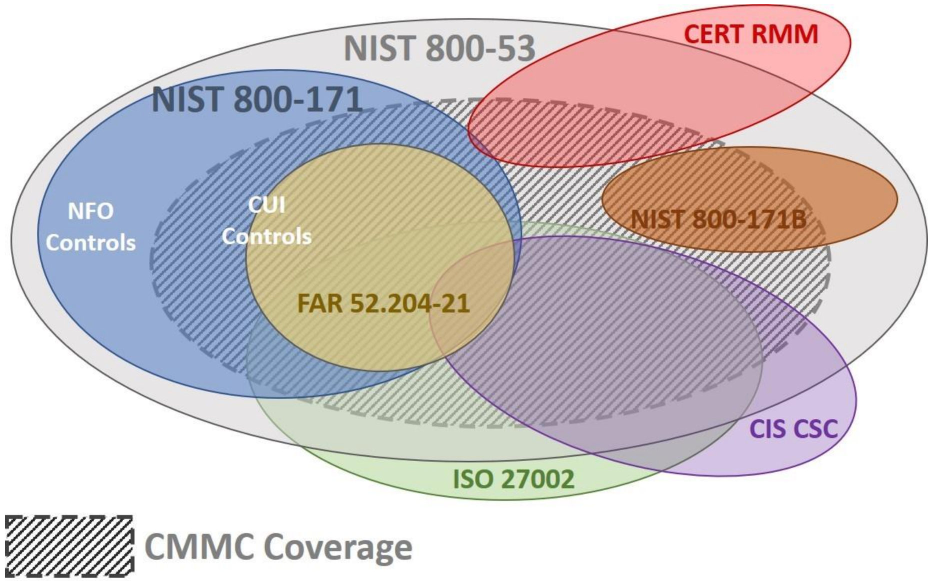


CMMC & NIST 800-171…

DOD CIO requested NIST to build out 800-53 Standards and establish a **Cyber Certification Framework NIST 800-171**.

OUSD A&S commissioned JHAPL (UARC) and SEI CERT (FFRDC) to expand NIST 800-171 into a **Cybersecurity Maturity Model** that is auditable and supports 5 maturity levels of CUI and FCI data handling.

CMMC Levels 1-3 encompass the 110 security requirements specified in NIST SP 800-171 rev1. **Additional practices and processes** are incorporated from other standards.



Note: NIST 800-53 in its entirety, is the key part of the new CMMC-COE Cyber Reference Architecture

Why the DoD Created CMMC…

Cybersecurity incidents have a negative impact on National Security.

This Photo by Unknown Author is licensed under CC BY-SA

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)

A new ransomware attack occurs every 14 seconds (Herjavec Group)

Ransomware-as-a-service and open source malware are reducing barriers to entry for criminals (Sonicwall)

The average data breach costs $3.9 Million worldwide, $8.9 Million in USA (Ponemon Institute)

CMMC-COE Mission…

Our mission, focused on DIB cybersecurity objectives, cost containment and expeditious CMMC compliance. Provide methods, technologies, expertise and education needed to enable the DIB improve cyber hygiene and resilience, via a cost effective and efficient collaboratory.

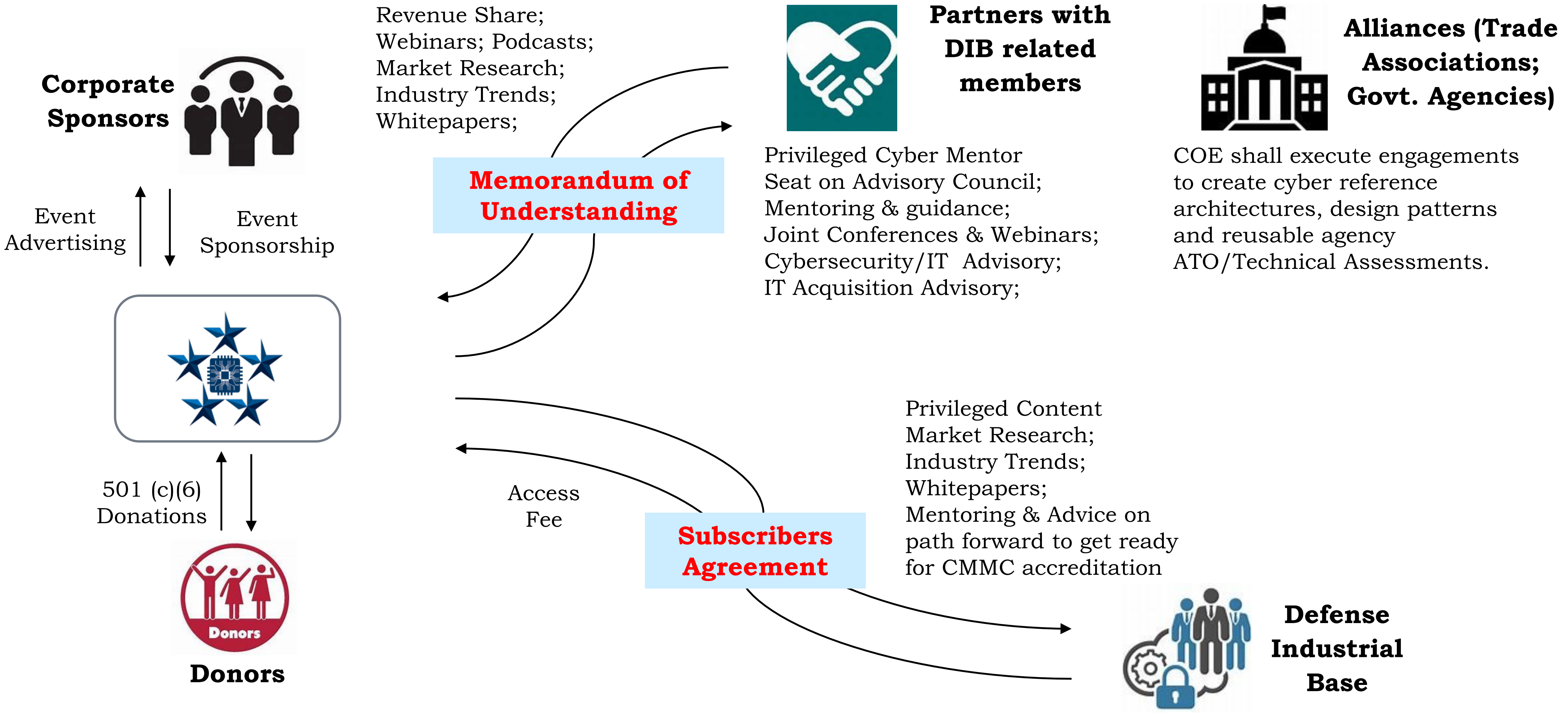
Vision…

As a unique non-profit public-private partnership, our vision is to accelerate Cybersecurity Maturity Model (CMM) adoption, and reduce time & cost for security compliance for our partners by leveraging commercial best practices, CMMC standards, and innovative solutions for a measurable success.

Strategic Goals…

- IT-AAC's expanded its Public/Private Partnership to establish the CMMC-COE.org to empower leading DIB and Cyber standards bodies, industry groups, and the DIB communities of practice. Advance, enhance and compliment diverse cybersecurity standards, supply chain risk management, industry cyber practices and emerging cyber solutions proven to improve cyber resilience.
- Operating at the intersection of technology, innovation and policy, CMMC-COE strives to establish a robust framework for collaborative knowledge sharing of standards, best practices, design patterns and cyber reference architectures in the CMMC ecosystem.
- Supported by corporate sponsors and donors, CMMC-COE aims to facilitate mentoring and guidance to the DIB through regular conferences, webinars, and the networking events in the CMMC ecosystem.
- CMMC-COE desires to be a honest broker and act as an Industry Advisory Council to Congress, Executive Branch and the White House on market innovation in cyber standards, practices and solutions.

Partnerships & Alliances…



Corporate Sponsors

Event Advertising

Event Sponsorship

501 (c)(6) Donations

Donors

Revenue Share;
Webinars; Podcasts;
Market Research;
Industry Trends;
Whitepapers;

Memorandum of Understanding

Partners with DIB related members

Privileged Cyber Mentor
Seat on Advisory Council;
Mentoring & guidance;
Joint Conferences & Webinars;
Cybersecurity/IT Advisory;
IT Acquisition Advisory;

Alliances (Trade Associations; Govt. Agencies)

COE shall execute engagements to create cyber reference architectures, design patterns and reusable agency ATO/Technical Assessments.

Access Fee

Subscribers Agreement

Privileged Content
Market Research;
Industry Trends;
Whitepapers;
Mentoring & Advice on path forward to get ready for CMMC accreditation

Defense Industrial Base