Securing the DoD Supply Chain
Cybersecurity Maturity Model Certification

Ms. Katie Arrington
Chief Information Security Officer for Acquisition
17 Capability Domains (v1.0)

Capabilities are assessed for Practice and Process Maturity

<table>
<thead>
<tr>
<th>PRACTICES</th>
<th>PROCESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td>Performed</td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td>Documented</td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td>Managed</td>
</tr>
<tr>
<td><strong>Level 4</strong></td>
<td>Reviewed</td>
</tr>
<tr>
<td><strong>Level 5</strong></td>
<td>Optimizing</td>
</tr>
</tbody>
</table>

- **Basic Cyber Hygiene**
- **Intermediate Cyber Hygiene**
- **Good Cyber Hygiene**
- **Proactive**
- **Advanced / Progressive**

Access Control (AC)  Incident Response (IR)  Risk Management (RM)
Asset Management (AM)  Maintenance (MA)  Security Assessment (SAS)
Awareness and Training (AT)  Media Protection (MP)  Situational Awareness (SA)
Audit and Accountability (AA)  Personnel Security (PS)  System and Communications Protection (SCP)
Configuration Management (CM)  Physical Protection (PP)  System and Information Integrity (SII)
Identification and Authentication (IDA)  Recovery (RE)
CMMC Practice Progression

LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
- Demonstrate compliance with Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
- Comply with the FAR
- Perform a select subset of 48 practices from the NIST SP 800-171 r1
- Perform an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
- Comply with the FAR
- Perform all 110 practices from the NIST SP 800-171 r1
- Perform an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE
152 PRACTICES
- Comply with the FAR
- Perform all 110 practices from the NIST SP 800-171 r1
- Perform an additional 20 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
- Comply with the FAR
- Perform all 110 practices from the NIST SP 800-171 r1
- Perform a select subset of 17 practices from Draft NIST SP 800-171B
- Perform an additional 40 practices to demonstrate an advanced cybersecurity program

Reduces risk of Advanced Persistent Threats (APTs)
CMMC Maturity Process Progression

LEVEL 1
PERFORMED

0 PROCESSES
✓ Select practices are documented where required

LEVEL 2
DOCUMENTED

3 PROCESSES
✓ Each practice is documented
✓ A policy exists that includes all activities
✓ A plan exists, is maintained, and resourced that includes all activities (includes mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders)

LEVEL 3
MANAGED

4 PROCESSES
✓ Each practice is documented
✓ A policy exists that includes all activities
✓ Adherence is verified through Examine or Test
✓ A plan exists that includes all activities
✓ Activities are reviewed and measured for effectiveness
✓ There is a standardized, documented approach across all applicable organizational units

LEVEL 4
REVIEWED

5 PROCESSES
✓ Each practice is documented
✓ A policy exists that includes all activities
✓ Adherence is verified through Examine or Test
✓ A plan exists that includes all activities
✓ Activities are reviewed and measured for effectiveness (results of the review is shared with higher level management and for issue resolution)

LEVEL 5
OPTIMIZING

DISTRIBUTION A. Approved for public release
CMMC Model Evolution
v0.4 to v0.5 to v0.6 to v0.7 to v1.0

DISTRIBUTION A. Approved for public release
**CMMC Model v1.0: Source Counts**

- **CMMC Model leverages multiple sources and references**
  - CMMC Level 1 only includes practices from FAR Clause 52.204-21
  - CMMC Levels 4 and 5 do not include QTY 16 practices from Draft NIST SP 800-171B because of implementation complexity/constraints and/or cost

### CMMC Model v1.0: Number of Practices per Source

<table>
<thead>
<tr>
<th>CMMC Level</th>
<th>Total Number Practices per CMMC Level</th>
<th>Source</th>
<th>48 CFR 52.204-21</th>
<th>NIST SP 800-171r1</th>
<th>Draft NIST SP 800-171B</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>17</td>
<td>17 *</td>
<td>17</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Level 2</td>
<td>55</td>
<td>-</td>
<td>48</td>
<td>-</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td>58</td>
<td>-</td>
<td>45</td>
<td>-</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Level 4</td>
<td>26</td>
<td>-</td>
<td>-</td>
<td>13</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Level 5</td>
<td>15</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>171</strong></td>
<td><strong>17</strong></td>
<td><strong>110</strong></td>
<td><strong>17</strong></td>
<td><strong>44</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Excluded</strong></td>
<td><strong>-</strong></td>
<td><strong>-</strong></td>
<td><strong>-</strong></td>
<td><strong>16</strong></td>
<td><strong>-</strong></td>
<td></td>
</tr>
</tbody>
</table>

* Note: QTY 15 safeguarding requirements from FAR clause 52.204-21 correspond to QTY 17 security requirements from NIST SP 800-171r1, and in turn, QTY 17 practices in CMMC

DISTRIBUTION A. Approved for public release
CMMC Accreditation Body Activities

CMMC Database
- Populated and accessible by DoD systems

Accreditation Body (AB) Manager
- Coordinate w/ CMMC PMO and CMMC Advisory Council
- Dispute resolution
- Capture metrics
- Integrate and coordinate functional areas

Training
- Train Individuals
- Train Organizations
- Train Instructors

Infrastructure (Support Systems)
- Knowledge Store
- Market Place
- Artifact Store
- Records Mgmt.

Accreditation
- Grant C3PAO accreditations
- Audit C3PAO
- Process Complaints

Credentialing
- Grant Individual credentials
- Certifiers
- Accredited Certifiers

Assessment Operations
- Technical Appeals
- Quality Control
- Manage Assessment Tool
- Publish CMMC Certificates
# CMMC Draft Schedule: CY20

## Rulemaking
- **Q2FY20**: DAR Council Meeting
- **Q4FY20**: Goal: Complete Rulemaking Process

## CMMC Roll-Out Plan
* Depends upon Rulemaking

- **Q2FY20**: Initial Planning
- **Q3FY20**: Initial RFIs with CMMC Requirement
- **Q4FY20**: Initial RFPs with CMMC Requirement
- **Q1FY21**: * Depends upon Rulemaking

## DoDI 5000.02 Cybersecurity Enclosure
- **Q2FY20**: Initial Planning
- **Q3FY20**: Complete reviews and approval

## CMMC Implementation Pathfinder(s) with Subset of DIB Sector
- **Q2FY20**: * Depends upon Rulemaking

## CMMC Accreditation Body (AB)
- **Q1FY21**: Establishment of CMMC AB Board
- **Q2FY20**: Initial Planning
- **Q3FY20**: Sign MOU (TBD)
- **Q4FY20**: Marketplace (TBD)
- **Q1FY21**: Certification process for candidate CMMC Third Party Assessment Organizations (C3PAOs)

## CMMC Databases & Infrastructure
- **Q2FY20**: * Depends upon Rulemaking
- **Q3FY20**: Database/Infrastructure Pathfinder
- **Q4FY20**: Initial Beta Testing

## CMMC AB Training
- **Q1FY21**: Train the trainers
- **Q2FY20**: CMMC classes for assessors
- **Q3FY20**: Refine Draft Training & Conduct Training Pathfinder with DoD
- **Q4FY20**: Initiate Training for CMMC 101, Levels 1-3
- **Q1FY21**: Initiate Training for CMMC Levels 4-5

## Draft CMMC Training Material to CMMC Accreditation Body (AB)
- **Q2FY20**: Deliver Draft Training CMMC 101
- **Q3FY20**: Deliver Draft Training CMMC Levels 1-3
- **Q4FY20**: Deliver Draft Training CMMC Levels 4-5
- **Q1FY21**: Coordinate and Conduct Training Pathfinder with CMMC AB

## Defense Acquisition University (DAU) CMMC Training
- **Q2FY20**: * Depends upon Rulemaking
- **Q3FY20**: Complete & Release v1.0
- **Q4FY20**: Update & Refine CMMC Assessment Guides

## CMMC Assessment Guides
- **Q2FY20**: * Depends upon Rulemaking
- **Q3FY20**: Deliver Levels 4-5 to CMMC AB
- **Q4FY20**: Update & Refine CMMC Assessment Guides

## CMMC Model
- **Q2FY20**: * Depends upon Rulemaking
- **Q3FY20**: * Depends upon Rulemaking
- **Q4FY20**: Potential update based on rulemaking process (TBD)
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

<table>
<thead>
<tr>
<th>Total Number of Contracts with CMMC Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY21</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY21</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>Level 1</td>
</tr>
<tr>
<td>Level 2</td>
</tr>
<tr>
<td>Level 3</td>
</tr>
<tr>
<td>Level 4</td>
</tr>
<tr>
<td>Level 5</td>
</tr>
<tr>
<td>Total</td>
</tr>
</tbody>
</table>

• All new DoD contracts will contain the CMMC requirement starting in FY26

DISTRIBUTION A. Approved for public release