UNDERSTANDING AND PREPARING FOR THE CMMC

AND THE NIST SP 800-171 INTERIM RULE

WALL EINHORN & CHERNITZER
CPAs & ADVISORS

Keiter
Your Opportunity Advisors

Experience | Knowledge | Relationships | Insight

WEC Bios

- Eileen Gwaltney, CPA
- Director of Government Contracting Services

egwaltney@wec.cpa | 757.664.3467

Eileen joined WEC in 2004 and has over 18 years of experience. She s the leader of the firm's Government Contracting Client Service Team. She has worked with contractors of various size across a number of industry segments, so she understands the complexities of the government contracting industry and is able to provide innovative, customized assurance and advisory solutions across a wide range of service areas.

- Karl Belka, CPA
- Advisory Services Manager

kbelka@wec.cpa | 757.533.4141

Karl joined WEC in 2019 having gained over 12 years of experience in public accounting and in the private sector with a government contractor. He specializes in DCAA compliance, preparation of incurred cost submissions, indirect rate development, collateral field exams and asset-backed lending (ABL). He also helps clients prepare for and navigate mergers and acquisitions through due diligence support services.

About Us

- Keiter is a Richmond-based CPA firm. Our Risk Advisory Services team delivers independent cybersecurity audit, consulting, and compliance services.
- We are a CMMC Registered Provider Organization

Scott McAuliffe, CPA, CISA, RP
Partner, Risk Advisory Services
smcauliffe@keitercpa.com
(804) 273-6247

Chris Moschella, CPA, CISA
Senior Manager, Risk Advisory Services
cmoschella@keitercpa.com
(804) 419-2902

Agenda

- Background
- Timeline & Key DFARS Clauses
- Enforcement
- Current Requirements (NIST 800-171)
- Assessment Methods
- CMMC Guidance
- Readiness Process

Background

- DoD identified the need to better protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) – both of which are UNCLASSIFIED
  - **FCI** - information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.
  - **CUI** - is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls
- Key Distinction: FCI is merely not intended for public release, CUI requires safeguarding
- Different security requirements depending on type of data – CUI requires more stringent safeguarding controls

Background

- CUI
  - 20 Categories
  - Defense Category
    - Controlled Technical Information
    - DoD Critical Infrastructure Security Information
    - Naval Nuclear Propulsion
    - Unclassified Controlled Nuclear Information – Defense
  - Controlled Technical Information - means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
  - Critical Infrastructure Security Information - information that, if disclosed, would reveal vulnerabilities in the DoD critical infrastructure and, if exploited, would likely result in the significant disruption, destruction, or damage of or to DoD operations, property, or facilities
  - Reference: https://www.archives.gov/cui
  - Training: https://securityhub.usalearning.gov/index.html

Background

- Four DFARS clauses implement two requirements
  - NIST SP 800-171 Compliance required by:
    - DFARS 252.204-7012, 7019, & 7020
  - CMMC Compliance required by:
    - DFARS 252.204-7021
- NIST SP 800-171 and the CMMC are cybersecurity frameworks for DoD Contractors
- Requirements for all DoD contractors:
  - Exception for contractors that provide commercial-off-the-shelf products or services.

Background

- Cybersecurity Maturity Model Certification (CMMC)
  - Based almost entirely on NIST SP 800-171
- NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*

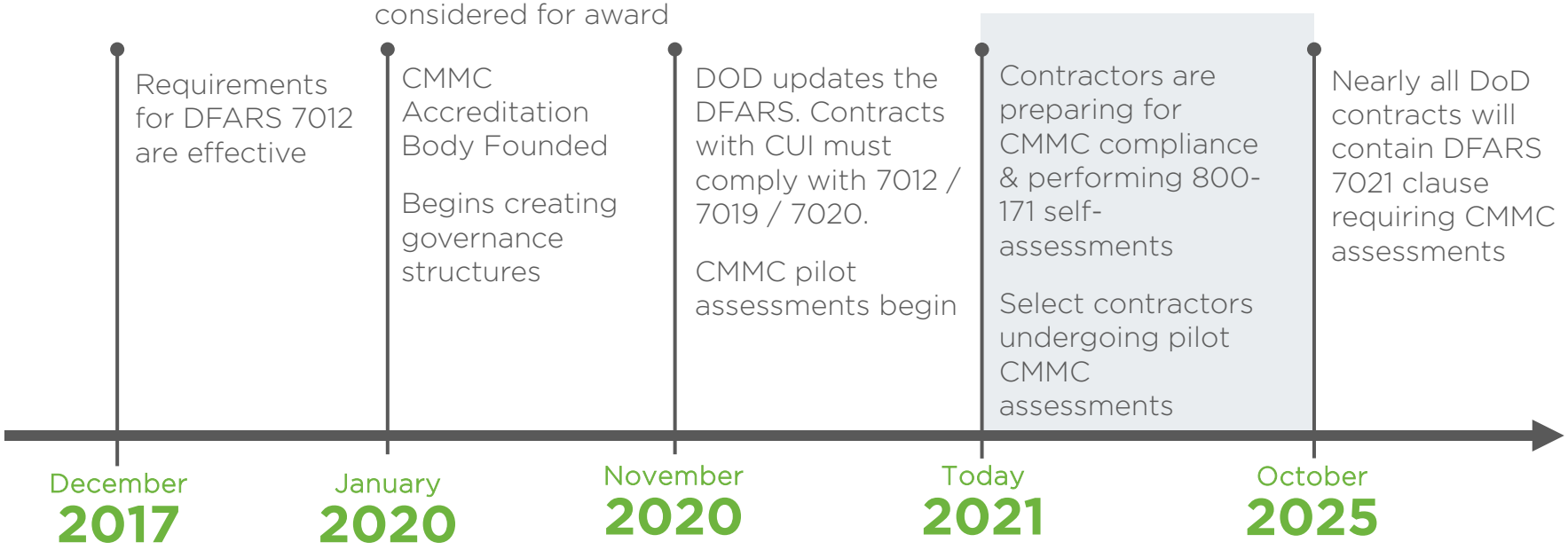
Timeline & Key DFARS Clauses

DFARS 7012 Req. to implement security controls in NIST SP 800-171 and report security incidents

DFARS 7019 Notice of requirement to have a NIST SP 800-171 self-assessment to be considered for award

DFARS 7020 Req. for NIST SP 800-171 assessment
- Basic – Self-assessment
- Medium/High – performed by gov

DFARS 7021 Requirement for third-party security assessments based on the CMMC



Timeline & Key DFARS Clauses

Requirements Appearing in Contracts

November
2020

October
2025

CMMC Accreditation Body

- CMMC AB has created structures to accredit organizations and certify individuals to perform consulting, assessments, and training
- Ecosystem of professionals is still forming
- Key Organizational Accreditations
  - Certified 3rd Party Assessment Organization (C3PAO)
  - Registered Provider Organizations (RPO)
  - More @ https://cmmcab.org/

Enforcement

- NIST SP 800-171 Enforcement:
  - Contract will not be awarded without a Basic, i.e. self-assessment recorded in the Supplier Performance Risk System (SPRS)
  - Self-assessments must be no less than 3 years old
    - Gov can request more frequent
    - Gov reserves right to send in their own auditors for Medium or High assessments
- CMMC Enforcement:
  - Government defines requirement in the contract (Maturity Level 1 – 5)
  - To be awarded a contract, an organization must have a certification at the maturity level designated in the request for proposal
  - i.e., no certification, no contract award
  - Certifications will last for three years

NIST SP 800-171 vs CMMC

NIST SP 800-171

- 110 Controls
- Contractor self-assessments
- Scoring: Start w/ 110 points and subtract for controls not implemented
- For controls not implemented, contractors must document a plan of action and milestones (POA&M)
- Results uploaded by contractor to SPRS

CMMC

ML 1	ML 3	ML 5
17 practices	130 practices	172 practices
FCI	**CUI**	**CUI**

- 100% compliance required
- Practices must be implemented for a period of time
- Assessments performed by certified 3rd party assessor organizations (C3PAO)
- Scoring: pass/fail
- No POA&Ms allowed

NIST SP 800-171 vs CMMC

NIST SP 800-171

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
3.1.1[a]	*authorized users are identified.*
3.1.1[b]	*processes acting on behalf of authorized users are identified.*
3.1.1[c]	*devices (and other systems) authorized to connect to the system are identified.*
3.1.1[d]	*system access is limited to authorized users.*
3.1.1[e]	*system access is limited to processes acting on behalf of authorized users.*
3.1.1[f]	*system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC

AC.1.001

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

CMMC Assessment Methods

- Assessors will:
  - Interview appropriate staff
  - Examine documentation* or observe processes
  - Test practices, when applicable
- Three types of findings:
  - MET
  - NOT MET
  - NOT APPLICABLE (N/A)

* Documentation must be in its final form – draft policies, procedures, etc. will not be accepted by assessors.

Cloud Service Providers

- Some practices will be “inherited” from cloud service providers
- You will have to provide your assessor evidence that your service provider meets the practice.
  - Example: Your Active Directory servers are housed within a Microsoft Azure. Practices related to datacenter security would be inherited. You would provide your assessor certifications from Microsoft that you are subscribed to a service that meets government requirements.
- Waiting for final guidance on reciprocity of FedRAMP certified platforms.
  - Likely there will be reciprocity, and likely companies will be required to use the government certified versions of platforms.
  - Example: Microsoft Government Cloud, AWS Gov Cloud, etc.

CMMC Guidance

- An organization's cybersecurity posture is assessed by evaluating *assessment objectives*, which fall under *practices* which fall under CMMC *domains*.
  - Domains: Groups of practices
  - Practices: High-level control language – Usually one sentence
  - Assessment Objectives: Specific list of requirements that must be met for each Practice

To pass the CMMC assessment, an organization must meet ***all*** assessment objectives as outlined by the CMMC Assessment Guide.

CMMC Requirements

CMMC		
ML 1 17 practices 0 process maturity reqs **FCI**	ML 3 130 practices 51 process maturity reqs **CUI**	ML 5 172 practices 85 process maturity reqs **CUI**

› Practices only, no Process Maturity requirements
› 59 total Assessment Objectives
	› Assessment Objectives
	  › 381 for practices
	  › 310 for process maturity
	  › 691 total
		› Unknown total # of Assessment Objectives – guidance not yet released

CMMC Process Maturity

- Process Maturity are governance requirements that are applied to each of the 17 Domains

CMMC ML	Process Maturity Requirement
ML 2	› Establish a policy for the domain › Document procedures to implement the policy for the domain
ML 3	› Establish, maintain, and resource a plan for the domain
ML 4	› Review and measure Domain practices for effectiveness
ML 5	› Standardize and optimize a documented approach for the Domain across all organizational units

Key Practice Areas: Access Control

- AC.1.001 (6 assessment objectives)
  - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- AC.1.002 (2 assessment objectives)
  - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- AC.1.003 (6 assessment objectives)
  - Verify and control/limit connections to and use of external information systems.
- AC.1.004 (5 assessment objectives)
  - Control information posted or processed on publicly accessible information systems.

Key Practice Areas: Access Control

- AC.1.001 (6 assessment objectives)
  - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
  - Assessment Objectives
  - Determine if:
    - [a] authorized users are identified;
    - [b] processes acting on behalf of authorized users are identified;
    - [c] devices (and other systems) authorized to connect to the system are identified;
    - [d] system access is limited to authorized users;
    - [e] system access is limited to processes acting on behalf of authorized users; and
    - [f] system access is limited to authorized devices (including other systems).

What Now?

- Market overview
  - ~ 120k orgs will need to comply with NIST 800-171
  - ~ 300k orgs will need to comply with the CMMC
    - ~60% @ ML 1 & ~40% @ ML 3 --- very few ML 5 expected
  - Expect supply crunch of consultants and assessors as Oct 2025 approaches
  - DoD expects contractor costs to manifest in Cost base
- Prep for CMMC and perform NIST SP 800-171 self-assessments

Do I need a NIST 800-171 self-assessment?

- Examine your contracts for insights.

Contract Date	Guidance
Before Dec 2017	› If you process CUI and your contract will come up for rebid before Oct 2025, YES.
Dec 2017 to Nov 2020	› If your contract contains DFARS 7012, YES.
After Nov 2020	› If your contract or RFPs contain DFARS 7012/7019/7020, YES.

- Some orgs have the resources to do this themselves. But if you need assistance, don't wait until the requirement appears in an RFP before you start.

What CMMC Level to prep for?

- Which level to prep for is a risk-based management decision:
  - Don't want to spend on unnecessary compliance, but don't want to miss out on contracts because your CMMC level is too low.
- Review your current contracts:
  - If DFARS 7012/7019/7020 or if you process CUI
    - Prepare for ML 3, minimum
  - If you expect to bid on contracts that require you to generate or receive CUI
    - Prepare for ML 3, minimum
  - If you only expect to ever interact with FCI
    - Prepare for ML 1

How Keiter Can Help

› Flexible approach to suit a wide-array of needs

DoD Cyber Compliance Support		
CMMC Only	Common to NIST and CMMC	NIST SP 800-171 Only
› Readiness Reports › Assessments (eventually)	› Identify Scoping › Draft System Security Plan › Drafting Policies › Vulnerability Scanning (RM.2.142) › Penetration Testing (CA.4.164/CA.4.22)	› Self-Assessment and Scoring › Draft POA&Ms

Readiness Process

- CMMC Readiness Report
  - Define Scoping
  - Summary of high-level observations and findings
  - Scorecard showing Met, Not Met, or N/A for each Practice and Assessment Objective
  - Detailed writeup for each Practice and Assessment Objective:
    - If Met – we will describe how you meet it and what information you will likely need to provide to assessors
    - If Not Met – we will describe the deficiency and provide recommendations
    - If N/A – we will describe why it does not apply
  - If ML 2 or greater – we can draft your SSP

Discussion and Questions

› Contact us: **cmmc@keitercpa.com**

Scott McAuliffe, CPA, CISA, RP
Partner, Risk Advisory Services
smcauliffe@keitercpa.com
(804) 273-6247

Chris Moschella, CPA, CISA
Senior Manager, Risk Advisory Services
cmoschella@keitercpa.com
(804) 419-2902