Review of the CMMC Proposed Rule

Kieri Solutions

December 27, 2023

www.kieri.com

Link to the recording (where we present these slides)

- https://www.youtube.com/watch?v=xHtHuYyynIQ

Speakers

Brian Hubbard
(CCA, PI)

Jil Wright
(CCA, PI)

Vince Scott
(CCA, PI)

Amira Armond
(CCA, PI)

Kieri Solutions, an Authorized C3PAO

www.kieri.com

- Assessment and preparation assistance
  - Expertise: 9 Certified CMMC Assessors and Instructors, plus CCPs
  - Serving Fortune 100s to small businesses
- Kieri Reference Architecture
  - Do-it-yourself (or with build help) *functional* Level 2 enclave.
  - Microsoft 365 / Windows Laptops / BYOD Phones
- Kieri Compliance Documentation
  - Do-it-yourself docs and instructions to run a compliant IT Department
  - Uses behavior stacking, just-in-time procedures, convenient record-keeping
  - Training library and monthly Q&As

AUTHORIZED C3PAO

Kieri Solutions cannot certify companies that we've consulted for (including KRA / KCD)

Disclaimer

Everything in this presentation is an opinion and is not to be construed as consulting advice or official guidance.

We are simply cybersecurity professionals reading the rule and trying to figure it out, just like you.

As more clarification is provided, our understanding will increase.

Did CMMC get harder?

(3) *NOT APPLICABLE (N/A).* A security requirement and/or objective does not apply at the time of the CMMC assessment. For example, CMMC security requirement SC.L1-3.13.5 "Public-Access System Separation" might be N/A if there are no publicly accessible systems within the CMMC Assessment Scope. During an assessment, an assessment objective assessed as N/A is equivalent to the same assessment objective being assessed as MET.

Assessors are enabled to accept requirements as
Not Applicable without relying on higher authority?

(9) If an OSC previously received a favorable adjudication from the DoD CIO for an alternative security measure (in accordance with DFARS provision 252.204-7008 (48 CFR 252.204-7008) or DFARS clause 252.204-7012 (48 CFR 252.204-7012)), the DoD CIO adjudication must be included in the system security plan to receive consideration during an assessment. Implemented security measures adjudicated by the DoD CIO as equally effective is assessed as MET if there have been no changes in the environment.

(2) *CMMC Level 2 Self-Assessment and CMMC Level 2 Certification Assessment*. An OSA is only permitted to have a POA&M for CMMC Level 2 if all the following conditions are met:

(i) The assessment score divided by the total number of security requirements is greater than or equal to 0.8;

(ii) None of the security requirements included in the POA&M have a point value of greater than 1 as specified in the CMMC Scoring Methodology set forth in § 170.24, except SC.L2-3.13.11 CUI Encryption may be included on a POA&M if it has a value of 1 or 3; and

(iii) None of the following security requirements are included in the POA&M:

(A) AC.L2-3.1.20 External Connections (CUI Data).

(B) AC.L2-3.1.22 Control Public Information (CUI Data).

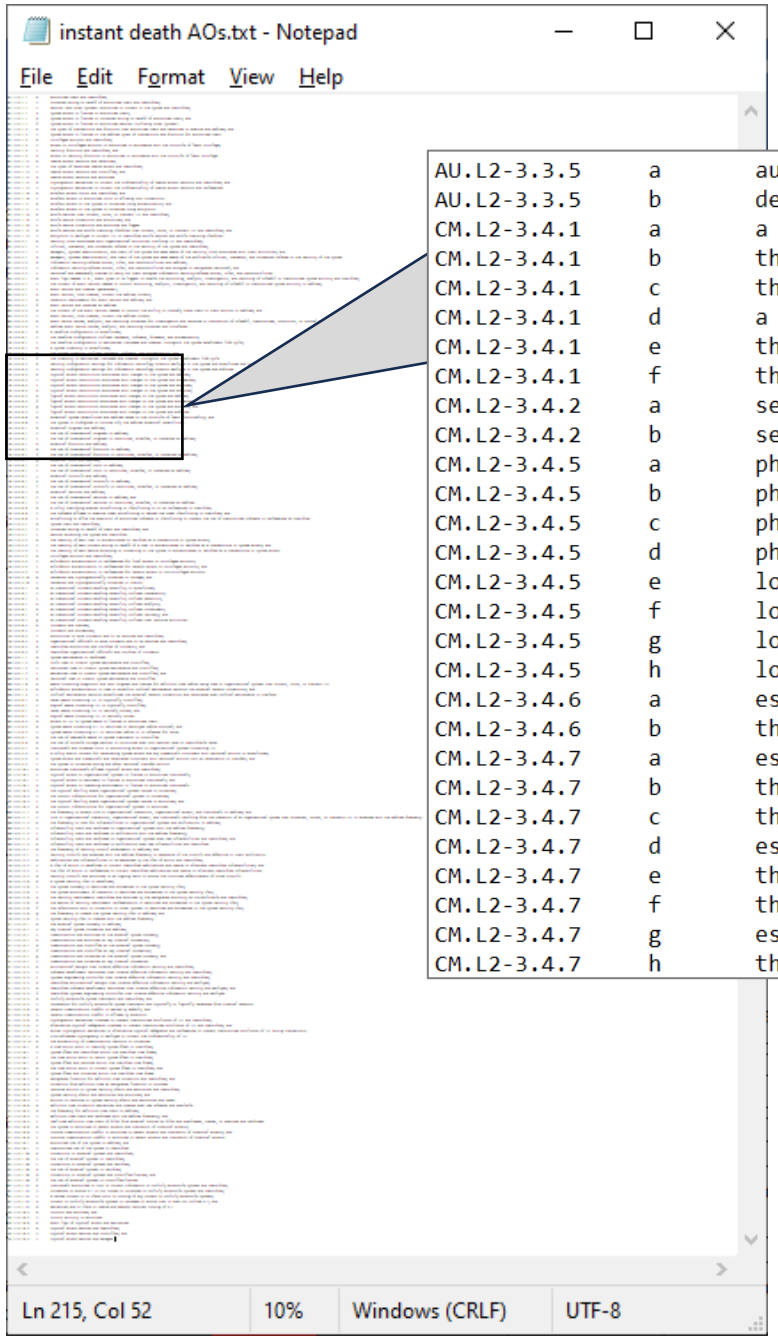
(C) PE.L2-3.10.3 Escort Visitors (CUI Data).

(D) PE.L2-3.10.4 Physical Access Logs (CUI Data).

(E) PE.L2-3.10.5 Manage Physical Access (CUI Data).

Discussion

We verified the point values have not changed from the DoD Assessment Methodology



AU.L2-3.3.5	a	audit record review, analysis, and reporting processes for investigation and
AU.L2-3.3.5	b	defined audit record review, analysis, and reporting processes are correlate
CM.L2-3.4.1	a	a baseline configuration is established;
CM.L2-3.4.1	b	the baseline configuration includes hardware, software, firmware, and docume
CM.L2-3.4.1	c	the baseline configuration is maintained (reviewed and updated) throughout t
CM.L2-3.4.1	d	a system inventory is established;
CM.L2-3.4.1	e	the system inventory includes hardware, software, and documentation; and
CM.L2-3.4.1	f	the inventory is maintained (reviewed and updated) throughout the system dev
CM.L2-3.4.2	a	security configuration settings for information technology products employed
CM.L2-3.4.2	b	security configuration settings for information technology products employed
CM.L2-3.4.5	a	physical access restrictions associated with changes to the system are defir
CM.L2-3.4.5	b	physical access restrictions associated with changes to the system are docum
CM.L2-3.4.5	c	physical access restrictions associated with changes to the system are appro
CM.L2-3.4.5	d	physical access restrictions associated with changes to the system are enfor
CM.L2-3.4.5	e	logical access restrictions associated with changes to the system are define
CM.L2-3.4.5	f	logical access restrictions associated with changes to the system are docume
CM.L2-3.4.5	g	logical access restrictions associated with changes to the system are approv
CM.L2-3.4.5	h	logical access restrictions associated with changes to the system are enforc
CM.L2-3.4.6	a	essential system capabilities are defined based on the principle of least fu
CM.L2-3.4.6	b	the system is configured to provide only the defined essential capabilities.
CM.L2-3.4.7	a	essential programs are defined;
CM.L2-3.4.7	b	the use of nonessential programs is defined;
CM.L2-3.4.7	c	the use of nonessential programs is restricted, disabled, or prevented as de
CM.L2-3.4.7	d	essential functions are defined;
CM.L2-3.4.7	e	the use of nonessential functions is defined;
CM.L2-3.4.7	f	the use of nonessential functions is restricted, disabled, or prevented as d
CM.L2-3.4.7	g	essential ports are defined;
CM.L2-3.4.7	h	the use of nonessential ports is defined;

215 of 320 (67%) assessment objectives are not allowed POA&M *instant certification failure*

AUTHORIZED C3PAO

(2) If the OSA utilizes an External Service Provider (ESP), other than a Cloud Service Provider (CSP), the ESP must have a CMMC Level 2 Final Certification Assessment. If the ESP is internal to the OSA, the security requirements implemented by the ESP should be listed in the OSA's SSP to show connection to its in-scope environment. 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. If using a CSP for Level 2 Self-Assessment, see § 170.16(c)(2). If using a CSP for Level 2 Certification Assessment, see § 170.17(c)(5).

External Service Provider (ESP) means external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and / or cybersecurity services on behalf of the organization. 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. (CMMC-custom term)

Cloud Service Provider (CSP) means an external company that provides a platform, infrastructure, applications, and/or storage services for its clients.(Source: CISA Cloud Security Technical Reference Architecture; see https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf; page 44.)

FedRAMP Moderate Equivalency for Cloud Providers

equivalent to those established by the FedRAMP Moderate (or higher) baseline. Equivalency is met if the OSA has the CSP's System Security Plan (SSP) or other security documentation that describes the system environment, system responsibilities, the current status of the Moderate baseline controls required for the system, and a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800-171 Rev 2 requirements. (See https://www.fedramp.gov/assets/resources/documents/FedRAMP_Moderate_Security_Controls.xlsx.)

Scoping errata

- No clarification about scoping for Virtual Desktop Infrastructure
- Security protection assets assessed against **all** requirements
  - adds 30-80% additional assessment effort compared to DIBCAC precedent
  - Security system types typically 3-1 ratio to CUI system types
- Out of Scope adds language “because they are physically or logically separated…”
- No language forcing onsite visits by assessors (1 site = precedent)
- Not much linking contract-specific CUI to certified information system

Discussion

CMMC is harder – what now?

1. In-house IT services unless you are SURE your provider will pass CMMC (and be early)?

   ESP can self-attest until you need certification, then must be certified before you

2. Migrate to FedRAMP clouds for security services (SIEM, antivirus, endpoint manager)?
3. Talk with your chosen C3PAO about scoping early?

   The “hard to secure” systems like dev labs, job-specific systems can often be categorized as Specialized Assets

4. Build an enclave that can pass ASAP, then migrate other systems to it over time?

KIERI

Reporting

CMMC Level 2 Self-Assessment Reporting

A senior official from the prime contractor and any applicable subcontractor will be required to affirm continuing compliance with the specified security requirements after every assessment, including POA&M closeout, and annually thereafter. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements and procedures).

Self-Assessment doesn't allow NOT-METs

Discussion

- CMMC Level 1 self-assessments do not allow any not-met requirements (must be perfect)
- CMMC Level 2 self-assessments have same POA&M requirements as certifications (180 days max, then must be perfect).
- No long-term compliant option for contractors other than full implementation
  - Either attest to full compliance or be ineligible to win contracts?
  - Contractors that won't attest are reliant upon CMMC being waived at the RFP?

What about Joint Surveillance?

§ 170.20 Standards acceptance.

(a) *NIST SP 800-171 Rev 2 DoD assessments*. In order to avoid duplication of efforts, thereby reducing the aggregate cost to industry and the Department, OSCs that have completed a DCMA DIBCAC High Assessment aligned with CMMC Level 2 Scoping will be eligible for CMMC Level 2 Final Certification Assessment under the following conditions:

(1) *DCMA DIBCAC High Assessment*. An OSC that achieved a perfect score with no open POA&M from a DCMA DIBCAC High Assessment conducted prior to the effective date of this rule, is eligible for a CMMC Level 2 Final Certification Assessment with a validity period of three (3) years from the date of the original DCMA DIBCAC High Assessment. Eligible DCMA DIBCAC High Assessments include ones conducted with Joint Surveillance in accordance with the DCMA Manual 2302-01 Surveillance. The scope of the CMMC Level 2 Final Certification Assessment is identical to the scope of the DCMA DIBCAC High Assessment.

Joint Surveillance Voluntary Assessments

- (Good) Translate into a CMMC Level 2 certification
- (Not as good) Expire 3 years after initial assessment
- Are JSVA worth it?
  - Different rules than CMMC assessments - much easier!
  - ?? Will DIBCAC change their scoping to match CMMC rule?
    - Expanded scoping not justifiable per current regulations
  - Avoids assessor shortage
  - Extend timeline to respond to CMMC changes

KIERI

Costs

CMMC Level 2 cost

- **C3PAO Costs:** C3PAO engagement inclusive of Phases 1, 2, and 3 (3-person team)

for 120 hours ($260.28/hr x 120hrs = **$31,234**)

This would be the “average” cost, which is skewed toward smaller businesses and enclaves.

Level of effort at 120 hours = 15 assessor-days per Level 2 assessment. Three assessors for one week.

Does not seem to include pre-and-post assessment planning, reporting, quality review, and appeals.

Does not include cost of external service provider assessments.

Ecosystem

CCPs will…

CCPs are eligible to become CMMC Certified Assessors and can participate as a CCP on CMMC Level 2 Certification Assessments with CCA oversight where the CCA makes all final determinations.

CCAs will…

(6) Be a CCP who has at least 3 years of cybersecurity experience, 1 year of assessment or audit experience, and at least one baseline certification aligned to either paragraph (b)(6)(i) or (ii) of this section through 15 February 2025 and aligned to paragraph (b)(6)(ii) of this section only beginning 16 February 2025.

(i) IAT Level II from DoD Manual 8570 Information Assurance Workforce Improvement Program.

(ii) Intermediate Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program.

KIERI

Approved Baseline Certifications

IAT Level I[2]	IAT Level II[2]	IAT Level III
A+ CE	CCNA-Security	CASP+ CE
CCNA-Security	CySA+ **	CCNP Security
CND	GICSP	CISA
Network+ CE	GSEC	CISSP (or Associate)
SSCP	Security+ CE	GCED
	CND	GCIH
	SSCP	CCSP
IAM Level I	**IAM Level II**	**IAM Level III**
CAP	CAP	CISM
CND	CASP+ CE	CISSP (or Associate)
Cloud+	CISM	GSLC
GSLC	CISSP (or Associate)	CCISO
Security+ CE	GSLC	
HCISPP	CCISO	
	HCISPP	
IASAE I	**IASAE II**	**IASAE III**
CASP+ CE	CASP+ CE	CISSP-ISSAP
CISSP (or Associate)	CISSP (or Associate)	CISSP-ISSEP
CSSLP	CSSLP	CCSP

DoD 8570 Certifications

https://public.cyber.mil/wid/cwmp/dod-approved-8570-baseline-certifications/

CYBER AB CMMC CERTIFICATION
AUTHORIZED C3PAO

KIERI

		Basic	Intermediate	Advanced
Foundational Qualification Options	**Education**	Associate degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university	Bachelor degree or higher from an accredited college or university
	OR	*OR*	*OR*	*OR*
	Training	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository
	OR	*OR*	*OR*	*OR*
	Personnel Certification	GSEC or Security+	CAP or CASP+ or Cloud+ or CYSA+ or PenTest+	CCISO or CISA or CISM or CISSP or CISSP-ISSEP or GSLC or GSNA
Foundational Qualification Alternative	**Experience**	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification	**On-the-Job Qualification**	Always Required	Always Required	Always Required
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Annual Maintenance	**Continuous Professional Development**	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.

DoD 8140 (Modernization of 8570):

https://dl.dod.cyber.mil/wp-content/uploads/cwmp/xls/unclass-dod_8140_foundational_qualification_options.xlsx

Lead CCAs (one per assessment required) will…

(7) Qualify as a Lead CCA by having at least 5 years of cybersecurity experience, 5 years of management experience, 3 years of assessment or audit experience, and at least one baseline certification aligned to either paragraph (b)(7)(i) or (ii) of this section through 15 February 2025 and aligned to paragraph (b)(7)(ii) of this section only beginning 16 February 2025.

(i) IAM Level II from DoD Manual 8570 Information Assurance Workforce Improvement Program.

(ii) Advanced Proficiency Level for Career Pathway Certified Assessor 612 from DoD Manual 8140.03 Cyberspace Workforce Qualification & Management Program.

KIERI

CCIs (CMMC Certified Instructor) will…

(5) Not provide CMMC consulting services while serving as a CMMC instructor.

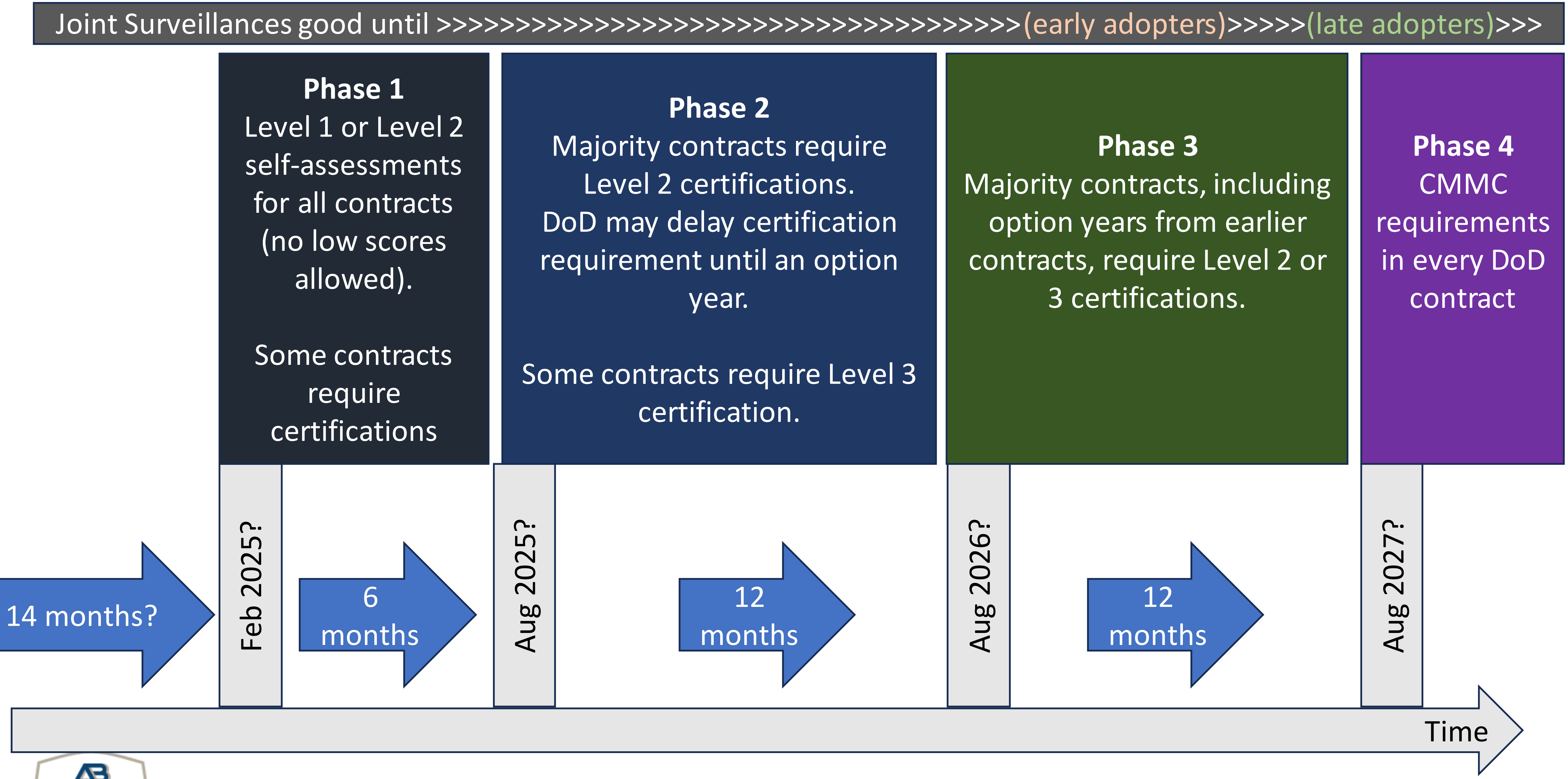
What is the COI concern?

Best guess: Instructor teaching students how to do CMMC then assessing (and passing) the students' companies because they did it "right".

If this is the concern, the rule should say "Not provide CMMC **assessment** services while serving as a CMMC instructor."

Professionals divided on whether this is limited to "during class" or is intended to prevent all consulting jobs during the time employed as an instructor.

Timeline



Discussion

Certification Availability

Discussion

- Today CMMC assessments “not allowed because CMMC doesn’t exist”

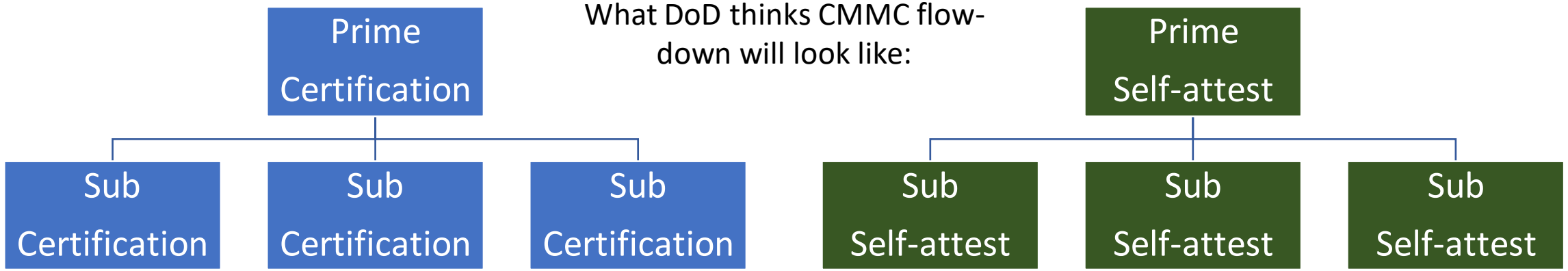
- How can we get dependencies (subcontractors and external providers) certified before day one?

(2) If a subcontractor will process, store, or transmit CUI in performance of the subcontract, CMMC Level 2 Self-Assessment is the minimum requirement for the subcontractor.

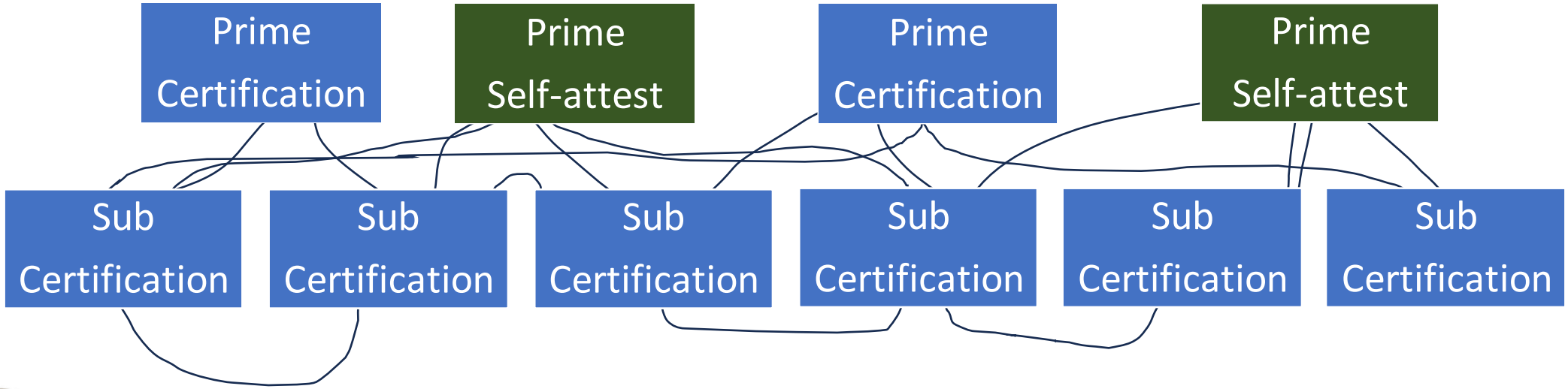
(3) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has a requirement of Level 2 Certification Assessment, then CMMC Level 2 Certification Assessment is the minimum requirement for the subcontractor.

(4) If a subcontractor will process, store, or transmit CUI in performance of the subcontract and the Prime contractor has a requirement of Level 3 Certification Assessment, then CMMC Level 2 Certification Assessment is the minimum requirement for the subcontractor.

What DoD thinks CMMC flow-down will look like:



What CMMC flow-down will actually look like:



Lack of language tying CMMC Certification to contract-specific CUI. Ultra Primes will need Level 3. All subs flowed down Level 2/3 certification??

CMMC Level 2 Certification Assessments

(C) For each Assessor conducting the assessment, name and business contact information.

(D) All industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope.

(E) The name, date, and version of the SSP.

(F) Title 32 program rule (32 CFR part 170) at time of assessment

(G) Certification date.

(H) Assessment result for each requirement objective.

(I) POA&M usage and compliance, as applicable.

Is this how changes to requirements (such as 800-171 Rev. 3) will be implemented (via 32 CFR rulemaking)?

Commenting. Will it help?

Discussion

Final thoughts?

Brian Hubbard
(CCA, PI)

Jil Wright
(CCA, PI)

Vince Scott
(CCA, PI)

Amira Armond
(CCA, PI)

Kieri Solutions, an Authorized C3PAO

www.kieri.com

- Assessment and preparation assistance
  - Expertise: 9 Certified CMMC Assessors and Instructors, plus CCPs
  - Fortune 100s to small businesses
- Kieri Reference Architecture
  - Do-it-yourself (or with help) *functional and expandable* Level 2 enclave.
  - Microsoft 365 / Windows Laptops / BYOD Phones
- Kieri Compliance Documentation
  - Do-it-yourself docs and instructions to run a compliant IT Department
  - Uses behavior stacking, just-in-time procedures, convenient record-keeping
  - Training library and monthly Q&As

CYBER AB CMMC CERTIFICATION AUTHORIZED C3PAO

Kieri Solutions cannot certify companies that we've consulted for (including KRA / KCD)

KIERI

Links to the CMMC Proposed Rule 32 CFR (CMMC Program Establishment)

- **Downloadable PDF of Federal Register text (this version has page numbers):** https://public-inspection.federalregister.gov/2023-27280.pdf
- **Federal Register home page for CMMC and comments:** https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program
- **Docket Information (the rule agenda):** https://www.regulations.gov/docket/DOD-2023-OS-0063
- **Public comments posted regarding rule:** https://www.regulations.gov/document/DOD-2023-OS-0063-0001
- **Regulatory Impact Analysis 32 CFR Part 170 (analysis of changes and cost):** https://www.regulations.gov/document/DOD-2023-OS-0063-0003
- **Initial Regulatory Flexibility Analysis 32 CFR (benefits and costs, impact to small business):** https://www.regulations.gov/document/DOD-2023-OS-0063-0002

Links to the CMMC Proposed Rule CMMC Guides

- **CMMC Guidance documents home and comments page:** https://www.regulations.gov/docket/DOD-2023-OS-0096/document
- **Notice of Guidance for CMMC:** https://www.regulations.gov/document/DOD-2023-OS-0096-0001
- **CMMC Model Overview:** https://www.regulations.gov/document/DOD-2023-OS-0096-0006
- **Scoping Guide – CMMC Level 1:** https://www.regulations.gov/document/DOD-2023-OS-0096-0007
- **Scoping Guide – CMMC Level 2:** https://www.regulations.gov/document/DOD-2023-OS-0096-0003
- **Scoping Guide – CMMC Level 3:** https://www.regulations.gov/document/DOD-2023-OS-0096-0008
- **Assessment Guide – CMMC Level 1:** https://www.regulations.gov/document/DOD-2023-OS-0096-0002
- **Assessment Guide – CMMC Level 2:** https://www.regulations.gov/document/DOD-2023-OS-0096-0005
- **Assessment Guide – CMMC Level 3:** https://www.regulations.gov/document/DOD-2023-OS-0096-0004
- **Hashing Guide (used during assessments only):** https://www.regulations.gov/document/DOD-2023-OS-0096-0009

Links to the CMMC Proposed Rule Assessment Reporting Templates

- **Assessment reporting home and comments page:** https://www.regulations.gov/document/DOD-2023-OS-0097-0001
- **Paperwork Reduction Act review:** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/content.docx
- **CMMC Level 2 Pre-Assessment Reporting:** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_2.xlsx
- **CMMC Level 2 Assessment Results Reporting:** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_4.xlsx
- **CMMC Level 3 Pre-Assessment Reporting Mock-up:** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_1.xlsx
- **CMMC Level 3 Assessment Results Reporting Mock-up:** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_3.xlsx
- **Hashing Guide (again):** https://downloads.regulations.gov/DOD-2023-OS-0097-0001/attachment_5.docx

Links to the CMMC Proposed Rule eMASS Reporting Job Aid

- **eMASS job aid home and comments:** https://www.regulations.gov/document/DOD-2023-OS-0097-0002
- **eMASS User Job Aid:** https://downloads.regulations.gov/DOD-2023-OS-0097-0002/attachment_1.pdf

Links to the CMMC Proposed Rule 48 CFR (DFARS 252.204-7012? 7021?

- **48 CFR tracking page (due in 2024):**

https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=0750-AK81