NDIA
AT THE HEART OF THE MISSION

CMMC 2.0 Implementation

What We Know
What We Don't Know
What We Think

August 9th, 2022

Sponsored by:

Microsoft
MSUS Partner Award
Winner 2022
SUMMIT7
COMPLIANCE

TODAY'S SPEAKERS

Col (Ret) Rachel McCaffrey, USAF

Senior Vice President of Membership & Chapters, NDIA

Executive Director, Women In Defense

Ryan Heidorn

Co-Founder and Managing Director, Steel Root

ML Mackey

Chair, NDIA Small Business Division

CEO, Beacon Interactive Systems

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

Background

What We Know

2021 Re-Cap

- **January to October 2021**
  - CMMC 1.0
    - **5 certification levels**
    - Level 3: All NIST SP 800-171 110 security requirements **plus additional requirements (130 total controls)**
    - 3rd Party Assessments Required
    - Training and Certification of Assessors (limited number certified)
    - Planned Phased CMMC implementation: no more than 15 prime contracts in FY 21
  - CMMC 1.0 was run out of USD (A&S) Office of Industrial Policy

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

2021-2022 Re-Cap

- **Nov 2021 – July 2022**
  - Government announced CMMC 2.0
    - **3 certification levels**
    - Level 2: All NIST SP 800-171 110 security requirements; **no additional requirements**
    - Return to some self-assessments
    - Return to Plan of Action and Milestone process (POAM) – **time-bound** and **enforceable**
    - Addition of a selective, time-bound waiver process
  - CMMC 2.0 transferred to OSD CIO
  - Per McAleese and Associates:
    - **HASC 2023 NDAA**: "Would require USD(A&S) to provide Congressional briefing, "in which it articulates its role in DIB cybersecurity across the entirety of the organization, as well as the role played by the Office of the Assistant Secretary of Defense for Industrial Base Policy".(p. 352)

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

Defining Controlled Unclassified Information (CUI)?

- **Federal Contract Information (FCI)**[1] – CMMC 2.0 Level 1
  - "FCI is information not intended for public release. FCI is provided by or generated for the Federal Government under a contract to develop or deliver a product or service."
- **Controlled Unclassified Information (CUI)**[1] – CMMC 2.0 Levels 2-3
  - "CUI and FCI share important similarities and a particularly important distinction. Both CUI and FCI include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is "not intended for public release," CUI is information that requires safeguarding and may also be subject to dissemination controls. In short: **All CUI in possession of a Government contractor is FCI, but not all FCI is CUI."**

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

CMMC 2.0 Overview[2]

- **Reduced from 5 to 3 Levels:**
  - Level 1 (Foundational): “for companies with FCI only; information requires protection but is not critical to national security”
  - **Level 2 (Advanced): “for companies with CUI”**
  - Level 3 (Expert): “for the highest priority programs with CUI”

- ***However, what is CUI?***
  - Surprisingly difficult to identify on covered contractor systems
  - All indicators point to the Government and prime contractors erring on the side of over-designation

CMMC 2.0 Key Highlights[2]

- CMMC 2.0 removes the unique practices that CMMC 1.0 introduced, including the maturity processes. *We are back to the NIST 800 series requirements.*
- Self-assessments reinstated for **Level 1** and ***some of Level 2****
- Allows for a very selective, time-bound waiver process
- Allows for limited POA&Ms: time-bound and enforceable
- The Cyber AB owns the CMMC Assessment Process (CAP); a draft of the CAP was recently released for public comment
- Voluntary assessments under the "Joint Surveillance" program commence August 2022

Sponsored by:

CMMC 2.0 Requirements

Government will require all companies handling/holding CUI to, <u>at minimum</u>, self-assess full compliance with NIST SP 800-171 annually

- Level 2
  - Requires compliance with all 110 NIST SP 800-171 security requirements
  - Non-prioritized acquisitions: **annual** self-assessment
  - Prioritized acquisitions: annual self-assessment AND **triennial** C3PAO assessments
- Level 3
  - Minimal information currently available
  - Expected to require compliance with all 110 NIST SP 800-171 requirements <u>**AND**</u> <u>a subset of NIST SP 800-172</u>
  - Expected to require annual self assessment and triennial government-led assessments

Sponsored by:

Microsoft MSUS Partner Award Winner 2022

SUMMIT7 COMPLIANCE

Rulemaking[2]

- **Do not expect rulemaking to change the underlying requirement to implement NIST SP 800-171**
- The DoD has already directed contracting officers to include CMMC as prescribed in 48 Code of Federal Regulations (CFR) Subpart 204.75. The required contract clause is DFARS 252.204-7021.
- However, nothing currently directs the DoD to do this (see 86 FR 64100), so…
- We await rulemaking in 32 CFR as the Government needs to direct itself to have CMMC in the first place
- The relevant parts of 48 CFR shall then be enforced upon DoD contract officers or may be edited or have new rules introduced as part of the rulemaking process
- During the NDIA New England Chapter's 6th annual cyber event, Stacy Bostjanick stated the Pentagon plans to publish the CMMC interim rule by May 2023.[3]
  - Late in the 9-to-24-month timeline offered in November 2021
  - Bostjanick also urged companies to "move forward and get that CMMC certification today"

Sponsored by:

NDIA Feedback Process

- NDIA plans to respond during the mandatory 60-day public comment period once the government releases the interim rule
  - *Send comments on the interim rule to: Jacob Winn, JWinn@NDIA.org*

What should you send?

- Company-specific information
  - What your product or service?
  - Who is your typical customer?
  - What is the challenge you are experiencing?
  - Why is it especially problematic for small business?
  - What is the biggest pain point?
- Any recommendations for mitigating the problem?
  - If you do not have a specific suggestion, please prioritize where mitigating action should initially focus

Sponsored by: Summit7 Compliance — Microsoft MSUS Partner Award Winner 2022

Unknowns

What We Don’t Know

CMMC 2.0 Baseline Unknowns

- Government has not yet indicated the criteria for “highest priority” programs / Level 3
- Government has not yet identified the subset of the NIST SP 800-17**<u>2</u>** requirements with which companies must comply to achieve Level 3 certification
- At Level 2, which companies will need to self assess and which will need a third-party assessment?
- *<u>Government has not yet indicated the number of contracts it expects will be impacted during the 4th quarter of FY23</u>*

CMMC 2.0 Technical Unknowns

- Reciprocity with other cybersecurity standards
- NIST SP 800-171 Rev. 3 and future updates
  - NFO requirements (see Appendix E)
- Practice inheritance and involvement of external service providers
- Cloud-native environments and zero trust architecture

Sponsored by:

CMMC 2.0 Policy Unknowns

CMMC Rulemaking remains opaque…

- Financial
  - Details of DoD's cost analysis for each level of CMMC 2.0
  - How companies will report and recoup CMMC business costs
- Operational
  - How program offices will be instructed to define, classify and identify CUI
  - Whether subcontractors will require the same CMMC Level certification as a prime contractor when a program's CUI or a subset of that CUI is passed
- Regulatory
  - Will the government implement any reciprocity with other cybersecurity standards, US or Allied
- Will Congress will direct further changes during its concurrent review during the 60-day public comment period

Sponsored by:

NDIA Feedback Process

What should you send?

- Company-specific information
  - What your product or service?
  - Who is your typical customer?
  - What is the challenge you are experiencing?
  - Why is it especially problematic for small business?
  - What is the biggest pain point?
- Any recommendations for mitigating the problem?
  - If you do not have a specific suggestion, please prioritize where mitigating action should initially focus

Sponsored by:

NDIA Recommendations

What We Think

Sponsored by:

Microsoft MSUS Partner Award Winner 2022

SUMMIT7

COMPLIANCE

What We Think

- **Government should mark CUI and define CUI requirements for each contract**
  - Standardization across contracts/programs
- **Government should identify threats and disseminate threat information and recommendations at the speed of relevance**

Sponsored by:

Secure your networks and computers immediately!

- **NDIA believes DIB companies must meet cybersecurity standards**
  - Effective Cyber hygiene and security is simply good business
  - Protect your IP
  - Make yourself a “hard target”
  - Turn on notification preferences for NDIA Connect CMMC Community
    - Set email communication preferences to “Yes” for cybersecurity
- **Where should companies be today?**
  - Remember that CMMC is not a new requirement
    - NIST SP 800-171 first published in June 2015
    - DFARS 252.204-7012 in enforcement since December 2017
    - DoD announced CMMC in 2019
    - In 2022, all DIB companies should have implemented NIST SP 800-171 (and be ready for CMMC Level 2)

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

If your company cannot meet Level 2 now

Bottom Line:

- Get compliant
- Accurately and honestly self assess (using NIST SP 800-171A)
- Be ready for third-party assessment once rules are finalized

- **Recommendations for businesses, especially smalls**
  - Start with a holistic design for full compliance rather than piecemealing security requirements. Potential for greenfield enclaves to help.
  - Beware snake oil; the CMMC service provider marketplace is not being policed. The Cyber AB's RPO program does not mean the providers are qualified.

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

NDIA is less enthusiastic about…

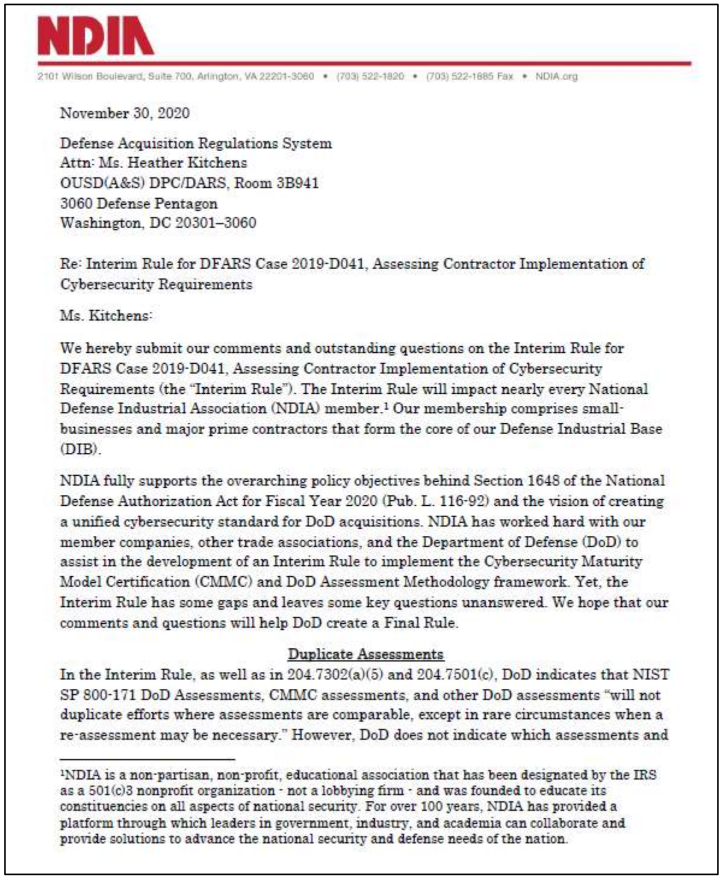
- **…Getting assessed now**
  - Too many unknowns, the CAP is not finalized
  - DoD wants to include CMMC requirements on contracts in 4th quarter FY23
- **…Cost with limited number of assessors**
  - Unfair to ask companies to pay for assessment without fully understanding all requirements
- **Anticipate Government will need to provide time for 3rd party assessments once rules finalized**
- **However, Government expected to outline early adopter benefits soon**

Sponsored by: Microsoft MSUS Partner Award Winner 2022 SUMMIT7 COMPLIANCE

What is NDIA Doing?

Sponsored by:

NDIA's CMMC 1.0 Comment: Themes and Issues



NDIA

2101 Wilson Boulevard, Suite 700, Arlington, VA 22201-3060 • (703) 522-1820 • (703) 522-1885 Fax • NDIA.org

November 30, 2020

Defense Acquisition Regulations System
Attn: Ms. Heather Kitchens
OUSD(A&S) DPC/DARS, Room 3B941
3060 Defense Pentagon
Washington, DC 20301–3060

Re: Interim Rule for DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements

Ms. Kitchens:

We hereby submit our comments and outstanding questions on the Interim Rule for DFARS Case 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements (the "Interim Rule"). The Interim Rule will impact nearly every National Defense Industrial Association (NDIA) member.[1] Our membership comprises small-businesses and major prime contractors that form the core of our Defense Industrial Base (DIB).

NDIA fully supports the overarching policy objectives behind Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92) and the vision of creating a unified cybersecurity standard for DoD acquisitions. NDIA has worked hard with our member companies, other trade associations, and the Department of Defense (DoD) to assist in the development of an Interim Rule to implement the Cybersecurity Maturity Model Certification (CMMC) and DoD Assessment Methodology framework. Yet, the Interim Rule has some gaps and leaves some key questions unanswered. We hope that our comments and questions will help DoD create a Final Rule.

Duplicate Assessments

In the Interim Rule, as well as in 204.7302(a)(5) and 204.7501(c), DoD indicates that NIST SP 800-171 DoD Assessments, CMMC assessments, and other DoD assessments "will not duplicate efforts where assessments are comparable, except in rare circumstances when a re-assessment may be necessary." However, DoD does not indicate which assessments and

[1] NDIA is a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)3 nonprofit organization - not a lobbying firm - and was founded to educate its constituencies on all aspects of national security. For over 100 years, NDIA has provided a platform through which leaders in government, industry, and academia can collaborate and provide solutions to advance the national security and defense needs of the nation.

Lack of ethics rules for the CMMC-AB to deter conflicts of interest

Lack of compatibility with a cloud-first world and the need for reciprocity between FedRAMP & CMMC

Pre-award cost allowability and recommendations for DoD to seek an appropriation to cover pre-award CMMC compliance costs

Concern about the use of scores as a competitive differentiator by contracting officers

Sponsored by:

Microsoft MSUS Partner Award Winner 2022

SUMMIT7 COMPLIANCE

NDIA’s CMMC 1.0 Comment: Themes and Issues

Issue identified in NDIA’S CMMC 1.0 comment	Issues mentioned in CMMC 2.0 Strategic Intent
Duplicate assessments	Yes
POAMs	Yes
Phase-in period	Yes
Ethics	Yes
Micro-purchase threshold	No
COTS	No
CUI	No
Cost Allowability	No
Dispute resolution	No
FedRamp reciprocity	No

NDIA’s CMMC 1.0 Comment: Themes and Issues

NDIA
AT THE HEART
OF THE MISSION

Issue identified in NDIA’S CMMC 1.0 comment	Issues mentioned in CMMC 2.0 Strategic Intent
Operational Technologies	No
Trade secret protection	No
Definition of key terms	No
Non-U.S. Contractors	No
Oversight of C3PAO fees	No
Audit Standards	No

Sponsored by:

Microsoft
MSUS Partner Award
Winner 2022
SUMMIT7
COMPLIANCE

NDIA's CMMC 1.0 Comment: Themes and Issues

Issue identified in NDIA'S CMMC 1.0 comment	Issues mentioned in CMMC 2.0 Strategic Intent
Operational Technologies	No
Trade secret protection	No
Definition of key terms	No
Non-U.S. Contractors	No
Oversight of C3PAO fees	No
Audit Standards	No

Issues mentioned

$\frac{\sim 4}{16}$

NDIA's CMMC Activities

- Tracking and reporting on any/all regulatory developments
- Established and maintains CMMC Partner Comparison tool to help NDIA members find low-cost solutions for self-assessment
- Continue to engage with CMMC Program Office and other government organizations
- Aggregate and anonymize NDIA member input/concerns on interim rule—**will solicit corporate member input!**
- Conduct future webinars to discuss new developments
- Educate policymakers about the impact and advocate for rational implementation

Sponsored by:

Tracking Similar Programs Abroad

- NDIA also expects CMMC-like programs to emerge in friend/allies/partner nations
- Countries such as the United Kingdom and Canada have begun to pursue cybersecurity requirements for defense companies
- Lagging the US in terms of development and implementation
- Strong hope they borrow from final, approved CMMC requirements
- Expect CMMC compliance will ensure foreign compliance – however too soon to tell
- NDIA will continue to monitor foreign regulations regarding foreign CUI-equivalents to continue to provide education and guidance

NDIA Business Institute: Upcoming Courses

NDIA
AT THE HEART OF THE MISSION

Carnegie Mellon University
Software Engineering Institute

Managing for Supply Chain Resilience

September 29-30 | Virtual

DAU

Defense Systems Acquisition Management

September 12 – 16 | Arlington, VA

MBDi

Mastering Business Development

September 27 – 28 | Arlington, VA

EGGLER
INSTITUTE OF TECHNOLOGY

Eggler Institute of Technology

On Demand

Contact Sandra Hubbard for more info: shubbard@NDIA.ORG

Microsoft
MSUS Partner Award
Winner 2022
SUMMIT7
COMPLIANCE

Questions?

Col (Ret) Rachel McCaffrey, USAF
rmccaffrey@ndia.org

Ryan Heidorn

ryan@steelroot.us
LinkedIn: /in/rheidorn

ML Mackey

ml.mackey@beaconinteractive.com

Thank you for attending!

Please email Jacob Winn, JWinn@NDIA.org, with any further questions or comments on today's webinar.

Also reach out to Jacob to get involved with NDIA's Small Business Division. Their next meeting will be on August 16th.

Sponsored by:

Sources

- 1: CUI FAQs, DCSA: https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/21-10-13%20CUI%20FAQ%20FINAL.pdf
- 2: See DoD's public Overview Briefing on CMMC 2.0 from December 3, 2021, for the source of this information
- 3: *Inside Cybersecurity*, "Pentagon plans to publish CMMC 'interim rule' by May 2023," by Sara Friedman: https://insidecybersecurity.com/share/13400