Cybersecurity Maturity Model Certification (CMMC)

DevilDog CyberSecurity

https://devildogcyber.com/
Origin

• CMU’s Software Engineering Institute
• Capability Maturity Model
  – 1990’s
• The term “maturity” relates to the degree of formality and optimization of processes
CMMI

• Capability Maturity Model Integration
  – 2000’s
• Originally three areas: development, services, procurement
• Purchased in 2016 by Information Systems Audit and Control Association (ISACA)
Who’s Helping Lead CMMC?

• Carnegie Mellon University
• Johns Hopkins University Applied Physics Laboratory
Maturity Levels

• Initial (chaotic, ad hoc, individual heroics)
  – The starting point for use of a new or undocumented repeat process

• Repeatable
  – The process is at least documented sufficiently such that repeating the same steps may be attempted
Maturity Levels

• Defined
  – The process is defined/confirmed as a standard business process

• Capable
  – The process is quantitatively managed in accordance with agreed-upon metrics
Maturity Levels

• Efficient
  – Process management includes deliberate process optimization/improvement
DoD Procurement

• “The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward”
DoD Procurement

• “The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements”
DoD Procurement

• “The intent is for certified independent 3rd party organizations to conduct audits and inform risk”
Based On

• DFARS
• NIST 800-171 rev 1
• NIST 800-171B
• United Kingdom’s Cyber Essentials
• Australia’s Essential Eight
Changes From NIST 800-171

• No self-assessment
  – External, independent review for all levels
• No Plan Of Action and Milestones (POAMs) allowed
• Not allowed to publish level achieved, only that are CMMC compliant
  – Attempt to release less information
Level Required?

• Level 1: every DoD contractor
  – Federal Contract Information (FCI)
  – Over 50,000 companies

• Level 2
  – Intermediate step to level 3
Level Required?

• Level 3
  – Controlled Unclassified Information
  – NIST 800-171 rev 1

• Level 4/5
  – NIST 800-171B
Reviews

- 1 – 3: every three years
- 4 – 5: every year
- Companies must pay upfront, but ongoing costs can be included in contract
Assessors

• Third-party assessment organization (3PAO)
• Currently an RFI for oversight organization
• Likely based on
  – FedRAMP
  – CMMI
  – SEI’s CERT-Resilience Management Model Capability Appraisals
Schedule

• Public comment of draft CMMC Rev 0.6 now
• CMMC Rev 1.0 will be released in January 2020
• Included in RFIs starting in June 2020
• Included in RFPs starting in Fall 2020
Vernacular

• CMMC model framework consists of 18 domains
• Domains are comprised of capabilities
• Capabilities are comprised of practices and processes, which are mapped to CMMC Level 1 through Level 5
  – Practices are activities performed at each level for the domain
  – Processes detail maturity of institutionalization for the practices
Domains

- Access Control
- Asset Management*
- Audit and Accountability
- Awareness and Training*
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection

- Personnel Security
- Physical Protection
- Recovery*
- Risk Management
- Security Assessment
- Situational Awareness*
- System and Communications protection
- System and Information Integrity
Processes

• Level 1
  – None

• Level 2
  – Establish a policy for domain
  – Establish practices to implement domain
  – Establish a plan for domain
Processes

• Level 3
  – Review domain activities for conformance
  – Provide resources for domain

• Level 4
  – Inform high-level management
  – Review domain activities for effectiveness
Processes

• Level 5
  – Standardize documentation for domain
  – Share domain improvements across the organization
Practices

• Level 1 – Basic Cyber Hygiene: 17
  – 48 CFR 52.204-21
  – NIST 800-171r1
• Level 2 – Intermediate Cyber Hygiene: 75
• Level 3 – Good Cyber Hygiene: 131
Practices

• Level 4 – Proactive: 193
  – NIST 800-171B

• Level 5 – Advanced / Progressive: 219
Examples of Level 1 Practices

• FAR requirements
• Anti-virus
• Ad hoc incident response*
• Ad hoc cybersecurity governance*
Examples of Level 2 Practices

• Risk management
• Awareness and training
• Back-ups & security continuity*
Examples of Level 3 Practices

• All NIST SP 800-171 Rev 1 requirements are met
• Multi-factor authentication
• Information Security Continuity Plan*
• Communicate threat information to key stakeholders*
Examples of Level 4 Practices

- Consideration of supply chain risk
- Threat hunting
- Out-of-band administration
- Use of Data Loss Prevention (DLP) technologies
- Detonation chambers
  - Sandboxes
- Inclusion of mobile devices
- Network segmentation
Examples of Level 5 Practices

- Deployment of organizational custom protections
- Cyber maneuver operations
- Hardware root of trust for boot
- Real-time asset tracking
- 24x7 SOC operation
- Context aware access control and step-up authentication
- Device authentication
- Autonomous initial response actions
Resources

- https://devildogcyber.com
DevilDog Cybersecurity Benefits

• Free assessment
  – Vulnerability assessment
  – Gap analysis
• Affordable subscription model
  – Three-tier pricing
• Compliance in three months
  – Depending on size and complexity
DevilDog Cybersecurity Benefits

• Quarterly review
  – Free with subscription
  – High-touch account manager and technical representative

• Guaranteed for certification for Lockheed/Martin subs
Thanks!