The Wait is Over…The Final CMMC Rule Explained

October 17, 2024

NeoSystems® FutureFeed Holland & Knight

Disclaimer

This webinar is provided as a public service. The content is intended for informational purposes only and is not intended to, nor does it, constitute legal or business advice. By providing this information, we are not acting as your lawyer. There are many subtleties to these topics that cannot be comprehensively addressed in a webinar. You are strongly encouraged to contact a competent attorney before taking any action. All content and opinions are strictly those of the presenter and are not representative of any presenter's employer(s), affiliated entities, clients, or their associates.

Agenda

1. Why the CMMC Program Exists and How We Got Here
2. How to Read the Rule (Hint: Don’t Start on Page 1)
3. What Else is Needed for CMMC Requirements to Appear in Contracts
4. The Basics: Levels, Assessments, POA&Ms, and Affirmation
5. Timeline for Rollout of the CMMC Program
6. Scoping
7. The Role and Value of External Service Providers
8. Cost of An Assessment
9. Looking Ahead
10. Questions (and Answers)

NeoSystems

FutureFeed

Holland & Knight

Our Speakers

Stuart Itkin
NeoSystems

Stuart Itkin brings unique perspective to CMMC and the challenges organizations face in satisfying government regulations. As Senior Vice President of NeoSystems, Stuart is focused on bringing managed IT and security services to address the cybersecurity and compliance needs of small and medium businesses. He formerly served as Vice President of CMMC and FedRAMP Assurance at Coalfire Federal and as Vice President of Product Management and Marketing at Exostar. Stuart was a member of the CMMC Standards Working Group and currently serves as a Director of MSPs for the Protection of Critical Infrastructure and for the CMMC Industry Standards Council.

James Goepel
FutureFeed

Jim is the General Counsel and Director of Education for FutureFeed. He helps ensure that the FutureFeed platform meets defense contractors' CMMC compliance needs and helps FutureFeed clients feel more confident in their compliance programs. Prior to earning his two law degrees, Jim was an IT and cyber professional and software developer with the United States Congress; a software developer on US Navy contracts; and an engineer with a large defense contractor in the space program. He is a former professor of cybersecurity and has written and taught a variety of courses, including the Cyber AB's initial Registered Practitioner course. Jim is also the author of 2 books on Controlled Unclassified Information.

Eric Crusius
Holland & Knight

Eric is a partner with the law firm of Holland & Knight. He is an accomplished and well-regarded government contracts and cybersecurity attorney with more than 20 years of experience. He is an experienced litigator, taking cases to trial in state and federal court on behalf of contractors. Eric also regularly counsels contractors of all sizes regarding their cybersecurity compliance obligations, assists companies with cybersecurity incident responses, and advises clients on strategic choices based on current and future cybersecurity and other regulatory requirements.

How We Got Here...

- DoD released DFARS 252.204-7012 requiring contractors to self-assess compliance with NIST SP 800-171.
- DoD doubted that contractors were compliant with NIST 800-171 despite the requirement in the DFARS.
- DoD then released DFARS 252.204-7020 requiring contractors to report their compliance with NIST SP 800-171 in the Supplier Performance Risk System.
- DoD has visibility into whether contractors are compliant with NIST 800-171 and likely sees that most of the DIB is not.
- DoD is now seeking further verification of compliance with required cybersecurity controls.

32 CFR 170 Final Rule (a.k.a. CMMC v.2.13)

- 470 pages
- 140,000 words
- Core concepts have not changed since CMMC 2.0
- Many changes

https://www.govinfo.gov/content/pkg/FR-2024-10-15/pdf/2024-22905.pdf

83092 **Federal Register** / Vol. 89, No. 199 / Tuesday, October 15, 2024 / Rules and Regulations

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 170

[Docket ID: DoD–2023–OS–0063]

RIN 0790–AL49

Cybersecurity Maturity Model Certification (CMMC) Program

AGENCY: Office of the Department of Defense Chief Information Officer (CIO), Department of Defense (DoD).

ACTION: Final rule.

SUMMARY: With this final rule, DoD establishes the Cybersecurity Maturity Model Certification (CMMC) Program in order to verify contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The mechanisms discussed in this rule will allow the Department to confirm a defense contractor or subcontractor has implemented the security requirements for a specified CMMC level and is maintaining that status (meaning level and assessment type) across the contract period of performance. This rule will be updated as needed, using the appropriate rulemaking process, to address evolving cybersecurity standards, requirements, threats, and other relevant changes.

DATES: This rule is effective December 16, 2024. The incorporation by reference of certain material listed in this rule is approved by the Director of the Federal Register as of December 16, 2024.

FOR FURTHER INFORMATION CONTACT: Ms. Diane Knight, Office of the DoD CIO at *osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil* or 202–770–9100.

SUPPLEMENTARY INFORMATION:

History of the Program

The beginnings of CMMC start with the November 2010, Executive Order (E.O.) 13556,[1] *Controlled Unclassified Information*. The intent of this Order was to "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls." Prior to this E.O., more than 100 different markings for this information existed across the executive branch. This ad hoc, agency-specific approach created inefficiency and confusion, led to a patchwork system that failed to adequately safeguard information requiring protection, and unnecessarily restricted information-sharing.

As a result, the E.O. established the CUI Program to standardize the way the executive branch handles information requiring safeguarding or dissemination controls (excluding information that is classified under E.O. 13526, Classified National Security Information [2] or any predecessor or successor order; or the Atomic Energy Act of 1954,[3] as amended).

In 2019, DoD announced the development of CMMC in order to move away from a "self-attestation" model of security. It was first conceived by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) to secure the Defense Industrial Base (DIB) sector against evolving cybersecurity threats. In September 2020, DoD published the 48 CFR CMMC interim final rule, *Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements* (DFARS Case 2019–D041 85 FR 48513, September 9, 2020),[4] which implemented the DoD's vision for the initial CMMC Program and outlined the basic features of the framework (tiered model of practices and processes, required assessments, and implementation through contracts) to protect FCI and CUI. The 48 CFR CMMC interim final rule became effective on 30 November 2020, establishing a five-year phase-in period. In response to approximately 750 public comments on the 48 CFR CMMC interim final rule, in March 2021, the Department initiated an internal review of CMMC's implementation.

In November 2021, the Department announced the revised CMMC Program, an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

The revised CMMC Program has three key features:

- *Tiered Model:* CMMC requires companies entrusted with Federal contract information and controlled unclassified information to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also describes the process for requiring protection of information flowed down to subcontractors.
- *Assessment Requirement:* CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- *Phased Implementation:* Once CMMC rules become effective, certain DoD contractors handling FCI and CUI will be required to achieve a particular CMMC level as a condition of contract award. CMMC requirements will be implemented using a 4-phase implementation plan over a three-year period.

Current Status of the CMMC Program

Separate from this rulemaking, DoD has a proposed acquisition rule (48 CFR part 204 CMMC Acquisition rule) to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to address procurement related considerations and requirements related to this program rule (32 CFR part 170 CMMC Program rule). The 48 CFR part 204 CMMC Acquisition rule also partially implements a section of the National Defense Authorization Act for Fiscal Year 2020 directing the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base.[5] The 48 CFR part 204 CMMC Acquisition rule, when finalized, will allow DoD to require a specific CMMC level in a solicitation or contract. When CMMC requirements are applied to a solicitation, Contracting officers will not make award, exercise an option, or extend the period of performance on a contract, if the offeror or contractor does not have the passing results of a current certification assessment or self-assessment for the required CMMC level, and an affirmation of continuous compliance with the security requirements in the Supplier Performance Risk System (SPRS) [6] for all information systems that process, store, or transmit FCI or CUI during contract performance. Furthermore, the appropriate CMMC certification requirements will flow down to subcontractors at all tiers when

[1] *www.federalregister.gov/citation/75-FR-68675* (November 4, 2010).

[2] *www.federalregister.gov/citation/75-FR-707* (December 29, 2009).

[3] *www.govinfo.gov/link/uscode/42/2011, et seq.*

[4] *www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.*

[5] *www.federalregister.gov/documents/2024/08/15/2024-18110/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.*

[6] *www.sprs.csd.disa.mil/* under OMB control number 0750–0004.

Where to Begin?

- Responses to Comments – p. 1
- Regulatory Necessities – p. 263 (121 pages)
- Rule – p. 384 (86 pages)

Start Here

83214 Federal Register / Vol. 89, No. 199 / Tuesday, October 15, 2024 / Rules and Regulations

commercially available off-the-shelf items; and,

Implementing a phased implementation for CMMC.

In addition, the Department took into consideration the timing of the requirement to achieve a specified CMMC level: (1) at time of proposal or offer submission, (2) after contract award, (3) at the time of contract award, or (4) permitting government Program Managers to seek approval to waive inclusion of CMMC requirements in solicitations and resulting contracts that involve disclosure or creation of FCI or CUI as part of the contract effort. Such waivers will be requested and approved by DoD in accordance with internal policies, procedures, and approval requirements.

The Department ultimately adopted alternatives (3) and (4). The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC level after the release of the solicitation and before contract award. The drawback of alternative 2 (after contract award) is the increased risk to the Department with respect to the costs, program schedule, and uncertainty in the event the contractor is unable to achieve the required CMMC level in a reasonable amount of time given its current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI.

CMMC does not require implementation of any additional security protection requirements beyond those identified in current FAR clause 52.204–21 and in NIST SP 800–171 R2 for CMMC Levels 1 and Level 2, respectively. CMMC Level 3 requirements are new and based upon NIST SP 800–172 Feb2021.

Steps Taken To Minimize Additional Cost of Credit

The DoD is not a ''covered agency'' under 5 U.S.C. 604.

E. Public Law 96–511, ''Paperwork Reduction Act'' (44 U.S.C. Ch

Sections of this ru… information … …ments. As requi… …rk Reduction …hapter 35), DoD has …d information collection packages to the Office of Management and Budget for review and approval. The titles and proposed OMB control numbers are as follows.

- Cybersecurity Maturity Model Certification (CMMC) Enterprise Mission Assurance Support-Service (eMASS) Instantiation Information Collection (OMB control number 0704–0676).
- Cybersecurity Maturity Model Certification (CMMC) Program Reporting and Recordkeeping Requirements Information Collection (OMB Control Number 0704–0677).

In the proposed rule, DoD invited comments on these information collection requirements and the paperwork burden associated with this rule. Five comments were received on the information clearance packages that were not applicable to the information collection requirements; however, the comments were applicable to other aspects of the rule, and they are addressed in the comments section of this preamble. There were no changes to paperwork burden included in the proposed rule that published December 26, 2023 (88 FR 89058) based on public comments received. To review these collections—including all background materials—please visit at *https://www.reginfo.gov/public/do/PRAMain* and use the search function to enter either the title of the collection or the OMB Control Number.

F. Executive Order 13132, ''Federalism''

Executive Order 13132 establishes certain requirements that an agency must meet when it promulgates a final rule that imposes substantial direct requirement costs on state and local governments, preempts state law, or otherwise has federalism implications. This final rule will not have a substantial effect on State and local governments.

G. Executive Order 13175, ''Consultation and Coordination With Indian Tribal Governments''

Executive Order 13175 establishes certain requirements that an agency must meet when it promulgates a f… rule that imposes substantial … compliance costs on … Tribes, preem… …ect… the di… …and …tween the Federal …t and Indian Tribes. This …al rule will not have a substantial effect on Indian Tribal governments.

List of Subjects in 32 CFR Part 170

Certification, CMMC, CMMC Levels, CMMC Program, Contracts, Controlled unclassified information, Cybersecurity, Federal contract information, Government procurement, Incorporation by reference.

■ Accordingly, the Department of Defense adds 32 CFR part 170 to read as follows:

PART 170—CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

Subpart A—General Information

Sec.
170.1 Purpose.
170.2 Incorporation by reference.
170.3 Applicability.
170.4 Acronyms and definitions.
170.5 Policy.

Subpart B—Government Roles and Responsibilities

170.6 CMMC PMO.
170.7 DCMA DIBCAC.

Subpart C—CMMC Assessment and Certification Ecosystem

170.8 Accreditation Body.
170.9 CMMC Third-Party Assessment Organizations (C3PAOs).
170.10 CMMC Assessor and Instructor Certification Organization (CAICO).
170.11 CMMC Certified Assessor (CCA).
170.12 CMMC Instructor.
170.13 CMMC Certified Professional (CCP).

Subpart D—Key Elements of the CMMC Program

170.14 CMMC Model.
170.15 CMMC Level 1 self-assessment and affirmation requirements.
170.16 CMMC Level 2 self-assessment and affirmation requirements.
170.17 CMMC Level 2 certification assessment and affirmation requirements.
170.18 CMMC Level 3 certification assessment and affirmation requirements.
170.19 CMMC scoping.
170.20 Standards acceptance.
170.21 Plan of Action and Milestones requirements.
170.22 Affirmation.
170.23 Application to subcontractors.
170.24 CMMC Scoring Methodology.
Appendix A to Part 170—Guidance

Authority: 5 U.S.C. 301; Sec. 1648, Pub. L. 116–92, 133 Stat. 1198.

Subpart A—General Information.

§ 170.1 Purpose.

(a) This part describes the Cybersecurity Maturity Model Certification (CMMC) Program of the Department of Defense (DoD) and establishes requirements for defense contractors and subcontractors to implement prescribed cybersecurity standards for safeguarding Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). This part (the CMMC Program) also establishes requirements for conducting an assessment of compliance with the applicable prescribed cybersecurity standard for contractor information systems that: process, store, or transmit FCI or CUI; provide security protections for systems which process, store, or transmit CUI; or

Why Not the Beginning?

- Responses to comments help guide courts and others in interpreting the requirements, but they **are not** authoritative.
- Regulatory analyses are necessary for Congressional and judicial review, but also not authoritative.
- What matters is the language in the regulation.

Other Pending Rules

- CMMC will be implemented with a Title 48 CFR rule that will go into the DFARS. Comments closed on this rule on Tuesday.
  - This will amend DFARS 204.75 and 252.204-7021 (and potentially add DFARS 252.204-7022).
- Update to DFARS 252.204-7012:
  - Expect an update to CUI definition, addition of NIST 800-172 as a standard for certain types of CUI, and clarity on how it will work with CMMC.
- NIST 800-171 Assessment Methodology Title 48 CFR rule that is expected to go into the DFARS late 2024/early 2025.

The Basics: 3-Level Tiered Structure

Foundational

- When contractor has Federal Contract Information (FCI) only
- 15 Requirements appearing Federal Acquisition Regulation (FAR) clause 52.204-21

Advanced

- When contractor handles Control Unclassified Information (CUI)
- 110 Controls appearing in NIST SP 800-171 Revision 2

Expert

- When contractor handles Highly Sensitive CUI on a Critical DoD Program
- 110 NIST SP 800-171 Controls plus 24 Level 3 NIST SP 800-172 requirements

Level requirements will appear in solicitation and contract requirements

The Basics: Assessments

Foundational

- Annual self-assessment
- Results submitted into Supplier Performance Risk System (SPRS)

Advanced

- 5% require only annual self-assessment, results submitted into SPRS
- 95% require triennial C3PAO assessment, results submitted into eMASS

Expert

- Must complete a Level 2 CMMC Final Assessment
- 24 NIST SP 800-172 requirements assessed by DCMA DIBCAC
- Results submitted into eMASS

POA&Ms, Conditional and Final Certification

Certification is a Condition of Award

- No POA&Ms allowed, must meet all FAR 52.204-21 requirements

- Plans of Action and Milestones (POA&M) allowed to achieve Conditional Certification
- A minimum assessment score is required (80% including all mandatory requirements "MET" for Level 2)
- POA&Ms created for all "NOT MET" requirements must be remediated within 180 days
- Final Certification achieved when all POA&M items re-assessed as met

A new assessment required if architectural or boundary changes to scope

Annual Affirmation

All must file an annual affirmation from an “affirming official”

- Affirming official described as someone:

  “who is responsible for ensuring the [company’s] compliance with the CMMC Program requirements and has the authority to affirm the [company’s] continuing compliance with the specified security requirements for their respective organizations.”

- Affirmation filed after POA&A closeout
- This creates a False Claims Act risk for the affirming official and the organization

Roll Out Timeline

- The CMMC program is now here:
  - CMMC assessments by C3PAOs can start in December
  - Contractual requirements will begin when the DFARS rule is finalized and released. Expected March 2025.
- Once the DFARS rule is released, CMMC will roll out in four phases with Level 1 and Level 2 self-certifications beginning immediately on the effective date.

Roll Out Timeline (Assumes 3/1/25 Effective Date)

Stage	Est. Timing	Required	Optional
1	March 1, 2025	• L1 and L2 self-assessments required as a condition of award.	• L1 and L2 self-assessments required at option period for previously awarded contracts. • L2 C3PAO Conditional or Final Certification required as a condition of award.
2	March 1, 2026	• L2 C3PAO Conditional or Final Certification required as a condition of award.	• L3 DIBCAC Conditional or Final Certification required as a condition of award. • May delay L2 C3PAO Conditional or Final Certification requirement until option period.
3	March 1, 2027	• L2 C3PAO Conditional or Final Certification for all option periods of previously awarded contracts. • L3 DIBCAC Conditional or Final Certification as a condition of award.	• May delay L3 DIBCAC Conditional or Final Certification requirement until option period.
4	March 1, 2028	• All contracts and options will have applicable CMMC requirements.	• None

Roll Out Timeline

- Even so, the CMMC program may come sooner for some:
  - Prime contractors may require their supply chains to be compliant sooner.
  - DoD noted in the rulemaking that it may require CMMC compliance earlier that noted in the rule:

"...the Department may include CMMC Level 2 certification requirements on contracts awarded prior to the CMMC DFARS coverage becoming effective, but doing so will require bilateral contract modification after negotiations."

Assessment Scoping

- **Level 1** – if it processes, stores, or transmits FCI, it is in scope.
- **Level 2**
  - IoT, IIoT, GFE, OT are in scope but not assessed.
  - If it processes, stores, or transmits CUI, or secures the environment, it is in scope.
  - If it could process, store, or transmit CUI but a policy prohibits it, it may also be assessed if the policy is not reasonable.
- **Level 3** – if it could or does process, store, or transmit CUI, it is in scope.

Put More Simply

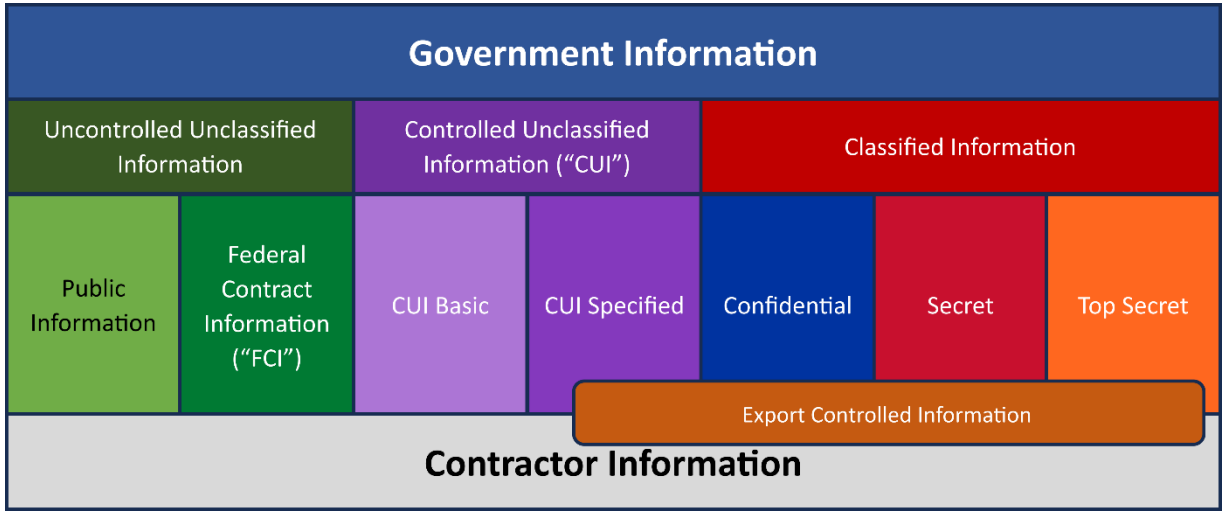
- If you want to exclude an asset (person, technology, location) from the assessment, do not give that asset the opportunity to store, process, or transmit FCI or CUI.
  - Isolate FCI/CUI in specific rooms/buildings
  - Isolate FCI/CUI to specific network segments and equipment
  - Isolate access to FCI/CUI to those with a lawful government purpose

Virtual Desktops

- One way to achieve the isolation is through virtual desktop interfaces (“VDI”)
  - Virtual PC runs in a secure cloud environment
  - All information stays up in the secure environment
  - Only keyboard, video, and mouse are streamed to the user’s device
- Can keep the user’s location and device out of scope
  - VDI must prohibit processing, storing, and transmitting of FCI/CUI beyond the keyboard/video/mouse
  - i.e., no printing, copying, screen captures, etc.

So…What are FCI and CUI?

- **FCI**
  - any non-public, unclassified government information
- **CUI**
  - non-public, unclassified information
  - created for or possessed on behalf of the federal government
  - a law, regulation, or government-wide policy says can be/needs to be safeguarded or dissemination can/should be limited



Who Decides When It's CUI?

- The government, not contractors.
  - You do NOT want to be reading and interpreting 400+ laws, regulations, and government-wide policies
- Government needs to tell the contractor:
  - "this thing I'm about to give you is CUI" (via CUI markings), or
  - "when you create information that looks and smells like **THIS**, it's CUI" (via a Security Classification Guide, memo, etc.)
- When you create information:
  - you review it to see if it meets the government's specifications
  - if so, add the CUI markings that they tell you to

Is a Contractor's Info CUI?

Not in that contractor's environment

HOWEVER, there are scenarios where that info becomes CUI when it is received by the government

When it comes back to you, it still isn't CUI

Is Security Protection Data ("SPD") CUI?

SPD is information about the contractor's security program

SPD inherently cannot be CUI in the contractor's environment

However, because of language in NIST SP 800-171, DoD requires that SPD be protected in contractor information systems as though it is CUI

External Service Providers

ESP = External Service Provider

CSP = Cloud Service Provider

MSP = Managed Service Provider

MSSP = Manages Security Service Provider

Value of an ESP

- They reduce burden by assuming full or partial responsibility for certain objectives
- You inherit those controls assumed by the ESP on your behalf
- They bring expertise and specialized resources, often on a shared services basis
- They bring best practices and proven solutions

ESP Requirements

When the ESP processes, stores or transmits	When utilizing an ESP that is:	
	A CSP	Not a CSP (MSP or MSSP)
CUI (with or without SPD)	The CSP must meet the requirements of the FedRAMP Moderate Baseline	Services provided by the ESP are in the OSA's assessment scope and will be assessed as part of the OSA's assessment
SPD (without CUI)	Services provided by the CSP are in the OSA's assessment scope and will be assessed as Security Protection Assets	Services provided by the ESP are in the OSA's assessment scope and will be assessed as Security Protection Assets
Neither CUI or SPD	Is not a CMMC ESP	Is not a CMMC ESP

ESPs – Caveat Emptor

32 CFR Part 170 Proposed Rule:

"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."

32 CFR Part 170 Final Rule

- No certification or qualification requirements for MSPs or MSSPs

What it means to you: Caveat Emptor

- Not all that claim to be capable are
- Be careful who you listen to
- Focus on trusted sources

Assessment

Examine	Interview	Test
• Review documentation • Traceability matrix is critical	• Ask questions of relevant personnel	• Screen share or in person • Demonstrate how/that something works

Assessments

Assessment Teams require 2 people

- Lead CMMC Certified Assessor
- CMMC Certified Assessor

Assessment must also be reviewed by a quality assurance person

- Observes the Assessment Team's conduct and management of the CMMC assessment process

Assessment Time and Cost

- JSVA assessments averaged approximately 200 hours of assessor time
- QA will require additional time
- Equivalent billing rates are typically $200-$300/hour
- Simple environments should assume $50,000-$60,000 for a CMMC Level 2 C3PAO assessment.

* Complex environments, site visits, disorganization, etc. will likely increase (and may significantly increase) costs.

Key L2 & L3 Assessment Concepts

- POA&Ms
  - Allowed, but must be remediated within 180 days
  - Minimum score: 88 for L2, 19 for L3
  - Only certain requirements can be POA&M'ed
- Operational Plans of Action
  - Allow for patches and other fixes that are necessary but push you out of compliance
- Enduring Exceptions
  - Special circumstances where compliance is not feasible (e.g., medical devices, OT)
- Affirmations
  - Annual statements of ongoing compliance made by a senior representative of the organization with appropriate authority

Key Assessment Tips

- Have your documentation in order
  - Compliance summary
  - Easy access to supporting documentation
- Minimize repetition
  - Single sources of truth reduce maintenance burdens
- Collect evidence
  - Ensure that you can prove that you not only have policies/procedures, but also are following them

Looking Ahead

- NIST 800-171 Revision 3 will supersede Revision 2 at some point in the future. Crystal ball: 3 years
- Don't think of CMMC in terms of compliance; Think of CMMC as letting us all sleep more soundly at night
- Don't hesitate to ask for help

QUESTIONS ?

Thank you for attending

stuart.itkin@neosystemscorp.com

eric.crusius@hklaw.com

jgoepel@futurefeed.co

NeoSystems® FutureFeed Holland & Knight