NDIA

CMMC Update:
Notice of Proposed Rulemaking
Impact

Current As Of: January 2024

Sponsored by:

COALFIRE® FEDERAL

TODAY'S SPEAKERS

Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO

Defense Cybersecurity Group

INFRAGARD National SME Cyberwarfare

Ryan Heidorn

Chief Technology Officer

C3 Integrated Solutions
Board Director, NDIA New England

Sponsored by:

COALFIRE FEDERAL

Secure Your Networks and Systems In Physical Space and Cyberspace

NDIA

- Secure your Networks. Now
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- DRAFT NIST 800-171Rev3 released 10 May 23
  - Final draft out for comment – Closes January 26th ~~12~~th
  - NDIA Corporate members can work with the Cybersecurity Division
- CMMC rule with OMB – Released 26 Dec 23

Sponsored by:

COALFIRE FEDERAL

Timeline Summary

NDIA

- 2 Processes running simultaneously – *and the goal posts appear to be moving*
- NIST 800-171 Rev3 Final – Comments ~~12 Jan~~ 26 Jan
  - New (later) estimate on when this will be final from NIST: Spring 2024 (April/May)
  - Some hints / indications of additional / new changes
- CMMC: Notice of Proposed Rulemaking (NoPRM)
  - Released 26Dec23
  - Linked explicitly to NIST 800-171 Rev 2
- Updates to DFARS 7019, 7020, 7021, and the base rule 252.204-7012
  - That process is starting now
  - Some indications DoD intends to attempt to align timing of DFARS updates and final CMMC rule release

Sponsored by:

COALFIRE FEDERAL

CMMC Implementation Timeline – NoPRM

- Notice published
  - 60-day comment period (26 February 2024)
- DoD must adjudicate comments
  - Average ~14 months (366 business days) ~14 Aug 2025
  - May go faster or slower
  - Some indications DoD is targeting March 2025
- DoD sends back to OMB/OIRA for 60-90-day review
- Publication of final rule
  - Q1 CY25? Q2 CY25? Later?

Impact on External Service Providers

- Finally… DoD acknowledges existence of MSPs / MSSPs
  - 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 External Service Providers -- Requirements

- An "ESP other than a CSP" must be certified at or above CMMC certification level of companies they support
  - If ESP <u>internal</u> (e.g., another business unit), separate certification not required, but requires SSP documentation of ESP's connection to in-scope environment
  - Requirements for CSPs fundamentally unchanged from DFARS 252.204-7012:
    - CSPs must be FedRAMP Authorized at the Moderate baseline or higher; or otherwise,
    - CSP may demonstrate "equivalency" through a System Security Plan and Customer Responsibility Matrix
    - <u>Note</u>: DoD CIO memo dated 12/21/23 sets a higher bar for "equivalency" than the CMMC proposed rule, removing mechanism for risk acceptance present in the FedRAMP authorization process and also requiring CSP to adhere to DFARS 252.204-7012 (c)-(g)
- <u>Key issue</u>: Proposed rule creates logical dependency on certifying MSPs
  - Company using "ESP other than a CSP" would need their MSP and/or MSSP to receive CMMC Final Certification before company can self-assess <u>or</u> be certified (see § 170.19(c)(1))

Sponsored by:

COALFIRE FEDERAL

Impact on External Service Providers

NDIA

- The definitions in the proposed rule miss the mark…
- Proposed rule does not define “ESPs other than CSPs”
- Proposed rule cites a CISA publication to define a CSP as:
  - *“[A]n external company that provides a platform, infrastructure, applications, and/or storage services for its clients.”*
- Definition overly broad and could be reasonably interpreted to include elements of an MSP or MSSP’s service delivery infrastructure
  - e.g., is an MSP that hosts a security tool “provid[ing]… applications… for its clients”?
  - Unclear who (an assessor? The OSC?) can determine whether an ESP is a CSP or “other than”

Sponsored by:

COALFIRE FEDERAL

Impact on External Service Providers

- Opportunity for clarification
- Differentiating CSPs from other types of ESPs indicates proposed rule likely intends to treat MSPs and MSSPs differently than CSPs
  - Proposed rule lists "MSP" and "MSSP" as acronyms in § 170.4(a) but does not otherwise define the terms
  - NDIA opinion: CMMC rule should use a narrower definition for "CSP" based on accepted definitions of cloud computing, for example:
    - DFARS 252.239-7010 "Cloud Computing Services"
    - NIST SP 800-145 "The NIST Definition of Cloud Computing"

Sponsored by:

COALFIRE FEDERAL

Impact on Cybersecurity Tools

NDIA

- **Security Protection Asset (SPA)**
  - Created first in CMMC 2.0 Scoping guide
  - C3PAO’s attempted interpretation to narrow negative impacts
  - DoD updates to Scoping Guide forcing broader interpretation
- **Security Protection Data: a new category of information**
  - Not clearly defined
  - Must meet full stack CMMC/FedRAMP security controls
- **Impact**
  - ESP definition + SPA + SPD + narrow path for FedRAMP equivalency = security tools with cloud component must be FedRAMP certified
  - Most modern commercial security tools have a cloud component
  - Likely to disqualify of many effective security tools from environments protecting DoD information

Sponsored by:

COALFIRE FEDERAL

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

- By The Numbers – ***CMMC Level 2***
  - 110 Controls with 320 Objectives with a total value of 313 Points used to determine your Self-Assessment score posted in SPRS
- **NOTE: 6 months after CMMC Rule implementation, only Self-Assessment score allowed is a perfect 110/110 / 320/320 / 313/313**

Sponsored by:

COALFIRE FEDERAL

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

- CIRRENTLY for Self-Assessment / SPRS reporting – PRESUMPTION is full implementation, so companies START with 313 Points which = 100%
- 88 points / 93% is currently "passing"
- When determining score, companies subtract
  - For every Control not met, deduct 5, 3, or 1 point
  - 0 Controls implemented = - 203 points
  - Retain 100 points, your score = - 103 points
  - Retain 203 points, your score = 0 points / 65% (203/313)
  - Retain 291 points, your score = + 88 points / 93% (291/313)

Sponsored by:

COALFIRE FEDERAL

Impact on Plan of Action and Milestones (POAMs)

- **New rule narrowly restricts utilization**
- **110 Controls / 320 Objectives / 313 Points**
- **2/3 / 215 Objectives are “No Fail”**
  - List in notes page of today’s backup slides
- **105 Objectives *initially* eligible for POAM**
- **POAMs must be cleared within 180 days**
- **Once POAMs cleared, a company must remain 110/110 / 320/320 / 313/313**

Sponsored by:

COALFIRE FEDERAL

Impact on Senior Company Official Affirmation

- Company “Senior Official” must affirm Self-assessment / Certification Assessment is accurate
- Company “Senior Official” also affirms 100% future compliance for all in-scope systems
- Unrealistic requirement?

Impact on Joint Surveillance Voluntary Assessments

- **JSVAs must have perfect score to convert**
- **C3PAOs advocating change to JSVA procedures**
  - Recent past: DCMA DIBCAC would not upload new scores even if contractor fixed problems and was re-assessed
  - Last week: Verbal confirmation that DIBCAC will allow re-assessment by C3PAO and will update score accordingly
- **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!!!!

Sponsored by: COALFIRE FEDERAL

Impact on Self Assessment for Level 1 & 2

NDIA

- **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

- **Certifications required for majority of CUI contract awards ~6 months after rule implementation**
  - August 2025 – November 2025?
  - 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)
  - Level 2 certification assessment requires a third-party assessment by a C3PAO

Sponsored by:
COALFIRE FEDERAL

Impact on Timeline for Certifications

NDIA

- **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)
- **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:

COALFIRE FEDERAL

Impact on Timeline for Certifications

- **CMMC Level 3 certification assessment**
  - Must pass CMMC Level 2 certification assessment with C3PAO first
  - Then eligible to schedule Level 3 certification assessment by DCMA
  - Slow roll-out anticipated (starting 18 months after rule final)

Notional introduction of contract requirements

About 1/3rd of contracts renew each year and can have DFARS 252.204-7021 added to them

	DFARS 252.204-7012 and SPRS score	Level 1 Self-Assessment	Level 2 Self-Assessment (for CUI contracts)	Level 2 Certification Assessment (for CUI contracts)	Level 3 Certification Assessment (for CUI contracts)
Now	all	none	none	none	none
(Phase 1) 48 CFR Rule final (DFARS 252.204-7021 updated)	all	all	95% contracts	5% contracts	none
(Phase 2) 6 months after Rule final	all	all	5-50% contracts	50%-95% contracts	1% contracts
(Phase 3) 12 months after Phase 2 starts	all	all	5% contracts	95% contracts	5% contracts

Sponsored by:

Secure Your Networks and Systems In Physical Space and Cyberspace

- Secure your Networks. Now
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- Communicate with your MSPs/MSSPs/ESPs
  - Be ready for implementation of the final rule

Sponsored by:

Questions?

Sponsored by:

Instant Failure