CMMC Update:
Rulemaking & Questions

Current As Of: December 2023

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

Scott Whitehouse

Director of Compliance Services

C3Integrated Solutions

Sponsored by:

COALFIRE FEDERAL

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
- 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 ~~12th~~
  - NDIA Corporate members can work with the Cybersecurity Division
- CMMC rule with OMB – Possible release Friday 22 Dec

Sponsored by:

Timeline Summary

- **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)**
  - **Expected any day – OMB review complete**
  - **Delay likely results from slow, bureaucratic process**

CMMC Implementation Timeline – Every indication NoPR

- Notice published (indications document more than 200 pages)
  - 2nd hand report: senior DoD official described as DoD's largest, most complex proposed rule
  - 60-day comment period (26 February 2024 if rule released Friday)
- DoD must adjudicate comments
  - Average ~14 months (366 business days) ~19 May 2025
  - May go faster or slower
- DoD sends back to OMB/OIRA for 60-90-day review
- Publication of final rule
  - Q1 CY25 (earliest possible in Vince's view)
  - Likely Q2 CY25 or later

When should companies be targeting assessments?

- CMMC Level 2 assessment: 18-24-month preparation process
- Not simply technical controls
- Must first understand CUI flow (transmit / handle / store) across your environment
- Second, must control with policy, procedural, and technical controls
- Third, must identify and gather evidence & artifacts needed to pass an assessment (non-trivial)
- Assessment timing depends on your readiness, and your risk of losing a contract because you lack certification
- Best Practice: Pick a date and conduct a Mock Assessment

Big Rock Challenges

- **Complexity and Cost: Compliance and Certification too difficult as currently defined**
- **Recommendations**
  - **DoD work with industry to define moderate, reasonable cybersecurity requirements**
  - **Discuss and understand compliance mechanism**
- **Impact: DoD cannot afford to lose companies below Cybersecurity Poverty Line**

What the timeline means for large prime contractors

REVIEW SUBCONTRACTOR DATABASE

CONFIRM CMMC READINESS WITH SUBS

REVIEW POAM WITH SUB

Sponsored by:

What the timeline means for small prime contractors

Identify your subcontractors

How do you interact with them?

Should you flow DFARS 7012 to your sub?

Ops processes for Primes

How will you store artifacts of subcontractor assessment?

How will subs be evaluated or onboarded in the future?

Who is responsible for communications when flowing DFARS to a sub?

Subcontractor Responsibilities

Know	Know your SPRS score and its defensibility
Review	Review your contracts with primes
Review	Review your contracts with the Government
Engage	Engage your executives – CMMC cannot be an IT-only initiative

Sponsored by:

What now? Immediate Actions

Perform a gap assessment

Talk with business stakeholders –

Existing contract renewal timeline

Planned contract application(s)

Prime/Sub relationships

Review your contracts!

Identify where your contracts stipulate DFARS 7012

This can be prime/subcontracts or with the Government

What now? Mid-Term (By 1 Jan 25)

Read	Read the rule
Execute on	Execute on POAM
Secure/verify	Secure/verify supply chain
Define	Define your timeline for assessment

Sponsored by:

Costs – Getting Compliant / Staying Compliant

- For small businesses, <200 employees
- Likely a 6-figure expense annually
  - Cost for 5-person company roughly = to 25-person company
- "Starting from zero" technical implementation:
  - $80 - $150K if outsourcing
  - Higher if in-sourcing
- Sustainment Budget: ~$3,500 - $4,000 / per user / per year
  - 5-person to 25-person company: $87,500 - $100,000
  - IT spend related to compliance, not total company IT spend
- Economies of scale: 50-100+ employees

Costs – Getting Compliant / Staying Compliant

- **Non-technical implementation:**
  - 1 year to prepare a reasonable estimate
  - ROM: ½ internal FTE = $30 - $52K *minimum*
  - Developing / Organizing 250-300 pages of documentation
- **Sustainment likely similar to maintain programs required under standards / regulations / contractual obligations**
  - Configuration Management, Vulnerability Management, Documentation updates, evidence gathering, annual Basic Self Assessment
- **"Getting Compliant" is not an end state**
  - NOT one and done
  - Requires ongoing security operations to stay compliant

Costs – 3rd Party Assessment Costs

- Limited data, and dependent on final CMMC rule and CAP
- Paying for assessment team's time
  - Costs will vary based on company size and preparation
  - Best Practices: Document scope; gather/organize objective evidence
- Well-prepared companies with great documentation may have shorter assessments and potentially lower costs
  - Much depends on assessor pricing, which could be Firm Fixed Price
- $30K likely low end
  - Could increase by $20K+ if not well-prepared
  - Triennial cost
- Cost of failure outweighs preparation costs for any company with significant DoD revenue
  - Companies with low DoD revenue may "opt out"

Assessments (Initial and Recurring)

- Will there be sufficient assessors?
- Role of Assessor vs role of MSP or Consultant
- Choosing an Assessor
- CMMC Assessment
  - Initial certification – preparation & cost
  - Recertification – Required every 3 years
    - Staying current with changing requirements
    - New Contracts can drive new cybersecurity requirements, especially if they include requirement to handle new types of information
- Potential for Partnership with 3PAO

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
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- Final DRAFT NIST 800-171Rev3 – comments due 12 Jan 24
- CMMC rule with OMB
- Communicate with your MSPs/MSSPs/ESPs
  - Be ready for implementation of the final rule

Sponsored by: COALFIRE FEDERAL

Rachel

Questions?

Sponsored by:

Guest Questions

- **Based on current draft, will CMMC be required for OTA contracts and CRADA or research contracts?**