THE CYBER AB
CMMC CERTIFICATION

15TH ANNUAL PEAK CYBER SYMPOSIUM

CMMC – NO LONGER A MYTH
ARE YOU READY FOR AN ASSESSMENT?

Oct 14, 2025

INTRODUCTION

Mike Crandall, CEO, Digital Beachhead

MIKE CRANDALL

CEO
Digital Beachhead

- CEO, Digital Beachhead
- Founder/President, Afghan Promise (non-profit)
- Adjunct Professor
- MBA / CISSP / NSA-IAM

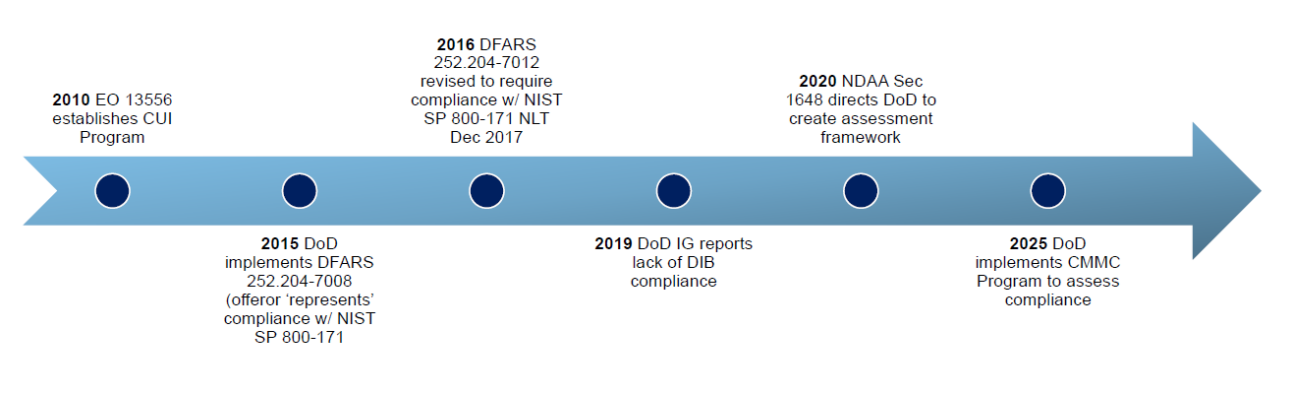
- 21-year Air Force Veteran (retired); 12 years corporate experience
- Founding contributor to Air Force's "Barrier Reef" Defense in Depth Concept; Implemented as Combat Information Transfer System/Base Information Protection (CITS/BIP) Air Force wide
- Designed/Developed/Implemented Air Force' s first operational Network Operations and Security Center (NOSC)
- Air Force lead securing $50B Satellite Control Network including GPS, Weather, Missile Defense systems
- Digital Beachhead currently supports Government Agencies and small to mid-size organizations providing Virtual/Fractional Chief Information Security Officer (vCISO) and other cyber risk management services

CMMC 2.0 IS HERE

On October 15, 2024, the Cybersecurity Maturity Model Certification (CMMC) Rule (titled 32 CFR) was published in the Federal Register as a final rule, officially establishing the CMMC program as the Department of Defense (DoD) program for protecting Controlled Unclassified Information (CUI) and sensitive contract information across the Defense Industrial Base.

The final rule went into effect on December 15, 2024

Title 48 CFR Rule Integrates CMMC Into DoD Solicitations, RFPs & Contracts



WHAT DOES THAT MEAN

ASSESSMENTS

- The CMMC Program is established with roles and responsibilities set
- Authorized C3PAOs can begin formal CMMC audits of Defense Contractors towards Level 2 Compliance
- Self Assessments in beginning of program; determined by program office

TITLE 48

- Published in Sept and now all RFPs/Solicitations will require CMMC starting Nov 10th 25
- FCI = CMMC Level 1 and self assessment
- CUI = CMMC Level 2 with mix of self assessment and third part assessment

WILL MY ORGANIZATION NEED CMMC LEVEL 2?

Memorandum dated 17 January 20205 the Office of the Secretary of Defense outlined:

CMMC Level 2 is required when CUI will be processed, stored, or transmitted on contractor-owned information systems in the performance of a DoD contract and flows down to subcontracts, or similar contractual instruments.

CMMC Level 2 Self Assessment is the minimum assessment requirement for CUI. It is sufficient only for CUI **outside** of the National Archive' s CUI Registry Defense Organizational Index Grouping.

CMMC Level 2 Certification is the minimum assessment requirement when the planned contract will require the contractor (or subcontractors) to process, store, or transmit CUI categorized **under** the National Archives CUI Registry Defense Organizational Index Grouping.

WHAT IS NATIONAL ARCHIVES CUI REGISTRY DEFENSE ORGANIZATIONAL INDEX GROUPING.

- **Defense**
  - Controlled Technical Information ****
  - DoD Critical Infrastructure Security Information
  - Naval Nuclear Propulsion Information
  - Privileged Safety Information
  - Unclassified Controlled Nuclear Information - Defense

**** Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code

https://www.archives.gov/cui/registry/category-list

COMMON CHALLENGES AND GAPS

Based on experience of helping Defense Contractors prepare for CMMC/NIST for the past 5+ years

1. **ACCESS CONTROL:** Understanding who has access with what permission/privileges
2. **AWARENESS AND TRAINING:** Proper documentation of all the different types of training
3. **AUDIT AND ACCOUNTABILITY:** Centralized audit logging with identified logging criteria – No SIEM biggest gap found
4. **CONFIGURATION MANAGEMENT:** Lack of form Configuration Control Board (CCB) or similar process to document changes including software updates
5. **IDENTIFICATION AND AUTHENTICATION:** Administrators need to have separate "user" account for daily access functions
6. **INCIDENT RESPONSE:** Training documentation based on "tabletop" exercise focused on identified risk
7. **MAINTENANCE:** Remote maintenance access and documentation of maintenance actions
8. **MEDIA PROTECTION:** Removable Media control to include identification, restrictions and encryption
9. **PHYSICAL PROTECTION:** Documentation on authorized access; how do you track physical access to facilities
10. **PERSONNEL SECURITY:** Background check documentation
11. **RISK ASSESSMENT:** Having a documented risk assessment process with outcomes; risks need to be defined and rated
12. **SECURITY ASSESSMENT:** Vulnerability scan frequency with documented results; documented anti-malware scans
13. **SYSTEM AND COMMUNICATIONS PROTECTION:** Firewall and/or router ACLs; documented data flow control
14. **SYSTEM AND INFORMATION INTEGRITY:** Documented follow up to security assessment findings that meet defined response timelines based on risk assessment

PEAK CYBER

LESSONS LEARNED BASED ON OUR DIBCAC AUDIT

Documentation is critical but must match technical implementation

- While there are 110 practices (controls) you must meet the objectives to have “met” the main practice
- 110 practices with 321 objectives
- Evidence must be available for each of the 321 objectives
- The System Security Plan (SSP) is a CRITICAL element and should contain information on how each objective is met
- SSP should contain Executive Summary, System Information, Authorized Software, System Inventory, Key Roles and Responsibilities and Implementation Status of all practices AND objectives

- All documents must be approved/signed with version history; this includes diagrams (network and data flow)
- Policies, Procedures and SSP must all be aligned and state the same thing! Technical implementation must match!
- Configuration Management needs full and complete documentation; if it changes baseline document then full CM process must be followed
- Having documentation separated by practice helps the auditor follow your processes much easier
- Having an evidence library separated by practice is the key to a successful audit

DOCUMENTATION AND EVIDENCE

- We recommend a Policy and Procedure document per practice (14 Documents)
- Policy is simple as you simply state the practice “shall” be accomplished
- Procedure is the main data point that describes “HOW” you are implementing each objective
- Other Documents required:
  - Incident Response Plan
  - Maintenance Plan
  - Media Posting Plan for publicly available systems (website, social media)
  - Risk Assessment Report
  - Configuration Management Plan
  - Authorized User List
  - System Baseline Documentation
  - Network Diagram / Data Flow Diagram / System Boundary Diagram

DOCUMENTATION AND EVIDENCE

- Evidence showing “how” each objective has been met (screenshots, diagrams, procedure documents and/or plans)
- Naming convention used: Objective_Year-CMMC Level-Assigned Audit Number_Company Name_Filename_date (Example: AC.L1.3.1.1a_24-CMMCL2-1104_DigitalBeachhead_authorized_users_2024120424)
- Some evidence covers more than one objective; recommend duplicating file using naming convention above
- Evidence MUST match the policy and procedure documentation exactly!!
- Creating an “Evidence Book” or central repository of evidence based on practice/objective is key!!

BEST PRACTICES FOR INTERNAL/SELF ASSESSMENT

- Creation of an independent audit team
  - Hire 3rd party auditor (need not be a C3PAO) or;
  - Use internal team that is not directly connected to controls such as senior operations managers
  - Be as critical and objective as possible; question each objective until it is clearly “Met”

- Follow the CMMC Assessment Process (CAP) to simulate an official C3PAO audit

- Require Senior Leadership involvement as they are the signatories for attestation
  - Full understanding of what they are signing and why
  - Agreement / Buy-In on the findings

- Make sure all your documentation compliments each other/matches; if you say screensaver comes on at 15 minutes make sure all systems have that set to 15 minutes

CONTINUOUS MONITORING AND IMPROVEMENT

- Where possible use automation tools for continuous monitoring
  - SIEM – setting up alerts for key logged actions (privilege account use, logon failures, etc)
  - XDR – Monitoring endpoints for unwanted/unexpected activity
  - Real time or frequent vulnerability testing
  - Develop scripts for user accounts that have been inactive for 30 days; set them to disabled
- Must be able to demonstrate how practices and objectives are monitored for compliance
- Build process improvements into your Change Management Plan
- If you can track/monitor an objective at any frequency, then do it and document it!

CMMC ASSESSMENT PROCESS (CAP)

Doctrine providing the overarching procedures and guidance for CMMC Third-Party Assessment Organizations (C3PAOs)

COMPLETE PRE-ASSESSMENT PLANNING

- Evidence collection approach
- Identify resources and schedule

PLAN AND PREPARE THE ASSESSMENT

- Establish roles and responsibilities
- Organize and prepare documents and templates
- Validate scope to include external Cloud providers
- Review organizations self assessment and findings

Phase 1 – VERIFY READINESS TO CONDUCT THE ASSESSMENT

- Access and verify evidence
- Make assessment feasibility determination

Phase 2 - CONDUCT THE ASSESSMENT

- Collect and examine evidence
- Conduct interviews and observation tests
- Score organization practices
- Finalize and record recommended findings

Phase 3 - REPORT RECOMMENDED ASSESSMENT RESULTS

- Deliver final findings
- Submit package and assessment documentation
- Archive or dispose of assessment artifacts

Phase 4 - CLOSE OUT POA&MS AND ASSESSMENT

- Perform POA&M close out assessment
- Update and close out assessment

PEAK CYBER

THE DIGITAL BEACHHEAD PLAYBOOK

Keep the process easy

CMMC Eco-system is currently not expansive

- Limited C3PAO companies (under 70)
- Limited number of CCA's available (under 400)
- Schedules are filling fast to get accessed

CMMC Level 2 Assessment

- Is an expense to prepare for (non inexpensive)
- Assessment can take a month or more to complete
- Most will require an onsite assessment
- Documentation must = implementation

info@digitalbeachhead.com

Get on our assessment calendar

THE PATH TO CYBERSECURITY BEGINS WITH A CONVERSATION

MIKE CRANDALL
DIGITAL BEACHHEAD CEO

THANK YOU