Securing the DoD Supply Chain
Cybersecurity Maturity Model Certification (CMMC)

July 15, 2019

Ms. Katie Arrington
HQE Cyber for ASD (A)
We need to make Security the Foundation
We need to Deliver Uncompromised

Cost, Schedule, Performance
ARE ONLY EFFECTIVE IN A SECURE ENVIRONMENT
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 new standard and maturity model will be named Cybersecurity Maturity Model Certification (CMMC)

- 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 L & M, 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.
Notional CMMC Model Development

Phase I: Control Frameworks
- NIST 800-171
- NIST 800-53
- RMF
- DISA STIGs
- FICO
- FedRAMP
- ISO 9000
- FIPS 140-2
- CMMI
- ISO 27001
- SANS
- AIA NAS9933
- Gartner

Phase I: Infosec Solutions
- Industry
- USCybercom
- NSA
- JHUAPL
- Financial Sector
- DOD CIO
- Mitre
- DOE
- MDA

Phase II: Mission Systems Development Environments
- USN
- SMC
- AF
- JHUAPL
- DHS
- NASA
- Army

Maturity model must be dynamic and threat informed.
## CMMC Phase 1: Model v0.2

<table>
<thead>
<tr>
<th>Level</th>
<th>Initial Thinking</th>
<th>CMMC v0.2: Updated Mapping of NIST SP 800-171 rev1</th>
<th>CMMC v0.1: Initial Mapping of Draft NIST SP 800-171 revB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMMC Level 5</td>
<td>Advanced / Progressive</td>
<td></td>
<td>4 security controls</td>
</tr>
<tr>
<td>CMMC Level 4</td>
<td>Proactive</td>
<td></td>
<td>26 security controls</td>
</tr>
<tr>
<td>CMMC Level 3</td>
<td>Good Cyber Hygiene</td>
<td>47 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 2</td>
<td>Intermediate Cyber Hygiene</td>
<td>46 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 1</td>
<td>Basic Cyber Hygiene</td>
<td>17 security controls</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**
- Number of controls per level will change in future revisions of CMMC model.
- Leveling criteria is still in flux and will therefore shift controls across levels.
## Draft CMMC Model v0.2

<table>
<thead>
<tr>
<th>Initial Thinking</th>
<th>Initial Mapping: Practices (Controls)</th>
<th>Initial Mapping: Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMMC Level 5</td>
<td>Advanced / Progressive</td>
<td>Draft NIST SP 800-171B</td>
</tr>
<tr>
<td>CMMC Level 4</td>
<td>Proactive</td>
<td>CMM derived sources (pending)</td>
</tr>
<tr>
<td>CMMC Level 3</td>
<td>Good Cyber Hygiene</td>
<td>NIST SP 800-171 rev1</td>
</tr>
<tr>
<td>CMMC Level 2</td>
<td>Intermediate Cyber Hygiene</td>
<td>Additional references reviewed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DIB SCC TF WG Top 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AIA NAS 9933</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• UK Cyber Essentials</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• AUS Essential Eight</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td>CMMC Level 1</td>
<td>Basic Cyber Hygiene</td>
<td></td>
</tr>
</tbody>
</table>

The draft CMMC model will continue to evolve and improve based on inputs and joint work with industry and DoD stakeholders.
Implementation (Pre-Award)
### Draft CMMC Model Development Schedule

<table>
<thead>
<tr>
<th>MAY</th>
<th>JUN</th>
<th>JUL</th>
<th>AUG</th>
<th>SEP</th>
<th>OCT</th>
<th>NOV</th>
<th>DEC</th>
<th>JAN</th>
</tr>
</thead>
</table>

#### Leveling Criteria
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Stakeholder Input & Perspectives
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [ ] Rev 1.0

#### Scope and Sources
- [x] NIST SP 800-171 rev1
- [x] NIST SP 800-171B
- [ ] AIA NAS9933
- [ ] DIB SCC TF
- [ ] WG: Top 10
- [ ] UK,
- [ ] AUS
- [ ] Other Sources… TBD

#### Threat Modeling (e.g., DoDCAR)
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Implementation and 3rd Party Assessment Considerations
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Listening Sessions
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Pathfinders
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Phase 2 Integration
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Revisions
- [ ] Rev 0.1
- [ ] Rev 0.2
- [x] Rev 0.3
- [ ] Rev 0.4
- [ ] Rev 0.5
- [ ] Rev 0.6
- [ ] Rev 0.7
- [x] Rev 1.0

#### Other Comments
- NIST SP 800-171 Rev 1, NIST SP 800-171B
- AIA NAS9933
- DIB SCC TF
- WG: Top 10
- UK, AUS
- Other Sources... TBD
- Begin Incorporating Integrity & Availability
- Complete I&A Incorporation
- Processes (CRA, RMM, etc.), NIST SP 800-53 r5, SP 800-
- Other Sources... TBD
- Threat Update 1
- Threat Update 2
- TBD
- Draft CONOPS
- Final CONOPS
- 12 Jun: Discussion on Options
- Incorporate Feedback 2
- Start Pathfinders
- 0.8→0.9 Edit/Review