Securing the DoD Supply Chain
Cybersecurity Maturity Model Certification

Ms. Stacy S. Bostjanick
Director CMMC
We need to make Security the Foundation
We need to Deliver Uncompromised

Cost, Schedule, Performance
ARE ONLY EFFECTIVE IN A SECURE ENVIRONMENT

DISTRIBUTION A. Approved for public release
DIB Cybersecurity Posture

Hypothesis: < 1% of DIB companies

Vast majority of DIB companies

• State-of-the-Art
  – Maneuver, Automation, SecDevOps

• Nation-state
  – Resourcing: Infosec dedicated full-time staff ≥ 4, Infosec ≥ 10% IT budget
  – Sophisticated TTPs: Hunt, white listing, limited Internet access, air-gapped segments
  – Culture: Operations-impacting InfoSec authority, staff training and test

• Good cyber hygiene
  – NIST SP 800-171 compliant, etc.
  – Consistently defends against Tier I-II attacks

• Ad hoc
  – Inconsistent cyber hygiene practices
  – Low-level attacks succeed consistently
Cybersecurity Maturity Model Certification (CMMC)

- The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.

- The CMMC levels will range from basic hygiene to “State-of-the-Art” and will also capture both security control and the institutionalization of processes that enhance cybersecurity for DIB companies.

- The required CMMC level (notionally between 1 – 5) for a specific contract will be contained in the RFP sections C & L, and will be a “go/no-go decision”.

- The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.

- The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.

- The CMMC will include a center for cybersecurity education and training.

- The CMMC will include the development and deployment of a tool that 3rd party cybersecurity certifiers will use to conduct audits, collect metrics, and inform risk mitigation for the entire supply chain.
CMMC Model Structure

18 Domains (Rev 0.4)

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Identification and Authentication</th>
<th>Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Management</td>
<td>Incident Response</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Maintenance</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Media Protection</td>
<td>Situational Awareness</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Personnel Security</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Cybersecurity Governance</td>
<td>Physical Protection</td>
<td>System and Information Integrity</td>
</tr>
</tbody>
</table>

Capabilities assessed for Practice and Process maturity

<table>
<thead>
<tr>
<th>Practices</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 – Basic Cyber Hygiene</td>
<td>Level 1 – Performed</td>
</tr>
<tr>
<td>Level 2 – Intermediate Cyber Hygiene</td>
<td>Level 2 – Documented</td>
</tr>
<tr>
<td>Level 3 – Good Cyber Hygiene</td>
<td>Level 3 – Managed</td>
</tr>
<tr>
<td>Level 4 – Proactive</td>
<td>Level 4 – Reviewed</td>
</tr>
<tr>
<td>Level 5 – Advanced / Progressive</td>
<td>Level 5 – Optimized</td>
</tr>
</tbody>
</table>

DISTRIBUTION A. Approved for public release
# Model Rev 0.4 Synopsis - Practices

<table>
<thead>
<tr>
<th>Description of Level Practices</th>
<th>CMMC Rev 0.3 Practices</th>
<th>New CMMC Rev 0.4 Material</th>
<th>CMMC Rev 0.4 Practices</th>
<th>Mapping: Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMMC Level 1</td>
<td>Basic Cyber Hygiene</td>
<td>17</td>
<td>+18 practices</td>
<td>35</td>
</tr>
<tr>
<td>CMMC Level 2</td>
<td>Intermediate Cyber Hygiene</td>
<td>46</td>
<td>+69 practices</td>
<td>115</td>
</tr>
<tr>
<td>CMMC Level 3</td>
<td>Good Cyber Hygiene</td>
<td>63</td>
<td>+28 practices</td>
<td>91</td>
</tr>
<tr>
<td>CMMC Level 4</td>
<td>Proactive</td>
<td>10</td>
<td>+85 practices</td>
<td>95</td>
</tr>
<tr>
<td>CMMC Level 5</td>
<td>Advanced / Progressive</td>
<td>4</td>
<td>+30 practices</td>
<td>34</td>
</tr>
</tbody>
</table>

NIST SP 800-171 rev 1
NIST SP 800-171 rev B

DISTRIBUTION A. Approved for public release
CMMC Development Schedule

May | Jun | Jul | Aug | Sep | Oct | Nov | Dec | Jan
---|---|---|---|---|---|---|---|---

CMMC Model WG
- Rev 0.1
- Rev 0.2
- Rev 0.3
- Rev 0.4
- Rev 0.5
- Rev 0.6
- Rev 0.7
- Rev 1.0

Framework & Level Definitions
- Confidentiality Only
- Incorporates Integrity & Availability
- Relevant Standards Included
- Full Reference & Mappings Complete

Scope and Sources
- NIST SP 800-53
- AIA NA99933
- DIB SCDT WG: Top 16
- UK MIB
- Processes (CRA, RMM, etc.), DISA Cloud SRG, NIST SP 800-53 r5 (partial)

Stakeholder Input & Perspectives
- CMMC Deep Dive with Industry
- Follow-up Deep Dive
- Public Comment Periods

Threat Modeling (e.g., DoDCAR)
- Initial DoDCAR Analysis
- Updated DoDCAR Analysis

Assessment Guidance
- Initial Drafts: 9 Domains
- Full Drafts: 18 Domains
- Updated Guidance

CMMC Phase 2 (CMMC-ED)
- Scoping and Model Development

CMMC Outreach WG
- Listening Sessions
- Initial Pathfinder

CMMC Implementation WG
- Mtg #1: Review Draft Charter
- Mtg #2: Complete Charter
- Mtg #3: Prepare RFI
- RFI for Interested Parties
- Solidify Members
- Draft Governance Documents
- Finalize Requirements and Training Material
- AB Established
- Transition of CMMC v1.0

CMMC Accreditation Body

DISTRIBUTION A. Approved for public release