CMMC – Its Coming: The Department of Defense Interim Rule

November 12, 2020

Paul Debolt

Partner, Venable LLP | 202.344.8384 | PADebolt@Venable.com

Dismas (Diz) Locaria

Partner, Venable LLP | 202.344.8013 | DLocaria@Venable.com

Stacy Bostjanick

OUSD A&S, Director of Cybersecurity Maturity Model Certification Policy | stacy.s.bostjanick.civ@mail.mil

Ross Nodurft

Senior Director of Cybersecurity Services, Venable LLP | 202.344.4403 | RBNodurft@Venable.com

Kendall Lucas

Assistant General Counsel, Deloitte | 571.882.7434 | kelucas@deloitte.com

VENABLE LLP

ACC Association of Corporate Counsel NATIONAL CAPITAL REGION

Agenda

- Securing the DOD Supply Chain
- Cybersecurity Maturity Model Certification
  - Overview
  - Levels 1-5
- CMMC Interim Rule
  - Overview
  - Requirements
  - Implications and Challenges

Securing the DoD Supply Chain

Cybersecurity Maturity Model Certification

Ms. Katie Arrington
Chief Information Security Officer for Acquisition

Interim Rule

NIST SP 800-171 DoD Assessment Methodology
DFARS Clause 252.204-7020

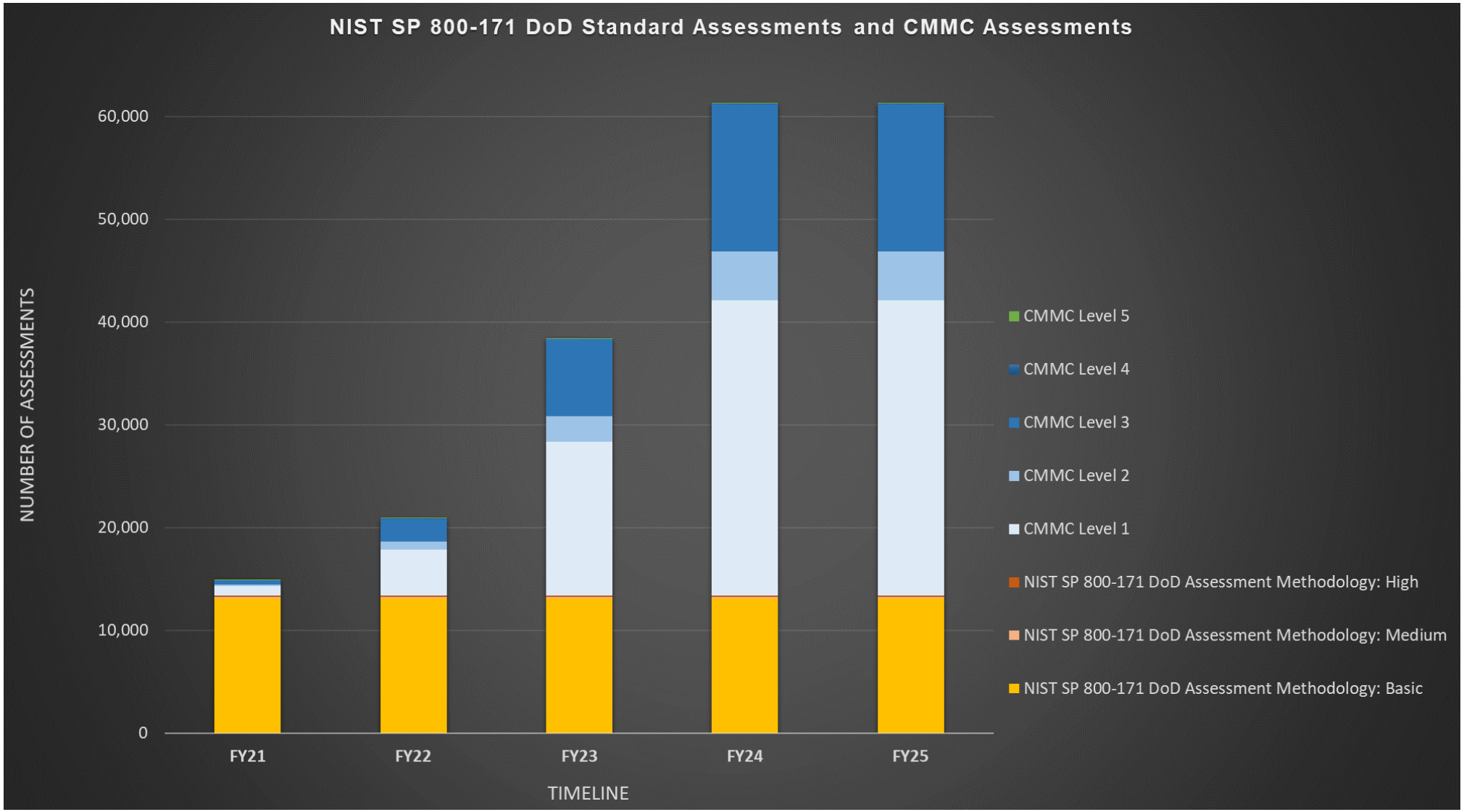
- Companies subject to DFARS clause 252.204-7012 must have a current NIST SP 800-171 assessment (Basic, Medium, or High) to be considered for award
- **Basic**: Self-assessment identifies how many NIST SP 800-171 security requirements a contractor has implemented and not implemented and results in a score; requirement to have Basic self-assessment to be phased in over three years
- **Medium/High**: DoD may perform at its discretion post-award, based on criticality of program, nature of information; finite number of assessments each year
- Results will be documented in DoD Supplier Performance Risk System (SPRS); prior to award, contractors will verify that offerors have current assessment in place

CMMC
DFARS Clause 252.204-7021

- OUSD(A&S) must approve the use of clause for new acquisitions until October 2025; over 220K contractors expected to achieve CMMC certification during that time
- After October 2025, required for all DoD contracts above micro-purchase threshold, excluding COTS
- For solicitations with the DFARS clause on CMMC, contractor must be certified at required CMMC level at time of award and must maintain certificate for duration of contract
- New clause must be flowed down; primes must ensure subs are certified at required CMMC level prior to awarding subcontract

NIST SP 800-171 DoD and CMMC assessments will not duplicate efforts or any other DoD assessments except for rare circumstances

NIST SP 800-171 DoD Standard Assessments & CMMC Assessments



Supplier Performance Risk System (SPRS)

Process for Offerors/Contractors to submit Basic NIST SP 800-171 DoD Assessment scores for posting in SPRS

- The interim rule (DFARS clause **252.204-7019** and **252.204-7020**) currently states that the Offeror/Contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to **webptsmh@navy.mil (email address)** for posting to the Supplier Performance Risk System (SPRS)

- SPRS now has increased functionality for Offerors/Contractors to enter scores directly
  - The NIST SP 800-171 DoD Assessment Methodology, posted at https://www.acq.osd.mil/dpap/pdi/cyber/index.html, states that "A contractor may post the results of their Basic Assessments… in SPRS (via the Procurement Integrated Enterprise Environment (PIEE))."
  - A link to a Quick Entry Guide for entering assessment scores can be found at the SPRS homepage

DoD Assessment Methodology – Basic Assessment Requirement

- **To comply with NIST SP 800–171 a company must:**
  - Implement 110 security requirements on their covered contractor information systems; or
  - Document in a ‘‘system security plan’’ and ‘‘plans of action’’ those requirements that are not yet implemented and when the requirements will be implemented
- **Basic Assessment is a self-assessment done by the contractor using a specific scoring methodology**
  - Tells the DoD how many security requirements have not yet been implemented
  - Is valid for three years
- **All offerors that are required to implement NIST SP 800–171 per DFARS clause 252.204–7012, will be required to complete a Basic Assessment and upload the resulting score into SPRS**
- **To submit the Basic Assessment, contractors must complete 6 fields:**
  - System security plan name (if more than one system is involved)
  - CAGE code associated with the plan
  - Brief description of the plan architecture
  - Date of the assessment
  - Total score
  - Date a score of 110 will be achieved

CMMC Pilot Programs

- **USD(A&S) memo, dated August 4, 2020, *Implementing the Cybersecurity Maturity Model Certification within the Department of Defense***
  - Provides guidance to Service and Component Acquisition Executives
  - Limits the number of solicitations specifying a CMMC requirement for FY 2021 to no more than 15 prime contracts, which will serve as CMMC pilot programs
  - Directs all PMs and Contracting Officers to avoid including CMMC as a requirement in RFIs and RFPs unless coordinated through OUSD(A&S)
- **Each Service Acquisition Executive nominate three acquisitions with an expected contract award date in FY 2021**
- **Each Component Acquisition Executive nominate a single acquisition with an expected contract award date in FY 2021**
- **Each nomination should be for a mid-sized program that require the contractor to process or store basic CUI. This requirement aligns to CMMC level three.**
- **Do not nominate acquisitions that are solely for provision of COTS products, or for operational technology systems supporting industrial or manufacturing operations**

Projected CMMC Roll-Out

- **OUSD(A&S) is working with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out**

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

- **All new DoD contracts will contain the CMMC requirement starting in FY26**
- **Assumes for every unique prime contractor, there are ~ 100 unique subcontractors**

CMMC Rollout - Breakout

- **Total number of unique DoD contractors and subcontractors is 220,966**
  - The total number of unique DoD contractors and subcontractors with a new CMMC certification requirement achieves a steady state of 47,905 by Year 4
  - Completed CMMC assessments on all total 220, 966 unique DoD contractors and subcontractors is achieved in Year 7; as a result, the number of unique DoD contractors and subcontractors that require a new CMMC certification is only 43,251 for Year 7

- **Phased rollout assumes the following percentages of DoD contractors and subcontractors require a CMMC certificate at each level:**
  - Level 1: approximately 60%
  - Level 2: approximately 10%
  - Level 3: approximately 30%
  - Level 4: approximately 0.06%
  - Level 5: approximately 0.06%

Projected CMMC Roll-Out

- **OUSD(A&S) will work with Services and Agencies to identify candidate programs that will have the CMMC requirement during FY21-FY25 phased roll-out**

CMMC Level	Total Number of Unique DoD Contractors and Subcontractors*						
	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
1	899	4,490	14,981	28,714	28,709	28,709	25,919
2	149	749	2,497	4,786	4,785	4,785	4,320
3	452	2,245	7,490	14,357	14,355	14,355	12,960
4	0	8	16	24	28	28	26
5	0	8	16	24	28	28	26
Totals	1,500	7,500	25,000	47,905	47,905	47,905	43,251

IAW Public Released Regulatory Impact Analysis which are part of DFARS Case 2019-D041

- **Assumes for every unique prime contractor, there are ~ 100 unique subcontractors**
- **Assumes 220,966 unique DoD contractors and subcontractors**
- **All new DoD contracts will contain the CMMC requirement starting in Year 6**

CMMC Rollout by Entity Size

Total Number of CMMC Initial Certifications Per Year (Years 1 – 7)								
Year	Size	Level 1	Level 2	Level 3	Level 4	Level 5	Total by Size	Total All
1	Small	665	110	335	0	0	1,110	1,500
	Other than Small	234	39	117	0	0	390	
2	Small	3,323	555	1,661	2	2	5,543	7,500
	Other than Small	1,167	194	584	6	6	1,957	
3	Small	11,086	1,848	5,543	4	4	18,485	25,000
	Other than Small	3,895	649	1,947	12	12	6,515	
4	Small	21,248	3,542	10,624	6	6	35,426	47,905
	Other than Small	7,466	1,244	3,733	18	18	12,479	
5	Small	21,245	3,541	10,623	7	7	35,423	47,905
	Other than Small	7,464	1,244	3,732	21	21	12,482	
6	Small	21,245	3,541	10,623	7	7	35,423	47,905
	Other than Small	7,464	1,244	3,732	21	21	12,482	
7	Small	19,180	3,197	9,590	7	7	31,981	43,251
	Other than Small	6,739	1,123	3,370	19	19	11,270	
1-7	Small	97,992	16,334	48,999	33	33	163,391	220,966
	Other than Small	34,429	5,737	17,215	97	97	57,575	
1-7	All	134,421	22,017	33,214	130	130	220,966	220,966

IAW Public Released Regulatory Impact Analysis which are part of DFARS Case 2019-D041

Assumes 74% of the unique DoD contractors are small entities

Cybersecurity Maturity Model Certification

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

CMMC Overview

- CMMC defines five levels of certification, based on focus, maturity processes, and cybersecurity practices. To achieve certification, a contractor must demonstrate both the process and practice maturity identified at the requisite level. The framework categorizes the practices into 17 capability domains. Each capability contains one or more practices and processes, which are assigned to one of the five levels of CMMC certification. This provides a helpful benchmark that organizations can utilize to evaluate their current level of maturity while creating achievable goals for improvement

- CMMC Levels follow the data or, in this case, Controlled Unclassified Information (CUI). If an organization is believed to never receive or generate CUI, the DoD will likely require Level 1 or 2 certification. If the supplier is expected to receive CUI, the DoD will likely require the contractor to achieve at least a Level 3 certification

CMMC Overview *cont'd*

- CMMC consists of 17 domains, which are largely based on the 14 families of security requirements from NIST SP 800-171

CMMC Levels

CMMC Level	Description
Level 1	Comprise 17 requirements, which consist of the safeguarding requirements specified in FAR 52.204-21, 15 of which correspond to 17 requirements from NIST SP 800-171. CMMC Level 1 covers approx. 15% of the NIST 800-171 controls Requires organizations to perform only specified practices and does not require documentation. Organizations will still need to demonstrate performance of these requirements to a CMMC third-party assessor
Level 2	72 requirements make up CMMC Level 2, which includes all requirements from Level 1. 48 new requirements come directly from NIST SP 800-171. CMMC Level 2 covers approx. 60% of NIST 800-171 controls. This level is intended to be a stepping stone for organizations between Levels 1 and 3 Requires an organization to establish and implement a policy that includes each of the 17 CMMC domains

CMMC Levels *cont'd*

CMMC Level	Description
Level 3	130 requirements. Includes all 110 requirements from NIST SP 800-171 and an additional 20 requirements from other sources. The DoD has stated that CMMC Levels 1-3 will be the target for many DoD contracts Requires maintaining a resource plan for each of the 17 domains
Level 4	156 requirements. Includes all 110 requirements from NIST SP 800-171, and an additional 46 requirements from other sources Requires review and measurement of domain policies and procedures to validate effectiveness of those activities
Level 5	171 requirements. Includes all 110 requirements from NIST SP 800-171 and an additional 61 requirements from other sources. The DoD has stated that CMMC Level 4-5 is designed to target DoD critical programs and will be reserved for a smaller subset of DoD contracts Requires a standardized and optimized approach for documentation across all organizational entities

CMMC Interim Rule

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

Overview of Recent Interim Rule

- September 29, 2020 – DoD issued an **interim rule** amending the DFARS to implement the DoD's Cybersecurity Maturity Model Certification Program
- Rule established the DoD Assessment Methodology, which will "assess contractor implementation of cybersecurity requirements and enhance the protection of classified information"
- Interim rule becomes effective on November 30, 2020
- DoD has requested public comment on the interim rule on or before November 30, 2020

What Does the Interim Rule Require?

- Assessment methodology augments the requirement in DFARS clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting that requires contractors to apply the cybersecurity of requirements of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 to covered contractor systems that are not part of an IT service or system operated on behalf of the USG
- Specifically, the assessment methodology:
  - Determines how well a contractor has implemented the NIST SP 800-171 controls
  - Includes three assessment levels (Basic, Medium and High) that reflect the depth of the assessment and confidence in the resulting score

What Does the Interim Rule Require?

- Basic assessment is a self-assessment by the contractor
- Medium and high assessments are conducted by the DoD
  - DoD assessments require contractors to provide the DoD with access to facilities, systems, and personnel when necessary for the DoD to conduct or renew a higher-level assessment
- DoD may perform medium- or high-level assessments based on the criticality of the program or sensitivity of the information handled by the contractor
- For medium- and high-level assessments DoD will provide summary-level scores to contractors as well as an opportunity for rebuttal and adjudication prior to posting the scores

What Does the Interim Rule Require?

- Results of assessment will be posted in the Supplier Performance Risk System (SPRS)
- DoD contracting officers will use SPRS to verify an offeror's compliance with the requirements prior to contract award
- Assessments are valid for 3 years
- Where applicable, prime contractors must ensure that their subcontractors have a current assessment in SPRS prior to awarding a subcontract

What Are the Challenges to the Implementation of the Interim Rule?

- Approximately 300,000 companies have some level of access to controlled unclassified information (CUI) and conduct business with the USG as either a prime or a subcontractor
  - Will the USG have the resources to conduct the required assessment?
  - Will the USG have to impose new limits on access to CUI?
  - Will the USG have to increase a higher standard for what constitutes “more sensitive CUI”?

Ongoing Questions

- Reciprocity with other compliance regimes: Currently, the IFR does not clearly delineate the process for providing reciprocity with other security compliance regimes and frameworks, e.g., FedRAMP.
- Small and medium business expenses:
  - Some effort to address the cost challenges associated with meeting the requirements of CMMC
  - Still unknown what it will truly cost:
    - To achieve the various CMMC levels and what the return might be on contracts requiring a more heightened level of security
    - To receive and pass an assessment
    - To challenge or refute an assessment
    - To do business under the CMMC regime

Questions?

VENABLE LLP

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION