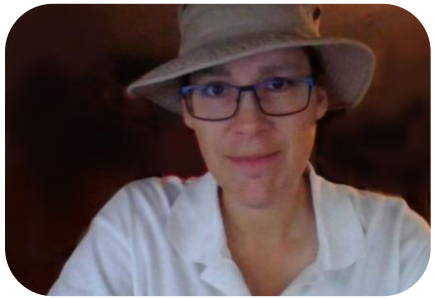
Review of the CMMC Final Rule
32 CFR (Establish CMMC Program)

October 14, 2024

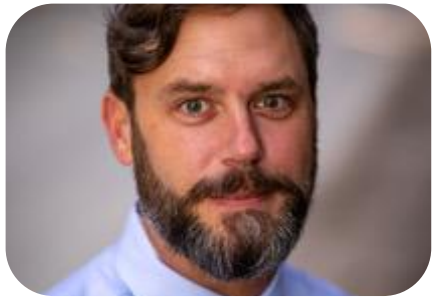
Speakers



Amira Armond (CCA, PI), Kieri Solutions

Vince Scott (CCA, PI), Defense Cybersecurity Group

Brian Hubbard (CCA, PI), MSPCyberX, Evolved Cyber



Logan Therrien (CCA), Kieri Solutions

Jonathan Weadon (CCA), Kieri Solutions

Kieri Solutions, an Authorized C3PAO

www.kieri.com

- Assessment and preparation assistance
  - Expertise: 12 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 network.
  - 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

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

KIERI

Review of 32CFR

Quoted text is from:
https://public-inspection.federalregister.gov/2024-22905.pdf

CUI Assets

"• Assets that process, store, or transmit CUI"

"[Assessor instructions:] Assess against all Level 2 security requirements"

"Process, store, or transmit means **data can be used by an asset** (e.g., accessed, entered, edited, generated, manipulated, or printed); data is inactive or at rest on an asset (e.g., located on electronic media, in system component memory, or in physical format such as paper documents); or data is being transferred from one asset to another asset (e.g., data in transit using physical or digital transport methods). (CMMC-custom term)"

Access?

“The DoD intended “Access” to be included in the “Process, store, or transmit definition as written in § 170.4(b).”

“**All assets within an OSA defined CMMC Level 2 or 3 assessment boundary have access to CUI** and can process, store, or transmit CUI. They are therefore subject to DFARS clause 252.204-7012 and required to meet NIST SP 800-171 requirements. This is the authority for including Contractor Risk Managed Assets (CRMAs) within CMMC assessments. For Level 2, DoD has decided to assume some risk and lessen the assurance burden for a class of these assets called Contractor Risk Managed Assets, as specified in table 3 to § 170.19(c)(1). DoD does not assume this risk at Level 3. CRMAs are subject to assessment against all CMMC requirements as specified in table 5 to § 170.19(d)(1).

Security Protection Assets

“• Assets that provide security functions or capabilities to the OSC’s CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI”

“[OSA Instructions] • Prepare to be assessed against CMMC Level 2 security requirements”

“[Assessor instructions:] Assess against Level 2 security requirements that are relevant to the capabilities provided “

Contractor Risk Managed Assets

"• Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place
• Assets are not required to be physically or logically separated from CUI assets"

"Contractor Risk Managed Assets (CRMA) should be prepared to be assessed against CMMC security requirements at Level 2, and included in the SSP, asset inventory, and network diagrams."

"All CMMC security requirements must be MET when the OSA chooses to designate certain assets as Contractor Risk Managed Assets."

"[Assessor instructions] • Review the SSP: • If sufficiently documented, do not assess against other CMMC security requirements, except as noted… [continues to discuss limited spot checks]"

Specialized Assets

“Specialized Assets, which are assets that can process, store, or transmit CUI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment, **are documented but are not assessed against other CMMC security requirements**, as addressed in table 3 to § 170.19(c)(1).”

Out of Scope Assets

"• Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets
• Assets that are physically or logically separated from CUI assets
• Assets that fall into any in-scope asset category cannot be considered an Out-of-Scope Asset"

"An endpoint hosting a VDI client configured to not allow any processing, storage, or transmission of CUI beyond the Keyboard/Video/Mouse sent to the VDI client is considered an Out-of-Scope Asset"

"[OSA instructions:] Prepare to justify the inability of an Out-of-Scope Asset to process, store, or transmit CUI"

Not Applicable and Alternate Implementations

“Not Applicable (N/A). A security requirement and/or objective does not apply at the time of the CMMC assessment. For example, Public-Access System Separation (SC.L2-3.13.5) 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.”

“If an OSC previously received a favorable adjudication from the DoD CIO indicating that a security requirement is not applicable or that an alternative security measure is equally effective (in accordance with 48 CFR 252.204-7008 or 48 CFR 252.204-7012), the DoD CIO adjudication must be included in the system security plan to receive consideration during an assessment. A security requirement for which implemented security measures have been adjudicated by the DoD CIO as equally effective is assessed as MET if there have been no changes in the environment.”

External Systems

“Establishing a VPN connection with MSP equipment **brings that equipment into the OSA's assessment scope**. The equipment must meet the OSA's requirements for external access and connection to the network.”

“When the ESP is using a **Virtual Desktop solution, then the endpoint client device will be considered out of scope** when it is configured to prevent storage, processing, or transmission of CUI on the end client beyond the Keyboard, Video, Mouse input that is part of the Virtual Desktop Infrastructure (VDI) solution.”

“When an ESP is providing staff augmentation to the OSA **and the OSA is providing all the systems used for remote access**, then the OSA’s policies and procedures apply **and the ESP is not considered to be processing, storing, or transmitting CUI**.

Security Protection Data

	When utilizing an ESP that is:	
When the ESP processes, stores, or transmits:	**A CSP**	**Not a CSP**
CUI (with or without SPD)	The CSP shall meet the FedRAMP requirements in 48 CFR 252.204-7012.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment.
SPD (without CUI)	The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.	The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets.

"Security Protection Data (SPD) means data stored or processed by Security Protection Assets (SPA) that are used to protect an OSC's assessed environment. SPD is security relevant information and includes but is not limited to: configuration data required to operate an SPA, log files generated by or ingested by an SPA, data related to the configuration or vulnerability status of in-scope assets, and passwords that grant access to the in-scope environment. (CMMC-custom term)"

A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP.

Clouds

“An ESP is considered a Cloud Service Provider (CSP) when it provides its own cloud services based on a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing that can be rapidly provisioned and released with minimal management effort or service provider interaction on the part of the OSA.”

“ESPs that are CSPs, and process, store, or transmit CUI, must meet the FedRAMP requirements in DFARS clause 252.204-7012. ESPs that are CSPs and do not process, store, or transmit CUI, are not required to meet FedRAMP requirements in DFARS clause 252.204-7012.”

“An ESP may utilize cloud offerings to deliver services to clients without being a CSP. An ESP that manages a third-party cloud service on behalf of an OSA would not be considered a CSP.”

Cost of Assessment

“For CMMC Levels 1 and 2, the cost estimates are based only upon the self-assessment, certification assessment, and affirmation activities that a defense contractor, subcontractor, or ecosystem member must take to allow DoD to verify implementation of the relevant underlying security requirements.”

“DoD did not consider the cost of implementing the security requirements themselves because implementation is already required by FAR clause 52.204-21, effective June 15, 2016, and by DFARS clause 252.204-7012, requiring implementation by Dec. 31, 2017, respectively; therefore, the costs of implementing the security requirements for CMMC Levels 1 and 2 should already have been incurred and are not attributed to this rule.”

Cost of Assessment

“An Assessment Team must include at least two people: a Lead CCA, as defined in § 170.11(b)(10), and at least one other CCA. Additional CCAs and CCPs may also participate on an Assessment Team.”

“[C3PAOs will] Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into the CMMC instantiation of eMASS. Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role. A quality assurance individual shall manage the C3PAO’s quality assurance reviews as defined in paragraph (b)(14) of this section and the appeals process”

“[C3PAOs will] Require all C3PAO company personnel participating in the Level 2 certification assessment process to complete a Tier 3 background investigation resulting in a determination of national security eligibility.”

Qualifications of CCA / Lead CCA

"[All assessment team members] Meet the equivalent of a favorably adjudicated Tier 3 background investigation when not eligible for a Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only."

"[to qualify as a CCA] Be a CCP who has at least 3 years of cybersecurity experience, at least 1 year of assessment or audit experience, and at least one foundational qualification, aligned to at least the Intermediate Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03"

CGRC/CAP or CASP+ or Cloud+ or PenTest+ or Security+ or GSEC

"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 foundational qualification aligned to Advanced Proficiency Level of the DoD Cyberspace Workforce Framework's Security Control Assessor (612) Work Role, from DoD Manual 8140.03"

CISM or CISSO or CPTE or CySA+ or FITSP-A or GCSA or CISA or CISSP or CISSP-ISSEP or GSLC or GSNA

Cost – Small entities

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.

Numbers over phase-in period

Table 8 - *Number of Total Entities Over Phase-In Period

	Level 1	Level 2	Level 2	Level 3	
Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	945	27	517	4	1,493
2	4,720	136	2,599	50	7,505
3	15,748	453	8,666	169	25,036
4	30,184	867	16,610	323	47,984
5	30,179	867	16,606	323	47,975
6	30,179	867	16,606	323	47,975
7	27,246	783	14,994	295	43,318
Tot	**139,201**	**4,000**	**76,598**	**1,487**	**221,286**

Certification Requirements

“Level 1 self-assessment. To comply with CMMC Level 1 self-assessment requirements, the OSA must meet the requirements detailed in paragraphs (a)(1) and (2) of this section.”

“Conditional Level 2 (Self). The OSA has achieved the CMMC Status of Conditional Level 2 (Self) if the Level 2 self-assessment results in a POA&M and the POA&M meets all the CMMC Level 2 POA&M requirements listed in § 170.21(a)(2). “

“Final Level 2 (Self). The OSA has achieved the CMMC Status of Final Level 2 (Self) if the Level 2 self-assessment results in a passing score as defined in § 170.24.”

“Conditional Level 2 (C3PAO). The OSC has achieved the CMMC Status of Conditional Level 2 (C3PAO) if the Level 2 certification assessment results in a POA&M and the POA&M meets all CMMC Level 2 POA&M requirements listed in § 170.21(a)(2).”

“Level 2 certification assessment requirements. The OSC must complete and achieve a MET result for all security requirements specified in § 170.14(c)(3) to achieve the CMMC Status of Level 2 (C3PAO).”

Essentially, Level 1 = all requirements MET
Level 2 = some may be POA&M’d for 180 days. Then all requirements MET
Level 3 = all requirements MET

Organization-Defined Parameters (ODPs)

"The security requirements in CMMC Level 3 are selected from NIST SP 800-172 Feb2021, and where applicable, Organization-Defined Parameters (ODPs) are assigned."

Examples:

"AC.L3-3.1.3e Employ ***secure information transfer solutions*** to control information flows between security domains on connected systems."

"IR.L3-3.6.2e Establish and maintain a cyber-incident response team that can be deployed by the organization within ***24 hours***."

KIERI

Rev 2 or Rev 3?

“Commenters expressed concern about the confusion between the NIST 800-171 R2 being included in the CMMC rule and not the recently published Rev 3.“

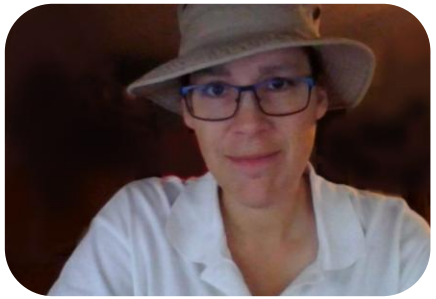
“[Response:] Specifying a revision benefits the CMMC Ecosystem by ensuring it moves forward from one NIST standard to the next in an organized manner. The DoD cites NIST SP 800-171 R2 in this final rule for a variety of reasons, including the time needed for industry preparation to implement and time needed to prepare the CMMC Ecosystem to perform assessments against subsequent revisions.”

KIERI

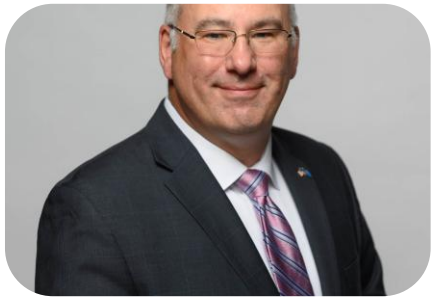
Kieri Solutions, an Authorized C3PAO

www.kieri.com

Questions and closing thoughts

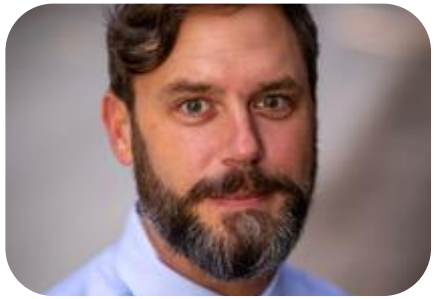


Amira Armond (CCA, PI), Kieri Solutions



Vince Scott (CCA, PI), Defense Cybersecurity Group

Brian Hubbard (CCA, PI), MSPCyberX, Evolved Cyber



Logan Therrien (CCA), Kieri Solutions

Jonathan Weadon (CCA), Kieri Solutions

AUTHORIZED C3PAO