Get Ready for CMMC

(Cybersecurity Maturity Model Certification)

September 22, 2022

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

Agenda

- Background
- DoD CMMC Initiative
- CMMC 2.0 (November 2021)
- Impact on you
- Requirements of CMMC
- Assessment Process (Getting Certified)
- DoD Cybersecurity Interim Rule
- Q & A
- Summary

Abbreviations & Acronyms

CA, Certified Assessor

CDI, Covered Defense Information, DFARS clause 252.204-7012

CMMC, Cybersecurity Maturity Model Certification

Cyber-AB, Cybersecurity Maturity Model Certification Accreditation Body

CUI, Controlled Unclassified Information

C3PAO, Certified Third-Party Assessor Organization

DCMA, Defense Contract Management Agency

DFARS, Defense Federal Acquisition Regulations Supplement

DoD, Department of Defense

EAR, Export Administration Regulations

FAR, Federal Acquisition Regulations

FCI, Federal Contract Information, FAR clause 52.204-21

ITAR, International Traffic in Arms Regulations

NIST, National Institute of Standards and Technology

OSC, Organization Seeking Certification

SPRS, Supplier Performance Risk System

BACKGROUND

- $600B in DoD trade secrets lost each year from 300K entities.
- 80% from entities & 1.1M from foreign students (34% from China).
- Adversaries getting more sophisticated.
- Compromises our troops & war fighting capabilities
- Contractors ignoring the DFARS clause, 252.204-7012
- Until 2018, companies were required to qualify after contract award,
  now you have to qualify before award.
- It only takes $2K to purchase the software to crack passwords.
- DoD wants to avoid risk from cyber attacks.
- Universities are centers for innovations and get hacked.
- 205 days to ID compromise, 69% notified by FBI, & 89% were not cyber compliant.

Examples

- March 2020, Lockheed Martin, GD, Boeing, Tesla, & SpaceX are among dozens of companies named as victims of compromised data accessed through a subcontractor in Colorado.
- June 2020, Chinese military officer was caught leaving the U.S. w/research materials from U.C. San Francisco, after lying on an application to obtain a visitor visa for a work-study exchange program.
- December 2020, Russia hacked into DHS, Departments of Treasury & Commerce, and Fortune 500 companies, as result of these entities using Solarwinds software loaded in March and April of 2020. 18K entities in the U.S. use Solarwinds software. The hack was discovered by Fireye, a private cybersecurity company.

Examples (continued)

The U.S. F35 jet fighter vs. the Chinese J31

- F35 first produced in 2006 for $78M each
- Chinese had no R&D, thus saved time & money
- Chinese produce each of their planes for $31M less

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

DoD Response

- **Restrict & Control -** the export of defense & military related technologies & information.
- **Secure -** 300,000+ DoD & non-DoD supplier information systems & networks.
- **Codify -** cybersecurity practices, processes, and assessment standards.
- **Enforce** – Supply chain accountability to protect the DoD intellectual property on non-DoD supplier networks.
- Introduce Cybersecurity Maturity Model Certification (CMMC) in 2020.

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

DoD CMMC 1.0 Initiative

- Started Jan 30, 2020
- CMMC-AB established June 2020
- Five-year rollout *
- levels to control information: *
  - Levels 1 through 5
  - Levels 1 through 3 will be the most common
  - Level 1 is everyday security hygiene
- 3rd party certification required before contract award *
- Certification process has started. Auditors are available.

CMMC 1.0/2.0 Current Status

- CMMC Certification required to be awarded a contract.
- No solicitations will be issued w/CMMC requirement during the 5-year roll-out unless approved by OUSD (A&S). *
- CMMC requirements in solicitations begin 1 Oct 2025. *
- There are still many unknowns with how certifications & assessments will happen.
- All practices & requirements are laid out for contractors to start implementing in NIST SP 800-171A.
- The Cyber-AB is currently training C3PAOs. As of September 19, 2022, there are 23 C3PAOs available.
- Audits (certifications) are available now.

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

CMMC 2.0 Proposed Changes

- Proposed changes November 2021.
- The changes need to go through the public comment period and rulemaking process, which takes 9-24 months.
- Once the changes are codified, the CMMC requirements will be in solicitations and resulting contracts.
- The DoD will publish comprehensive cost analysis for each level of CMMC 2.0.
- CMMC levels would change from 5 to 3 levels.
- CMMC level 1 would be a self-assessment.

Cybersecurity Compliance Drivers

- Federal Contract Information (FCI): FAR clause 52.204-21 (JUN 2016)
  - Equals CMMC Level 1

https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#id1669B0A0E67

- Covered Defense Information (CDI): DFARS clause 252.204-7012 (DEC 2019)
  - Adequate security (currently NIST SP 800-171 Rev 2)
  - Cyber incident response & reporting

https://www.acquisition.gov/dfars/part-252-clauses#DFARS-252.204-7012

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

FAR Requires 17 Safeguards

- FAR clause 52.204-21, Basic Safeguards on Covered Contractor Information Systems (JUN 2016)

  - 15 subparagraphs comprising 17 basic requirements of ALL Government contractors to protect federal contract information (FCI) and non-public data generated by or for a contract

- These 17 safeguards are all included in NIST SP 800-171 Rev 2.

- Constitute all the CMMC Level 1 practices.

NIST SP 800-171 Rev 2

- Published FEB 2020.
- **NIST** refers to National Institute of Standards and Technology **Special Publication 800-171**, which governs Controlled Unclassified Information (CUI) in Non-Federal Information Systems and Organizations. Doing so helps the federal government successfully carry out its designated missions and business operations. If you or another company you work with **has** a contract with a federal agency, you must be compliant with this policy.
- This is CMMC Level 1 requirements.

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

CMMC vs. NIST SP 800-171

- NIST 800-171 (contracts with CUI)
  - Current requirement
  - DoD contractors that process/store CUI
  - 110 controls & 320 assessment objectives
  - Can have a Plan of Action and Milestones (POA&M)
  - Perform self-assessment and submit score to DoD
  - DCMA/DCSA conducting audits with DoD assessment methodology

- CMMC (for all contracts)
  - 5 levels of cybersecurity maturity from basic to advanced
  - 17 practices (AKA controls) – 173 practices (Level 3 has 130 practices)
  - Practices must be implemented
  - All DoD contractors will need a certification
  - No self-assessment *

IMPACT ON YOU

- You have to pay to play with DoD.

  DoD estimate for assessment & recertification is:

  - Level 1 – about $1,000
  - Level 3 – about $51,000

- Requires 3rd party audit and certification prior to award. *
- CAs will most likely charge by the hour plus travel costs. Ask for an estimate.
- Certification costs are allowable, as an overhead expense.
- Subcontractors will have the same CMMC level as the prime contractor or lower based on the 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 COTS or Micro-purchases ($10K)

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

REQUIREMENTS OF CMMC

Created from 10+ information protection & industry cybersecurity standards:

- Model addresses everything from asset controls to systems & information integrity
    - 17 domains; 43 capabilities
    - 5 processes across 5 levels to measure process maturity
    - 171 practices across 5 levels to measure technical capabilities
- Includes 5 maturity levels (basic cyber hygiene to highly advanced practices)
    - Level 1, everyday basic cyber security (you should already be at this level). (110 Controls for FCI)
    - Level 2, Intermediate cyber security. IT companies will need at least this.
    - Level 3, Good cyber security. When there is CUI (for technical information). (130 Controls for CUI)
    - Levels 4 & 5, Proactive & Advanced cyber security. DoD has not yet determined who will need this.
- Each maturity level includes all prior level domains, capabilities, practices, & processes
- Adherence to "ALL" level practices & processes & all prior levels required to achieve certification.
- DoD plans on adding additional practices & processes to the standard; the overall number growing to 479 by 2025.

REQUIREMENTS OF CMMC

	CMMC Level	Practices	Processes	Contractor example
FAR + DFARS + NIST 800-171	1	17	none	grounds maintenance, janitorial
FAR + DFARS + NIST 800-171	2	55	2	IT services
FAR + DFARS + NIST 800-171	3	58	1	CUI
	4	26	1	higher data sensitivity
	5	15	1	higher data sensitivity

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

CMMC Maturity Levels

Maturity Level	Assessment Objective: Does the organization …	Nutshell
1. Performed	perform the practice? (17 safeguards)	Do it
2. Documented	perform the practice AND have a written process and policy?	Do it & document it
3. Managed	perform the practice AND have a written process and policy AND establish, maintain, and resource a plan demonstrating the management ..of activities for practice implementation, to include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders?	Do it, document it, demonstrate resources for it
4. Reviewed	perform the practice AND have a written process and policy AND establish, maintain, and resource a plan demonstrating the management of activities for practice implementation, AND review and measure practices for effectiveness, to include the ability to take corrective action when necessary?	Do it, document it, demonstrate resources for it, measure its effectiveness and fix it
5. Optimized	perform the practice AND have a written process and policy AND establish, maintain, and resource a plan demonstrating the management of activities for practice implementation, AND review and measure practices for effectiveness, to include the ability to take corrective action when necessary AND standardize and optimize process implementation across the organization?	Do it, document it, demonstrate resources for it, measure its effectiveness and fix it, automate it & have feedback loops for it across the enterprise

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

CMMC by the Numbers

	Level 1 Basic	Level 2 Intermediate (gray area)	Level 3 Good	Level 4 Proactive (gray area)	Level 5 Advanced/Progressive (gray area)
Who?	All contractors	Some CUI processors	All CUI processors	APT-targeted organizations	APT-targeted organizations
What?	17 Practices	72 Practices	130 Practices (includes some 800-171)	156 Practices (all of 800-171 +20 additional)	171 Practices (includes enhanced assessment objectives from 800-171B)

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.

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

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

NAICS Codes that are CUI

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

WASHINGTON PTAC

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)

CMMC JOURNEY

1. Leadership, Preparation, & Alignment – Learn & understand the CMMC Model, applicable requirements, & impacts to you organization.

2. Determine CMMC Level & Boundary – Identify your current regulated data (FCI, CUI, ITAR) level & organizational aspirations for future DoD contracts.

3. Identify Compliance Gaps – Identify CMMC level compliance gaps across your business & operations including cloud, on-premise, home office, etc.

4. Remediate Gaps – Develop & implement "good enough, better, & best" solution to mitigate gaps & achieve organizational strategies.

5. Audit Preparation – Prepare team & organize CMMC documentation, evidence, & secure artifacts for easy auditor consumption.

6. Audit Execution – Engage C3PAO & address audit issues real time to achieve certification. Certification is good for 3 years. (C3PAOs provided at www.cyberab.org Marketplace)

7. Post Audit Performance – Perform ongoing compliance program practice & process adherence & resiliency activities.

CMMC BENEFITS

- Reduce cyber risk. Prevent unauthorized disclosures to protect FCI, CUI, ITAR, & EAR info from disclosed to unauthorized entities and individuals.
- Require compliance program. Provides a framework that enforces a systematic compliance program, good enough for the DoD, that demonstrates reasonable due care & diligence.
- Compete with large business. Improves competitive position to compete with larger competitors by demonstrating the highest level of information protection & cyber security.
- Build trust relationship with DoD. By demonstrating cybersecurity & organizational effectiveness, trust is created, non-compliance penalties are avoided, & agencies see you as a low risk contractor, leading to more business.

The Clause, FAR 52.204-21 (JUN 2016)
Exception is COTS (FAR Part 12)

CMMC Level 1 Requirements:

Requirement	AKA
Identify, report, & correct info & info system flaws in a timely manner.	Patch your IT stuff
Provide protection from malicious code at appropriate locations within organizational information systems.	Install antivirus software (such as Defender, Norton, McAfee)
Update code protection mechanisms when new releases are available.	Update your antivirus software
Perform periodic scans of the information system & real-time scans of files from external sources as files are downloaded, opened, or executed.	Use the antivirus software
Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.	Shred paper, wipe hard drives
Limit physical Access to organizational information systems, equipment, & the respective operating environments to authorized individuals.	Lock doors & windows
Escort visitors & monitor visitor activity; Maintain audit logs of physical access; Control & manage physical access devices	Monitor ALL entry & keep an inventory of keys, codes, & tokens

The Clause, FAR 52.204-21 (continued)

CMMC Level 1 Requirements:

Requirement	AKA
Control information posted or processed on publicly accessible information systems.	Don't post Fed info on Facebook (social media)
Identify & authenticate information system users, processes acting on behalf of users or devices.	Require individual user names & passwords
Limit information system access to authorized users, process acting on behalf of authorized users or devices (including other information systems).	Control access to system - requires you to know who/what has access!
Limit information system access to the types of transactions & functions that authorized users are permitted to execute.	"Least privilege"
Verify & control/limit connections to & use of external information systems.	Catalog all connections, use tools like firewalls
Monitor, control, & protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries & key internal boundaries of the information systems.	Use tools like firewalls & IDS, & segment internal network
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	Implement a "DMZ"

The Clause, FAR 52.204-21 (continued)

CMMC Level 3 Requirements:

Requirement	AKA
Define procedures for the handling of CUI data.	Do all the stuff in NIST 800-171
Implement a policy restricting the publication of CUI on externally-owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).	Engage social media policy
Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.	Execute software peer review, static code analysis
Use encrypted sessions for the management of network devices.	Disable telnet on routers/switches
Collect audit information (e.g., logs) into one or more central repositories.	Implement a Security Info & Event Mgmt (SIEM) tool
Review audit logs.	Use the SIEM

The Clause, FAR 52.204-21 (continued)

CMMC Level 3 Requirements:

Requirement	AKA
Detect & report events.	Do all the stuff already required by the 800-171 Incident Response controls
Analyze & triage events to support event resolution & incident declaration.	same as above
Develop & implement responses to declared incidents according to predefined procedures.	same as above
Perform root cause analysis in incidents to determine underlying causes.	same as above
Regularly perform & data backups	Backup CUI daily (offsite) & test that data can be completely restored to your systems in a timely manner
Regfularly perform complete, comprehensive, and resilient data backups, as organizationally defined.	same as above

The Clause, FAR 52.204-21 (continued)

CMMC Level 3 Requirements:

Requirement	AKA
Periodically perform risk assessments to identify & prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	Do the stuff already required by the 800-171 Risk Assessment family
Develop & implement risk mitigation plans.	Execute POA&M
Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.	Legacy software running on Windows 7? Isolate from network
Receive & respond to cyber threat intelligence from information sharing forums & sources and communicate to stakeholders.	Monitor US-CERT alerts (e.g.) and distill/disseminate

The Clause, FAR 52.204-21 (continued)

CMMC Level 3 Requirements:

Requirement	AKA
Implement Domain Name System (DNS) filtering serices.	Use UTM firewall to blacklist known malicious or newly created websites/domains
Employ spam protection mechanisms at information system access entry & exit points.	Purchase spam protection (O365, AppRiver, etc.)
Implement e-mail forgery protections.	Explicitly configure servers that can send e-mail for your org.
Utilize sandboxing to detect or block potentially malicious e-mail.	Procure e-mail link & attachment inspection service (opens link/attachment in isolated network)

CMMC Assessment Process

1. The Organization Seeking Certification (OSC) will submit a Request for Assessment (RFA) to enter into a contract with a C3PAO to obtain a CMMC assessment.

   To find a C3PAO, go to www.cyberab.org, select “marketplace, under “Ecosystem Role” select ”C3PAO”. You will find all the certified & qualified C3PAOs there.

2. One or more CAs will be assigned by the C3PAO to conduct the CMMC assessment. The C3PAO and the CA may be the same company or person.
3. The CA will conduct the CMMC assessment on behalf of the C3PAO.
4. The C3PAO will report the results to the Cyber-AB who reviews it for accuracy & completeness.
5. The C3PAO issues the certificate, which is good for 3 years, unless there is a violation.
6. The Cyber-AB will handle adjudication actions where the OSC disagrees with the findings of the CA/C3PAO. Do not expect:
   - Adjudications to be a timely process.
   - Interim “pass” findings will be issued while adjudications are ongoing.

DoD Proposed Changes

1. Initiated November 2021
2. Will take 9 to 24 months to implement.
3. In the “public comment” stage currently with 2 stages after that.
    - “Rule Making” is the final step
4. Other federal agencies disagree with proposed DoD changes.

DoD Proposed Changes (continued)

5. Some proposed changes:
   - 5 levels to 3 levels
     - Level 1, 17 requirement (FCI) fundamental
     - Level 2, 110 Controls (320 objectives) (old level 3) advanced
     - Level 3, NIST 800-171 + NIST 800-172 (old Levels 4 & 5) expert
   - Level 1 is self-assessment
   - Level 2 is audited by a C3PAO
   - Will go into effect when approved, vice 5 years
   - DoD to provide cost estimate for each level
6. and others

WASHINGTON PTAC

Organizations to Help Contractors

- Project Spectrum, https://www.projectspectrum.io/#/
- Totem Technologies, https://www.totem.tech/
- Ignyte Institute, https://www.ignyteinstitute.org/
- Impact Washington, https://www.impactwashington.org/cybersecurity-consulting.aspx

WASHINGTON PTAC

Pause

- That’s it for CMMC.
- Now let’s talk about the DoD Interim Rule.

DoD Cybersecurity Interim Rule

- **Effective December 1, 2020**.
- Applies only to requirements with CUI. Does not apply to COTS or micro-purchases.
- Clauses are: DFARS 204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (NOV 2020)
  DFARS 204-7020, NIST 800-171 DoD Assessment Requirements (NOV 2020)
- Prime & subcontractors must have a cyber security assessment performed and recorded prior to contract award.
- Assessments may be "Basic, Medium, or High".
  - Basic is performed by your company, using NIST SP 800-171A 110 controls.
  - Medium or High will be performed by DCMA and recorded by DCMA. (Very few companies will be Medium or High)
- Post assessment on-line at SPRS, through an account in PIEE. https://piee.eb.mil/xhtml/unauth/home/login.xhtml
- Scores may range from -220 to 110 because each practice is weighted for importance.
- Assessment in SPRS is good for 3 years.
- Solicitation may identify a minimum score requirement.
- G may find your proposal non-responsive & assessment is subject to the False Claims Act.

SPRS Questions
(Supplier Performance Risk Assessment)

1. Assessment date:
2. Score:
3. Assessing Scope: (select “enterprise”, if assessing your entire company)
4. POA&M completion date: (date you plan to achieve all 110 controls)
5. Systems Security Plan (SSP) assessed: (plan title)
6. SSP version/revision (plan title, version, and date)
7. SSP date: (date of your plan)
8. Included CAGE codes:
9. Include HLO: (if applicable)

Five Clause to look for

FAR clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)

DFARS clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (NOV 2020)

DFARS clause 252.204-7020, NIST 800-171 DoD Assessment Requirements (NOV 2020)

DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification Requirements (NOV 2020)

QUESTIONS ??

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

Summary

- Get started now, if you want to be a DoD contractor or subcontractor.
- Conduct self-assessment yourself, using NIST Handbook 162, OR hire a company to assist you. RPOs and RPs available now to hire. To find an RPO or RP, go to www.cyberab.org, select “marketplace, under “Ecosystem Role” select ”RPO or RP”. As of September 19, 2022, there are 2,221 available.
- Expect to wait: C3PAOs will be in short supply, so plan several months delay before an audit can start.
- There are qualified auditors (C3PAOs) now. You may request an audit anytime now.

Summary (continued)

- Must be certified at time of contract award.
- Get secured and stay secured. DoD wants and needs contractors.
- GSA has already started including CMMC requirements in some solicitations.
- Applies to prime contractors and subcontractors.
- Add your CMMC certification level to your Capability Statement.

TASK: Read the solicitation to see what cybersecurity requirement there is.

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC

See your local PTAC for assistance

For the WA Olympic Peninsula it is:
James Davis at 360-377-9499
Kitsap@washingtonptac.org

To find your local Washington PTAC office go to:
https://washingtonptac.org

To find a PTAC office in other states go to:
https://www.aptac-us.org

KITSAP ECONOMIC DEVELOPMENT ALLIANCE

WASHINGTON PTAC