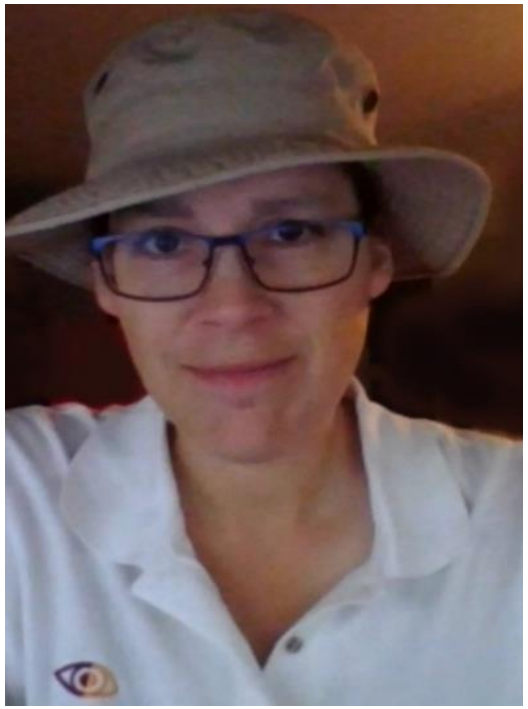
CMMC Update:
Notice of Proposed Rulemaking Review

Current As Of: September 2024

Sponsored by:

TODAY'S SPEAKERS



Amira Armond
Founder
Kieri Solutions

Cassia Baker
Research Faculty
Georgia Institute of Technology

Vince Scott
CEO
Defense Cybersecurity Group
INFRAGARD DIB Sector

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your Contracts**
  - Your contracts should tell you what information you must protect
  - Negotiate and understand information security and CUI requirements up front whenever possible
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Sponsored by:

Timeline Summary of Two Rulemakings

- **2 Rule Processes are running simultaneously**
  - CMMC 2.0 (32CFR): Notice of Proposed Rulemaking
    - Released 26DEC2023
      - CMMC Program Creation and specifics of how CMMC will run
      - Linked explicitly to NIST SP 800-171 Rev 2
      - Final Rule expected before the end of Sept (any day)
      - Includes Assessment and Scoping Guides
  - CMMC DFARS Case 2019-D041 (48CFR)
    - Released 15AUG2024
    - Largely Updates **DFARS 252.204-7021** putting CMMC into contracts
    - Comments Due 15OCT2024
      - NDIA Cybersecurity Division Drafting Comments
      - Send input to mseeds@ndia.org

Sponsored by:

48CFR Rule

- **Updates 252.204-7021**
  - Contractor shall only process, store, or transmit data on information systems that have a CMMC certificate at Level _____ or higher…
  - Notify the Contracting Officer within 72 hours if there is a *lapse of security* or change in compliance status…
  - Ensure that subcontractors have a current CMMC certificate appropriate to level flowed down

- **Does NOT update 252.204-7012**

- **Implications of the DoD UID, SPRS, CMMC eMASS**

Sponsored by:

CMMC 2.0 32CFR Rule Review

32CFR170 fundamental points

- **CMMC is rolling out**
- **Initial Self Assessments will begin concurrently with the rollout of the 48CFR rule going final around April 2025**
  - CMMC Self Assessments are different than the current 171 self assessments
  - They are based on CMMC not the DoD Assessment Method
  - The minimum score is 88/110
  - Security Protection Assets are now covered entities/devices
  - External Service Providers (MSPs & MSSPs) will need their own CMMC certification
  - Cloud based security tools will need to be FedRAMP or FedRAMP equivalent

Sponsored by:

Impact on External Service Providers

DoD includes MSPs / MSSPs as in scope

- **CMMC proposed rule defines "External Service Provider" (ESP) as:**
  - "[E]xternal people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and / or cybersecurity services on behalf of the organization."
- **"External Service Provider" category includes:**
  - Cloud Service Providers (CSPs)
  - "ESP[s] other than a CSP" (seemingly to include MSPs and MSSPs)
- **Proposed rule references new data type: Security Protection Data**
  - "In the CMMC Program, CUI or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP"
  - Key issue: "Security Protection Data" not defined outside examples of "log data" / "configuration data", but critical to defining an ESP

Sponsored by:

Impact on Cybersecurity Tools

- **CMMC Level 2 scoping guide (in 32CFR draft):**

  "Security Protection Assets provide security functions or capabilities within the OSA's CMMC Assessment Scope. Security Protection Assets are part of the CMMC Assessment Scope and are assessed against all CMMC requirements. "

- **DoD updates to Scoping Guide forcing stronger protections for security assets**
- **On-prem examples of SPAs**

Antivirus	SIEM	Switches (vLANs)
Patch deployment	Vulnerability scanner	Network inventory scanner
Directory	Firewalls	Group Policy / scripts
Door lock / badge systems	IT ticket system	Config Mgmt database

Sponsored by:

Impact on Cybersecurity Tools

- **Security Protection Data: a new category of information**
  - Not clearly defined. Meant to force certification for external providers.
  - Examples that have “configuration data” or “logs”

Cloud-provided RMM	External SIEM	Firewall mgmt. cloud
GRC websites	External vuln scanner	External ticket system
Cloud-provided directory	Security Operations Center	Cloud endpoint mgmt.
RPOs (diagrams, SSPs, inventories)	C3PAOs (assessment results and artifacts)	MSPs (diagrams, config mgmt., passwords)

- **Impact**
  - Security tools non-cloud must match CMMC Level of OSA
  - Security tools with cloud component must be FedRAMP authorized
    - Most modern commercial security tools have a cloud component

Before we talk POAMs,
Let's examine some confusing numbers

- **By The Numbers – *CMMC Level 2***
  - 110 Controls with 320 Assessment Objectives with a total value of 313 Points used to determine your Self-Assessment score posted in SPRS
    - A score of 0 indicates 65% implemented
    - A score of 88 indictates 93% implemented
- 6 months after CMMC Rule implementation, only Self-Assessment score allowed is a perfect 110/110 / 320/320 / 313/313

Sponsored by:

Impact on Plan of Action and Milestones (POAMs)

New rule narrowly restricts utilization

- 2/3 / 215 Objectives are “No Fail”
  - List in notes page of today’s backup slides
- POAMs must be cleared within 180 days
- Once POAMs cleared, a company must remain 110/110 / 320/320 / 313/313

Sponsored by:

Impact on Senior Company Official Affirmation

- Company “Senior Official” must affirm Self-assessment / Certification Assessment is accurate
  - Affirmation equivalent to a legal oath
- Company “Senior Official” also affirms 100% **future** compliance for all in-scope systems
  - Affirmation required in addition to self assessed score and in addition to certification where required

Sponsored by:

Impact on Joint Surveillance Voluntary Assessments

- **JSVAs must have perfect score to convert**
- **Any requirement can be POA&M'd and re-assessed by C3PAO within 180 days**
- **Companies using cloud-based services where CUI is stored/handled/transmitted**
  - Effective now: FedRAMP 3PAO audit of cloud required to verify all 800-53 Moderate Baseline controls performed
  - **Memo > Proposed Rule**
  - In-house / Migrate off non-compliant clouds!!!!

Impact on Self Assessment for Level 1 & 2

- **How to perform a Level 1 self-assessment**
  - 59 Assessment Objectives from Level 1 Assessment Guide **Yes/No**
  - **No POA&M allowed**

- **How to perform a Level 2 self-assessment**
  - 320 Assessment Objectives from Level 2 Assessment Guide
  - Do External Service Providers and Clouds meet requirements? **Yes/No**
  - Level 2 POA&M “allowed” only for first 6 months, even for self-assessment

Impact on Timeline for Certifications

- **Self-certifications (attesting to perfect compliance) required for almost all contract awards ~6 months after rule implementation**
  - August 2025 start seeing clauses?
  - New contracts will get DFARS 252.204-7021 clause
    - The contract should specify Level 1, Level 2 self-assessment, or Level 2 certification assessment
    - About 1/3rd of contracts renew each year
    - Variability introduced by contract officers (some may forget to add 7021 clause, some may require Level 3 arbitrarily)
  - Gradual switch from self-certification to third party certification for CUI contracts over 3 years.
  - 2027 = all renewing contracts include

Sponsored by:

Impact on Timeline for Certifications

- **CMMC Level 2 certification requirement for MSPs / MSSPs / RPOs**
  - If they have security protection data (passwords, network diagrams, SSPs, logs, vulnerability reports, patch reports, firewall configuration backups)
  - <10 MSPs/MSSPs/RPOs have passed a C3PAO assessment of their in-scope (SPD) environment so far. Critical resource.

- **No language about company-specific waivers in rule**
  - Certification either for all bidders, or for none
  - Flows down to all subcontractors that handle CUI
  - Subcontract to more than one prime? Plan for early certification

Sponsored by:

Questions

Sponsored by: