Cybersecurity Maturity Model Certification “CMMC” & the State of Cybersecurity in Industry

Corbin Evans, NDIA
Current State of Cybersecurity

2020 SURVEY WITH VERIFY
Survey Results

Themes Heard from Industry
• Cost Implications (all tiers)
• Truth on Current Cyber Status
• Contract Privity vs. Supply Chain Illumination
• “Shift” of Responsibility & Risk
• DIB Resilience (cost & frustration)

Top Challenges (in order)
• Keeping up with changing requirements
• Understanding how regulations apply to their business
• Applying requirements to their specific environment(s)
• Getting budget allocated
Current State of Cybersecurity – Recent Survey Results

Cybersecurity Responsibility

NIST 800-171 Compliance

Self-Assessed Maturity (1-5)

Incident Response Plan
Program Overview

- CMMC is the DOD’s new effort to secure unclassified data held by defense contractors
- The program will have 5 levels
  - Level 1: Basic Security
  - Level 5: Advanced/Progressive Security
- Every contractor that does business with the DOD will need a CMMC certification by 2026
  - The amount of CUI you handle will determine the CMMC level required
- CMMC will be rolled out throughout 2020
- NDIA.org/CMMC
CMMC Practice Progression

**LEVEL 1**
- **BASIC CYBER HYGIENE**
  - 17 PRACTICES
  - ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

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

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

**LEVEL 4**
- **PROACTIVE**
  - 156 PRACTICES
  - ✓ Comply with the FAR
  - Encompasses all practices from NIST SP 800-171 r1
  - Includes a select subset of 11 practices from Draft NIST SP 800-171B
  - Includes an additional 15 practices to demonstrate a proactive cybersecurity program

**LEVEL 5**
- **ADVANCED / PROGRESSIVE**
  - 171 PRACTICES
  - ✓ Comply with the FAR
  - Encompasses all practices from NIST SP 800-171 r1
  - Includes a select subset of 4 practices from Draft NIST SP 800-171B
  - Includes an additional 11 practices to demonstrate an advanced cybersecurity program
CMMC Roll Out Timeline (*Approximate*)

- **January 2020:** CMMC 1.0 released
- **February 2020 – June:** AB Formalized & 3PAOs Trained
- **June 2020:** 10 RFIs released (certifications slated to start)
- **June 2020:** Rulemaking Process for CMMC Begins
- **September 2020:** 10 RFPs released with CMMC language
- **2020 – 2026:** Gradual Ramp Up of Program
- **2026:** All new contracts will contain CMMC language
QUESTIONS?

Corbin Evans, CEVANS@NDIA.org