PREPARING FOR THE CYBERSECURITY MATURITY MODEL CERTIFICATION

Tulsa SAME Chapter – March Meeting

March 16, 2021

guernsey
ENGINEERS
ARCHITECTS
CONSULTANTS

CMMC–AB
PROVISIONAL
ASSESSOR

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
C3PAO

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED

TIM FAWCETT, CISSA, CISSP

DIRECTOR OF CYBERSECURITY CONSULTING

CMMC–AB PROVISIONAL ASSESSOR

- 20 YEARS OF INFORMATION ASSURANCE EXPERIENCE PERFORMING IT AUDITS, RISK ASSESSMENTS, AND CYBER THREAT AND VULNERABILITY ANALYSES
- CONSULTED FOR SCORES OF COMPANIES FROM START-UPS TO FORTUNE 500 COMPANIES
- CERTIFIED INFORMATION SECURITY PROFESSIONAL, A CERTIFIED INFORMATION SYSTEMS AUDITOR, CMMC PROVISIONAL ASSESSOR

CYBERSECURITY SERVICES

- RISK ASSESSMENT / GAP ANALYSIS
- CMMC SUPPORT
- CYBER PROGRAM DEVELOPMENT
- INCIDENT MANAGEMENT
- PENETRATION TESTING
- INVESTIGATION AND FORENSICS
- CONFIGURATION AUDITING
- VULNERABILITY ANALYSIS AND MANAGEMENT
- TRAINING AND AWARENESS
- GSA SCHEDULE 70 HACS

AGENDA

- DEFENSE SUPPLY CHAIN
- CERTIFICATION REQUIREMENTS
- CMMC ECOSYSTEM
- IMPLEMENTING THE CMMC MODEL

DEFENSE SUPPLY CHAIN

DEFENSE INDUSTRIAL BASE (DIB)

The worldwide industrial complex that enables research and development as well as design, production, delivery, and maintenance of military weapons systems/software systems, subsystems, and components or parts, as well as purchased services to meet US Military requirements.

- Domestic and foreign entities
- Worldwide production assets
- 200,000+ DIB companies and subcontractors
- Military weapon systems and subsystems
- Systems, components, and parts

DoD SUPPLY CHAIN (DSC)

EXTENDING BYOND THE DIB

Examples:

- Food suppliers
- Janitorial services
- Construction and excavation
- Office and computer equipment
- Telecommunications

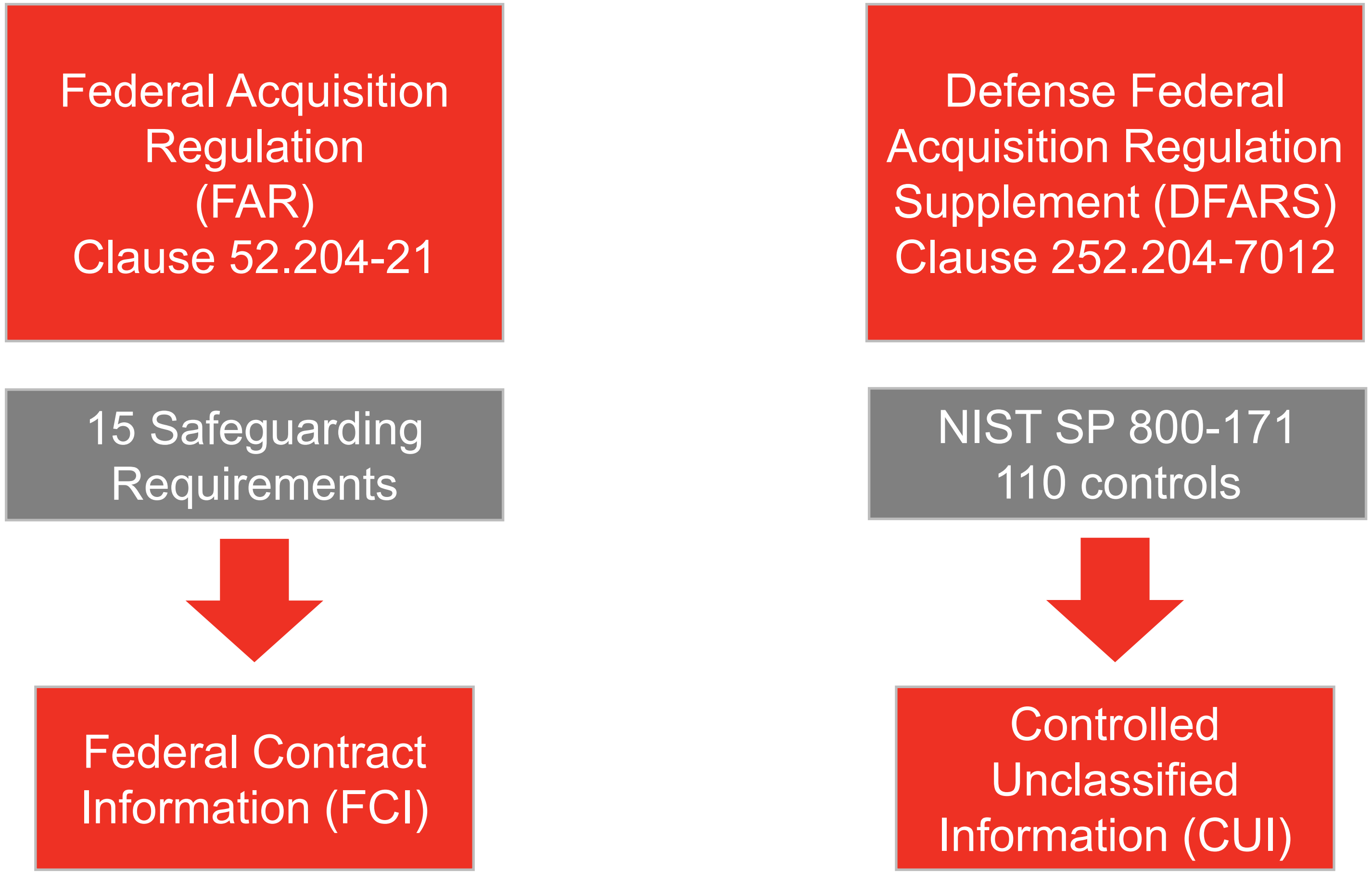
Risks:

- Business E-mail compromise
- Island hopping
- Supply chain disruption
- Supply chain corruption
- Troop Movements

SAFEGUARDING INFORMATION

CERTIFICATION REQUIREMENTS

CURRENT SAFEGUARDING OBLIGATIONS



Federal Acquisition Regulation (FAR) Clause 52.204-21

15 Safeguarding Requirements

Federal Contract Information (FCI)

Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012

NIST SP 800-171 110 controls

Controlled Unclassified Information (CUI)

SELF DoD CERTIFICATION

FAR 52.204-21

Most FAR-based contracts, including contracts with non-DoD federal agencies, include FAR 52.204-21. Contracts that don’t explicitly include it may still have it read in under the Christian Doctrine.

> (The **Christian doctrine** provides that a mandatory statute or regulation that expresses a significant or deeply ingrained strand of public procurement policy shall be read into a federal contract by operation of law, even if the clause is not in the contract.)

SELF DoD CERTIFICATION

DFARS 252.204-7012

DFARS contracts that involve CUI are supposed to include DFARS 252.204-7012. Again, may be read in under the Christian Doctrine if it isn't there.

By signing a contract with the federal government, contractors are attesting that they meet these requirements.

FEDERAL CONTRACT INFORMATION (FCI)

INFORMATION NOT INTENDED FOR PUBLIC RELEASE

Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government

Examples:

- Nonpublic information provided to a contractor (e.g., with a request for proposal).
- Information developed during the course of a contract, grant, or other legal agreement (e.g., draft documents, reports, or briefings and deliverables).
- Privileged information contained in transactions (e.g., privileged contract information, program schedules, or contract-related event tracking).

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

INFORMATION THAT REQUIRES SAFEGUARDING

Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies.

- Digital, physical documents, representations, images, and items (parts).

- Executive Order 13556 and 32 CFR, part 2002 designates the National Archives and Records Administration (NARA) as CUI Executive Agent for the CUI Registry. Their guidance is binding.

⚠ The term does not include information that is lawfully publicly available without restrictions or classified information.

INTERIM RULE

DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. DoD Assessment Methodology

Interim Rule: Creates the following new solicitation provision and contract clauses:

- **DFARS 252.204-7019** – Contractors submit their self-assessment compliance score to DoD
- **DFARS 252.204-7020** – Self-assessment required for awards starting November 30, 2020; Contractor gives access to DCMA auditors to validate their self-assessment; Roll down to Subcontractors
- **DFARS 252.204-7021** –Implements the CMMC over 5 years.

FALSE CLAIMS ACT

ANY PERSON WHO KNOWINGLY SUBMITS FALSE CLAIMS TO THE GOVERNMENT

- Any person who knowingly submits false claim to the government.
- The Department of Justice obtained more than $3 billion in settlements and judgments from civil cases involving fraud and false claims against the government in the fiscal year ending Sept. 30, 2019.
- Claims can be brought by whistleblowers who get between 15% and 30% of the award.

1 - United States v. Aerojet Rocketdyne Holdings, Inc., 381 F. Supp. 3d 1240 (E.D. Cal. 2019)
2 - United States ex rel. Glenn v. Cisco Systems, Inc., No. 1:11-cv-00400- RJA (W.D.N.Y. July 31, 2019)

DFARS CLAUSE 252.204-7012

CLOUD SERVICE PROVIDER REQUIREMENTS

If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract

- The cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline. (Sovereignty Requirements)

- Plus: The cloud service provider must comply with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

CMMC ECOSYSTEM

CMMC HISTORY AND INDEPENDENCE

FORMATION OF CMMC-AB

- CMMC-AB was formed as an independent non-stock corporation in January 2020. Formal recognition as a nonprofit entity with the US Internal Revenue Service (IRS) is pending.

- The CMMC-AB operates like any other private nonprofit organization.

- Independence does not mean information is siloed – strong relationships with OSD(A&S) and DoD

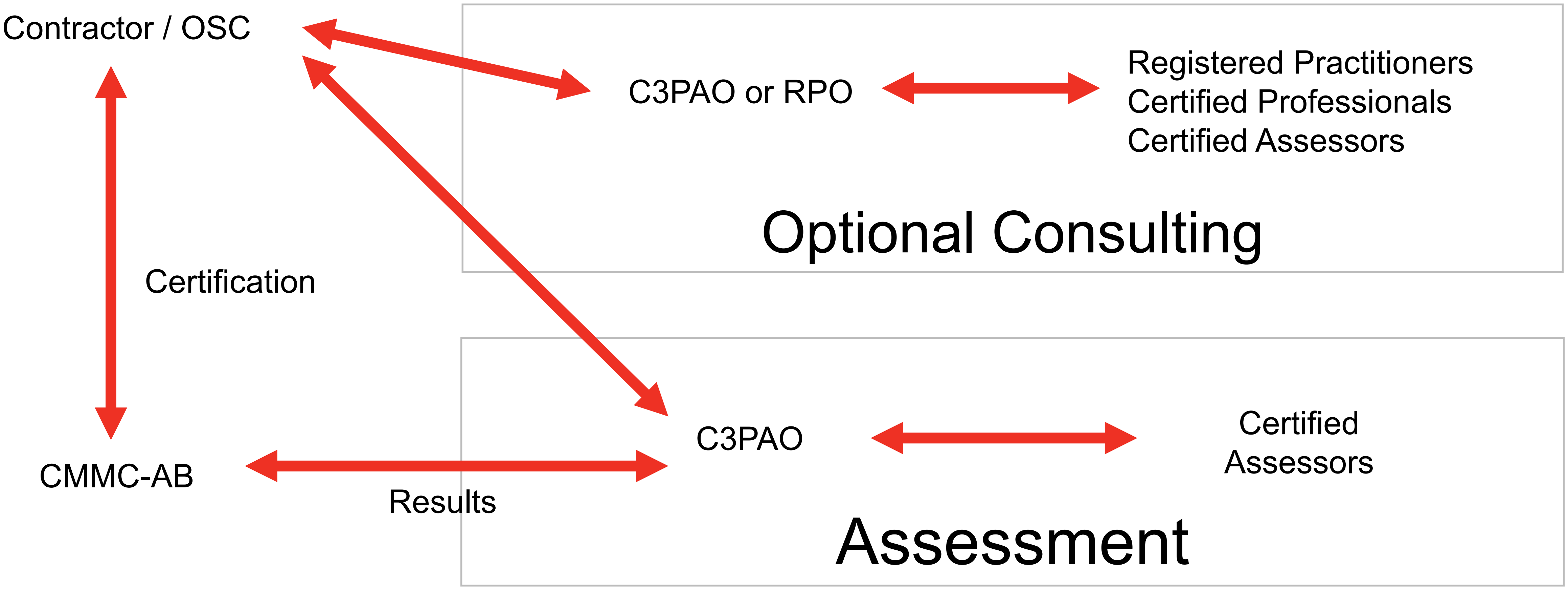
CMMC PARTICIPANTS

WHO IS INVOLVED WITH CMMC?

- **Reliant Organizations**
- **Organizations Seeking Certification**
- **Individuals Performing Services**
    - Registered Practitioners
    - Certified Professionals
    - Certified Assessors
- **Service Provider Organizations**
    - Registered Provider Organizations (RPO)
    - Certified Third Party Assessment Organizations (C3PAO)

CONSULTING AND CERTIFICATION PROCESS

OPTIONAL CONSULTING VS ASSESSMENT



Contractor / OSC

C3PAO or RPO

Registered Practitioners
Certified Professionals
Certified Assessors

Optional Consulting

Certification

C3PAO

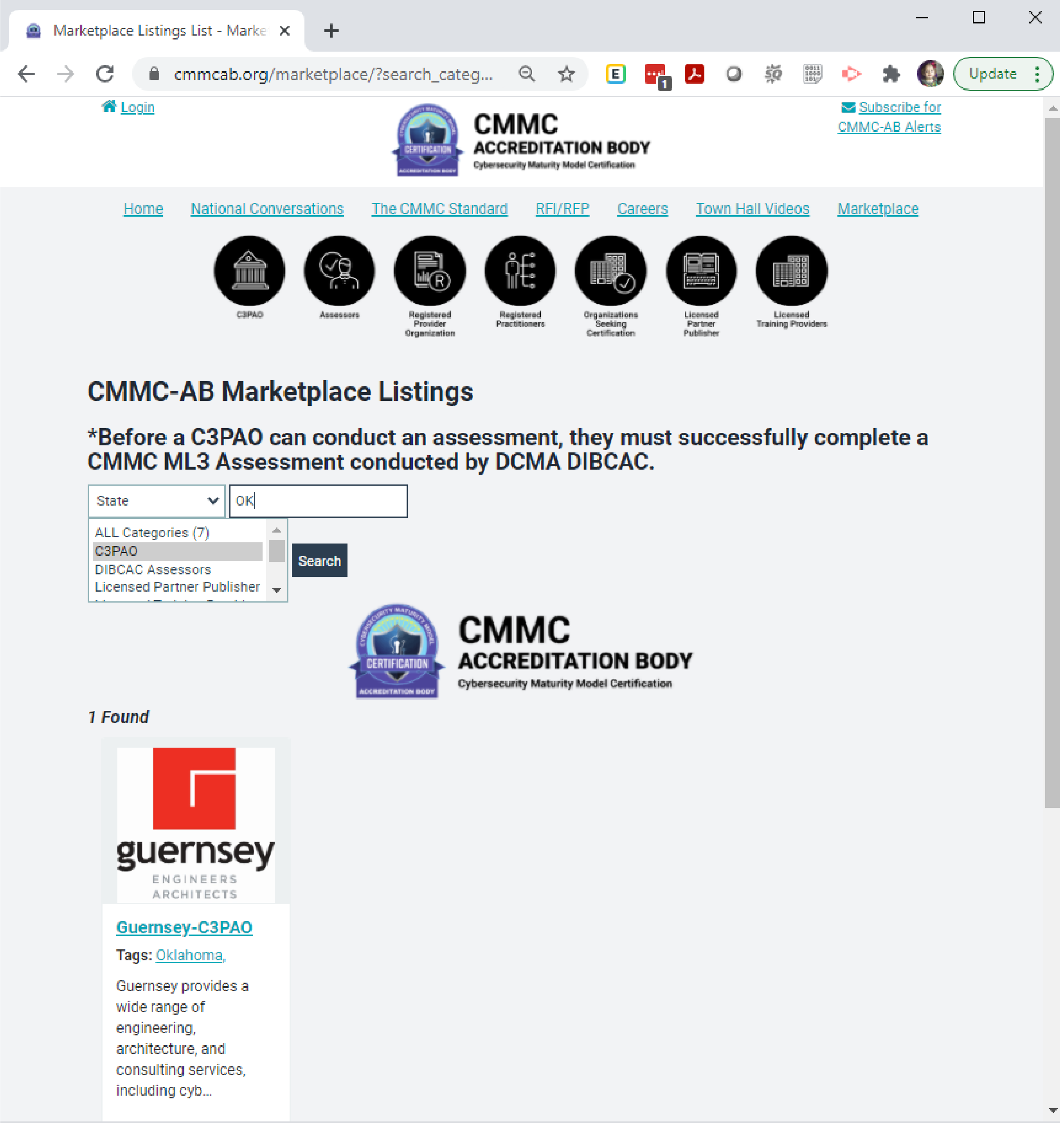
Certified Assessors

CMMC-AB

Results

Assessment

CMMC Marketplace


Marketplace Listings List - Marke
cmmcab.org/marketplace/?search_categ...
Update
Login
CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification
Subscribe for CMMC-AB Alerts
Home
National Conversations
The CMMC Standard
RFI/RFP
Careers
Town Hall Videos
Marketplace
C3PAO
Assessors
Registered Provider Organization
Registered Practitioners
Organizations Seeking Certification
Licensed Partner Publisher
Licensed Training Providers
Search
CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification
guernsey
ENGINEERS
ARCHITECTS

CMMC-AB Marketplace Listings

***Before a C3PAO can conduct an assessment, they must successfully complete a CMMC ML3 Assessment conducted by DCMA DIBCAC.**

State: OK

ALL Categories (7)
C3PAO
DIBCAC Assessors
Licensed Partner Publisher

1 Found

Guernsey-C3PAO

Tags: Oklahoma,

Guernsey provides a wide range of engineering, architecture, and consulting services, including cyb...

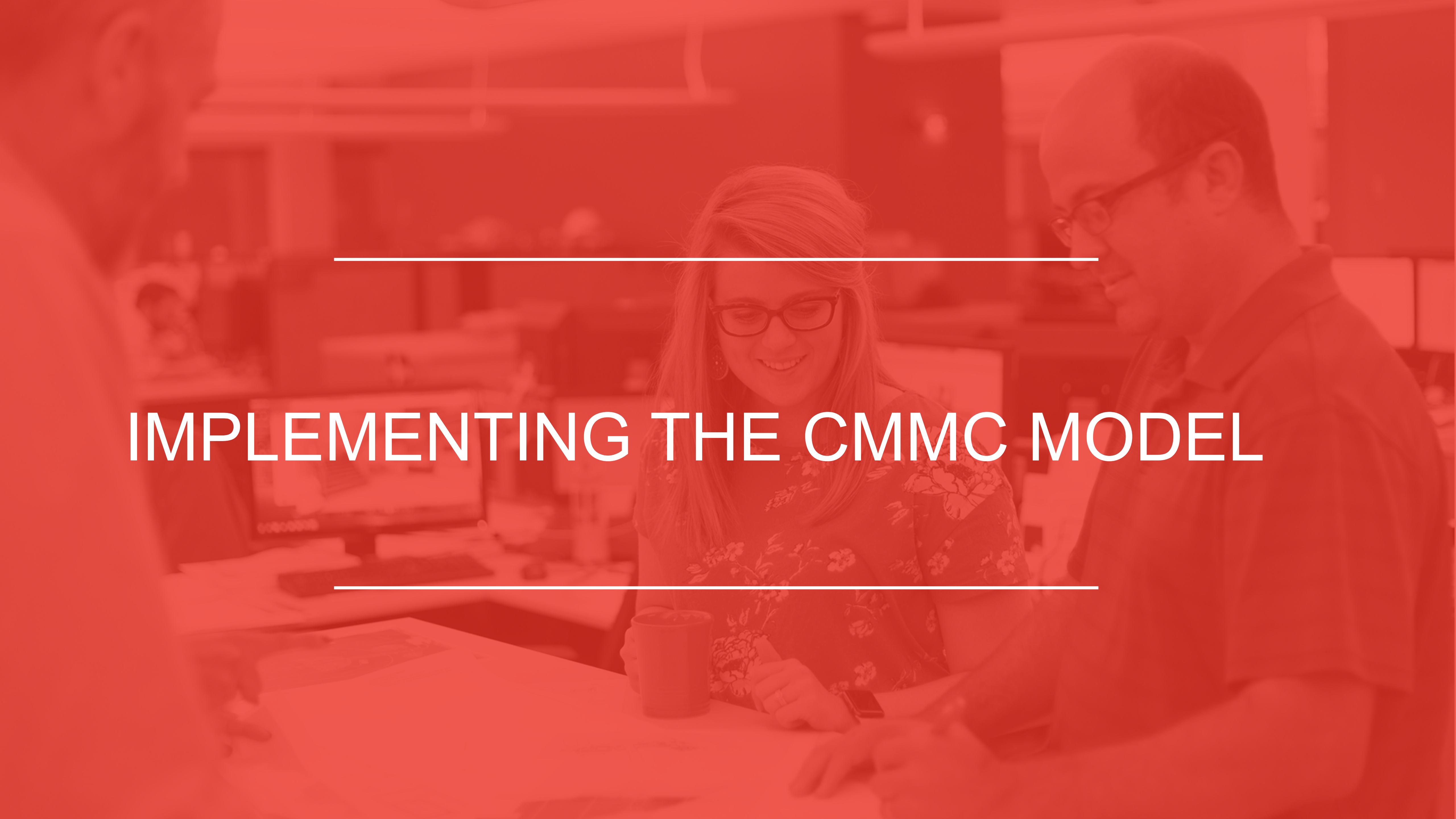
Rumor Mill

Approved C3PAOs
The DOD has added two requirements that must be completed prior to conducting an assessment: The C3PAO must complete a CMMC ML3 Assessment, and a Tier 3, non-clearance Suitability Determination.
As far as we know, the DOD has not yet scheduled with DIBCAC for the CMMC ML3 Assessments, and no background checks have been conducted. This is 100% on them, and we have no control over their actions. **- Jeff Dalton**

Reciprocity
They are supposed to make an announcement about reciprocity (like DCMA High) soon. Sounds like it's going to require delta assessments of the additional practices that CMMC brings to the table. **– Jeff Dalton**

FYI Per the DOD:
C3PAOs (and their assessor) that wish to perform Level 1 Assessments do NOT require a DIBCAC Level 1 CMMC Assessment. **- Jeff Dalton**

Cost
I have been trying to track this closely, and I haven't seen anything either. It isn't clear if it will just be assessment costs that are allowable or if the preparation and maintenance/operation is also allowable. And what happens for a new company that isn't ML3 certified, jumps through all the hoops, and then isn't awarded the contract? (Yes, I know they have better cybersecurity, but the timing of investments may have been different but for their submission of the proposal). Then there is the question of wherever all costs are allowable or only some, and whether the entirety of the cost is allowable or only some percentage. **– James Goepel**



IMPLEMENTING THE CMMC MODEL

WHAT IS THE CMMC MODEL?

CYBERSECURITY STANDARDS & BEST PRACTICES

- “The CMMC Model combines various cybersecurity standards and best practices and maps the resulting controls and processes across several maturity levels that range from basic to advanced cyber hygiene.”

- The CMMC model encompasses the basic safeguarding requirements for protecting Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

- Requires 3rd Party Certification

- 100% Conformity is the expected

CMMC PRACTICES

- Assigned to a specific CMMC level and domain
- Most practices from FAR and NIST 800-171

CMMC Level	CMMC Level Practices	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B	Other CMMC practices
Level 1	17	15	17	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11
Total	171	15	110	15	46

May Be Major Changes

- **Policies and Procedures** – Probably not adequate
- **Acceptable Use and other policies** – Verified every year
- **Training** – Required, tracked
- **Multifactor authentication** - For local and network access to privileged accounts and for network access to non-privileged accounts. That is pretty much all access.
- **Accounts assigned to non-employees -** must be set with an expiration date that is required to be reset based on continued need.
- **Split tunneling not allowed -** This includes local printer access.
- **Audit Logging** – Central repository, restricted access, reviewed

May Be Major Changes

- **Vulnerability Management –** This has to be looked at.
- **Configuration Management –** “we use default settings”
- **Change and Vendor Management -** ALL software must be evaluated for security and compliance. Depending on the system there may be DFARS requirements etc.
- **Software Whitelisting/Blacklisting** – Including Browsers and Addons
- **Incident Response –** Documented and Tested
- **Physical Security** – Controlled, Logged, Monitored
- **Enclave** – ID CUI, In summary, all four areas—physical, network, session, and infrastructure—must be examined and brought under control.
- **Risk Assessment** (The CMMC assessment is not this)
- **Data Classification**

Enclave or not to Enclave?

Enclave

1. (I) A set of system resources that operate in the same security domain and that share the protection of a single, common, continuous security perimeter. (Compare: domain.)
2. (D) /U.S. Government/ "Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.“

Physical controls: locks, card key access, backups, Cameras, Visitors

Network controls: Protected at the network layer, including OSI layers two through four.

Session controls: Authentication and authorization mechanisms.

Infrastructure controls: Virtual machines, physical servers, storage area networks, and backup systems.

Buyer Beware

Software

- Some software is better than others
- Software alone will not protect your systems
- Software will not guarantee you pass CMMC assessment
- Who is responsible for this software, what are the currently responsible for?
- Software can automate controls, but appropriate and knowledgeable people must perform controls
- More expensive software can be more expensive to operate and manage
- COTS rule applies, but Cloud Requirements Remain

Services

- If money is no object, I have the solution for you, but you can't make this go away.
- Often, lower cost service will meet the requirements
- Security is important, but not just another job for IT. There is actually a conflict of interest.
- Managed Service Providers are not all the same
- You must have your own controls, even if it is to verify SLAs
- The way this works is your MSP will need to be CMMC – Receptacle solutions must happen eventually

AGENDA

- DEFENSE SUPPLY CHAIN
- CERTIFICATION REQUIREMENTS
- CMMC ECOSYSTEM
- IMPLEMENTING THE CMMC MODEL

TIM FAWCETT, CISSP, CISA
DIRECTOR OF CYBER SECURITY CONSULTING
CMMC LEVEL 1-3 PROVISIONAL ASSESSOR

GUERNSEY
5555 N. GRAND BLVD.
OKLAHOMA CITY, OK 73112
T: 405.416.8182
M: 918.808.0558
TIMOTHY.FAWCETT@GUERNSEY.US

WWW.LINKEDIN.COM/IN/TIMOTHY-FAWCETT
GUERNSEY.US/CYBERSECURITY
GUERNSEY.US/CMMC

guernsey
ENGINEERS
ARCHITECTS
CONSULTANTS

CMMC–AB
PROVISIONAL
ASSESSOR

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
C3PAO

CYBERSECURITY MATURITY MODEL CERTIFICATION
CMMC-AB
RPO
REGISTERED