ALLIANCE
NORTHWEST

ALLIANCE NORTHWEST

BREAKOUT SESSION

DoD Cybersecurity Maturity Model Certification (CMMC) Current Status

WASHINGTON APEX ACCELERATOR

DoD Cybersecurity Maturity Model Certification (CMMC) Current Status

March 20, 2025

This APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense.

Agenda

- Background
- Current status
- The Big Changes
- CMMC Certifications
- Impact on the Contractor
- What will it Cost ??
- CMMC Certification Level Requirements
- FAR 15 Information Safeguards
- What is CUI ??
- The Five Clauses
- Organizations to Help
- Summary
- Q & A

WASHINGTON APEX ACCELERATOR

Abbreviations & Acronyms

CA, Certified Assessor

CMMC, Cybersecurity Maturity Model Certification

Cyber-AB, Cybersecurity Maturity Model Certification Accreditation Body

CUI, Controlled Unclassified Information

C3PAO, Certified Third-Party Assessor Organization

NIST, National Institute of Standards and Technology

OSC, Organization Seeking Certification

RP, Registered Practitioner

RPO, Registered Practitioner Organization

RPA, Registered Practitioner Advanced

SPRS, Supplier Performance Risk System

CMMC

- CMMC is for unclassified procurements
  - Controlled Unclassified Information (CUI)

- CMMC is not for classified procurements
  - Such a “secret” or “top secret” contracts.

- CMMC is not the DoD Interim Rule

The Hierarchy

DoD – Department of Defense

↓

Cyber-AB – Cybersecurity Maturity Model Certification – Accreditation Board (Body)
(a non-profit, independent organization)

↓

C3PAO - Certified Third-party Assessor Organization
(Commercial company)(Issues the 3-year certificate)

↓ ↑

CA - Certified Assessor
(sub-contractor to or employee of C3PAO)

↓

OSC - Organization Seeking Certification (you, the company)

WASHINGTON APEX ACCELERATOR

CMMC Current Status

- CMMC became law on December 16, 2024
- CMMC Must be codified by changing Title 48 CFR CMMC acquisition rule
- CMMC will be phased-in over a 3-year period
  - March 2025, some Level-1 solicitations
  - March 2026, some Level-2 solicitations
  - March 2027, some Level-3 solicitations
  - March 2028, all solicitations

CMMC Implementation

The DoD Numbers

- DoD has more than 300,000 contractors (Prime + Subcontractors)
- 60-70% will need CMMC Level-1 certified
- So, 90,000 will need CMMC Level-2 certification
- There will be about a half dozen contractors at CMMC Level-3 certification

WASHINGTON APEX ACCELERATOR

CMMC Big Changes in the Final Rule

- Level 1 is self-certification using FAR Clause 52.204-21
  15 safeguards vice NIST SP 800-171A rev. 2, 110 controls
- All certifications require annual affirmation & recorded in SPRS
- Three phase-in period starting March 2025

CMMC (for all DoD contracts)

- 3 levels of cybersecurity maturity from basic to advanced
  - Level-1, 15 safeguards from FAR clause 52-204-21
  - Level-2, 110 controls from NIST SP 800-171A Revision 2
  - Level-3, 134 controls from NIST SP 800-171A Revision 2 & NIST SP 800-172

- All Practices & Controls must be implemented
- All DoD contractors will need a certification (some exceptions)
- Self-assessment for Level 1 and some Level 2 (during the phase-in period)

WASHINGTON APEX ACCELERATOR

CMMC Certification

- CMMC Certification required to be awarded a contract or subcontract
- Level-2, All practices & requirements are laid out for contractors to start implementing in NIST SP 800-171A rev. 2
- The Cyber-AB is currently training Registered Practitioners and C3PAOs
- Audits (certifications) are available now
- As of March 8, 2025, there are: 1,631 RP
  201 RPA
  340 RPO
  64 C3PAO

WASHINGTON APEX ACCELERATOR

Impact on the Contractor

- Level 1 & some Level 2, Requires self-assessment and certification prior to award
  And annual affirmation

- Levels 2 & 3, Requires 3rd party audit and certification prior to award
  And annual affirmation

- CAs will most likely charge by the hour plus travel costs - ask for an estimate

- Certification costs are allowable, as an **overhead expense**

WASHINGTON APEX ACCELERATOR

Impact on the Contractor
(continued)

- Subcontractors will have the same CMMC level as the prime contractor or lower based on the Statement of Works (SoW)
- Prime contractors are responsible for all subcontractor tiers
- Increased non-compliance penalties and risks including: the loss of current and future contracts, personal & corporate liability, & negative company brand
- Does not apply to Commercial Off The Shelf **(COTS)** or **Micro-purchases (<=$10K)**

WASHINGTON APEX ACCELERATOR

What Will it Cost?

Table 10 - Small Entities (per Assessment)

Assessment Phase ($)	Level 1 self-assessment[40]	Level 2 self-assessment[40]	Level 2 certification assessment	Level 3 certification assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	**$5,977**	**$37,196**	**$104,670**	**$12,802**

*Reflects the 3-year cost to match the periodicity.

**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	Conducted by Organization Seeking Assessment (OSA) annually Results entered into the Supplier Performance Risk System (SPRS)	Not permitted	After each assessment Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	After each assessment and annually thereafter Assessment will lapse upon failure to annually affirm Entered into SPRS
Level 2 (C3PAO)	110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

CMMC Model

	Model	Assessment
LEVEL 3	**134** requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

CMMC Level 1 Federal Contract Information Safeguards
FAR 52.204-21

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

CMMC Level 1 Federal Contract Information Safeguards

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

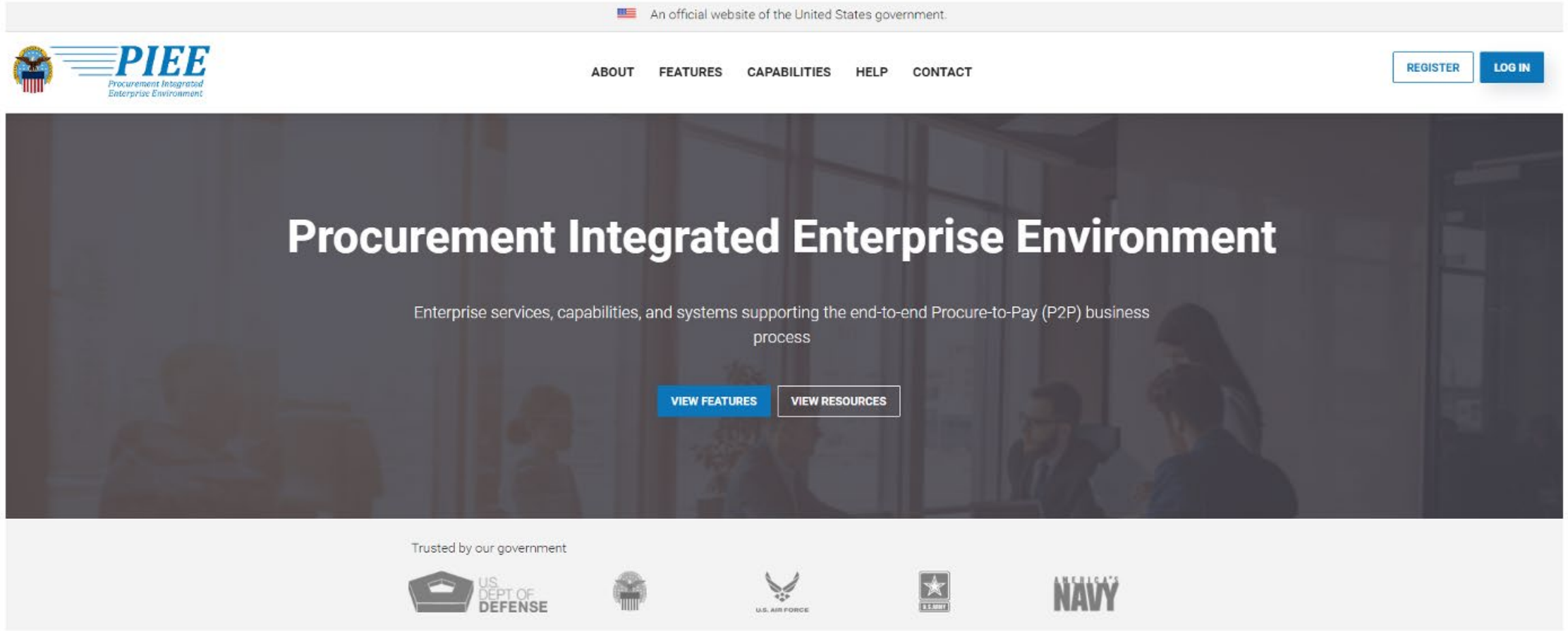
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Procurement Integrated Enterprise Environment

https://piee.eb.mil



Supplier Performance Risk System (SPRS)

https://www.sprs.csd.disa.mil/

How do you know what is CUI ?

DoDI 5200.48, Controlled Unclassified Information (CUI)

- CUI will be identified in the Security Classification Guide to ensure such information receives appropriate protection

- The program office or requiring activity must identify DoD CUI in the solicitation and resulting contract and which CMMC level certification is required

CUI Link: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF?ver=2020-03-06-100640-800

WASHINGTON APEX ACCELERATOR

Controlled Unclassified Information (CUI)

Examples of Controlled Technical Information (CTI)

- Federal Contract Information
- Research & Engineering Data
- Engineering Drawings
- Specifications
- Standards
- Process Sheets
- Manuals
- Technical Reports
- Technical Orders
- Catalog-item Identifications
- Data Sets
- Studies & Analyses
- Computer Software Executable Code
- Source Code

WASHINGTON APEX ACCELERATOR

Examples of NAICS Codes with CUI

NAICS	Title
236220	Building Construction
541330	Engineering
541519	Computer Services
561210	Facility Support Services

WASHINGTON APEX ACCELERATOR

Look for these Five Clauses

FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (NOV 2021)

DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (JAN 2023)

DFARS clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (NOV 2023)

DFARS clause 252.204-7020, NIST 800-171 DoD Assessment Requirements (NOV 2023)

DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements (JAN 2023)

WASHINGTON APEX ACCELERATOR

Organizations to Help Contractors

Project Spectrum - https://www.projectspectrum.io/#/

(they provide no-cost training)

Impact Washington - https://www.impactwashington.org/cybersecurity-consulting.aspx

(for manufacturing companies)

WASHINGTON APEX ACCELERATOR

Summary

- Get started now, if you want to be a DoD contractor or subcontractor
- Expect to wait: C3PAOs are in short supply, so plan for several months delay before an audit can start
- There are qualified auditors now (64 C3PAOs)
- You may request an audit anytime now
- Must be certified at time of contract award
- Add CMMC certification level to the Capability Statement

TASK: Read all future solicitations to see if there are cybersecurity requirements.

WASHINGTON APEX ACCELERATOR

QUESTIONS
For Terry

WASHINGTON APEX ACCELERATOR

WA APEX Accelerator Advisor

Mr. Terry Homburg
homburg@kitsapeda.org

www.napex.us

ALLIANCE
NORTHWEST