Securing the DoD Supply Chain

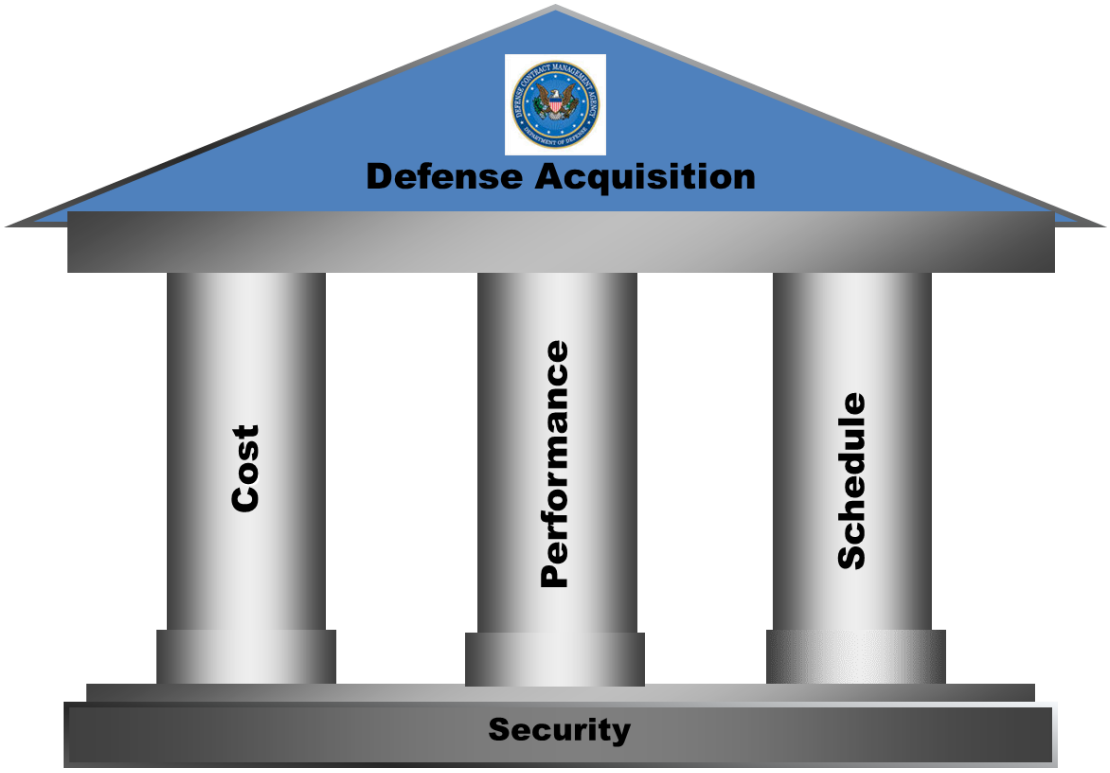
Cybersecurity Maturity Model Certification

Ms. Katie Arrington
Chief Information Security Officer, Office of the Under Secretary of Defense for Acquisition and Sustainment

We need to make Security the Foundation
We need to Deliver Uncompromised

Cost, Schedule, Performance

ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT



DIB Cybersecurity Posture

Hypothesis:
< 1% 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

Vast majority of DIB companies

Cybersecurity Maturity Model Certification (CMMC)

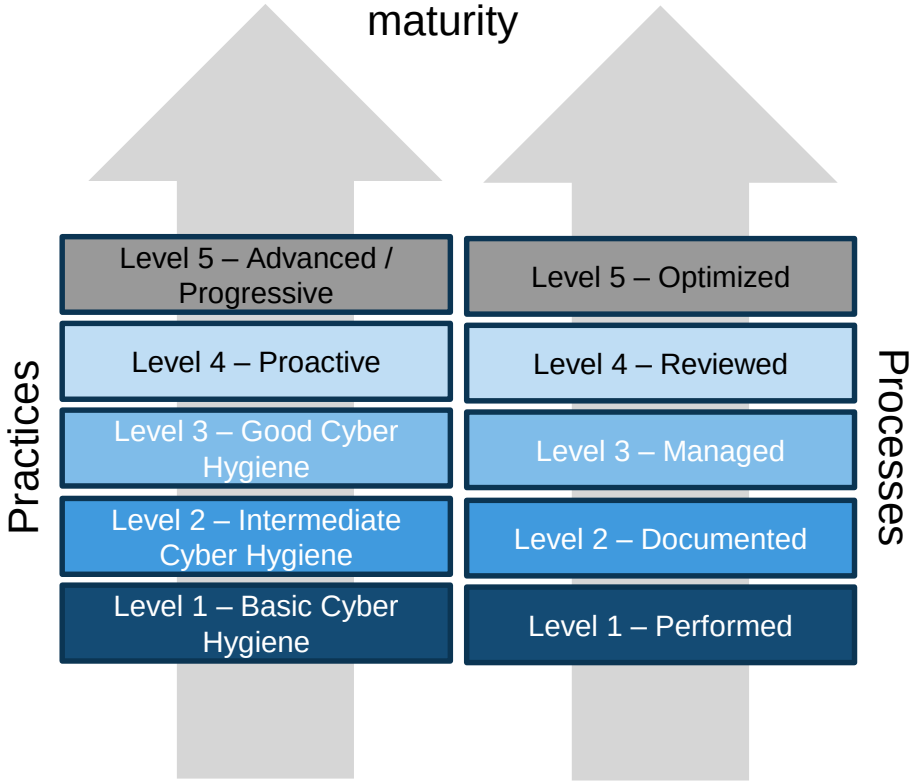
- **The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.**
- **The CMMC levels will range from basic hygiene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

Access Control	Identification and Authentication	Recovery
Asset Management	Incident Response	Risk Assessment
Awareness and Training	Maintenance	Security Assessment
Audit and Accountability	Media Protection	Situational Awareness
Configuration Management	Personnel Security	System and Communications Protection
Cybersecurity Governance	Physical Protection	System and Information Integrity

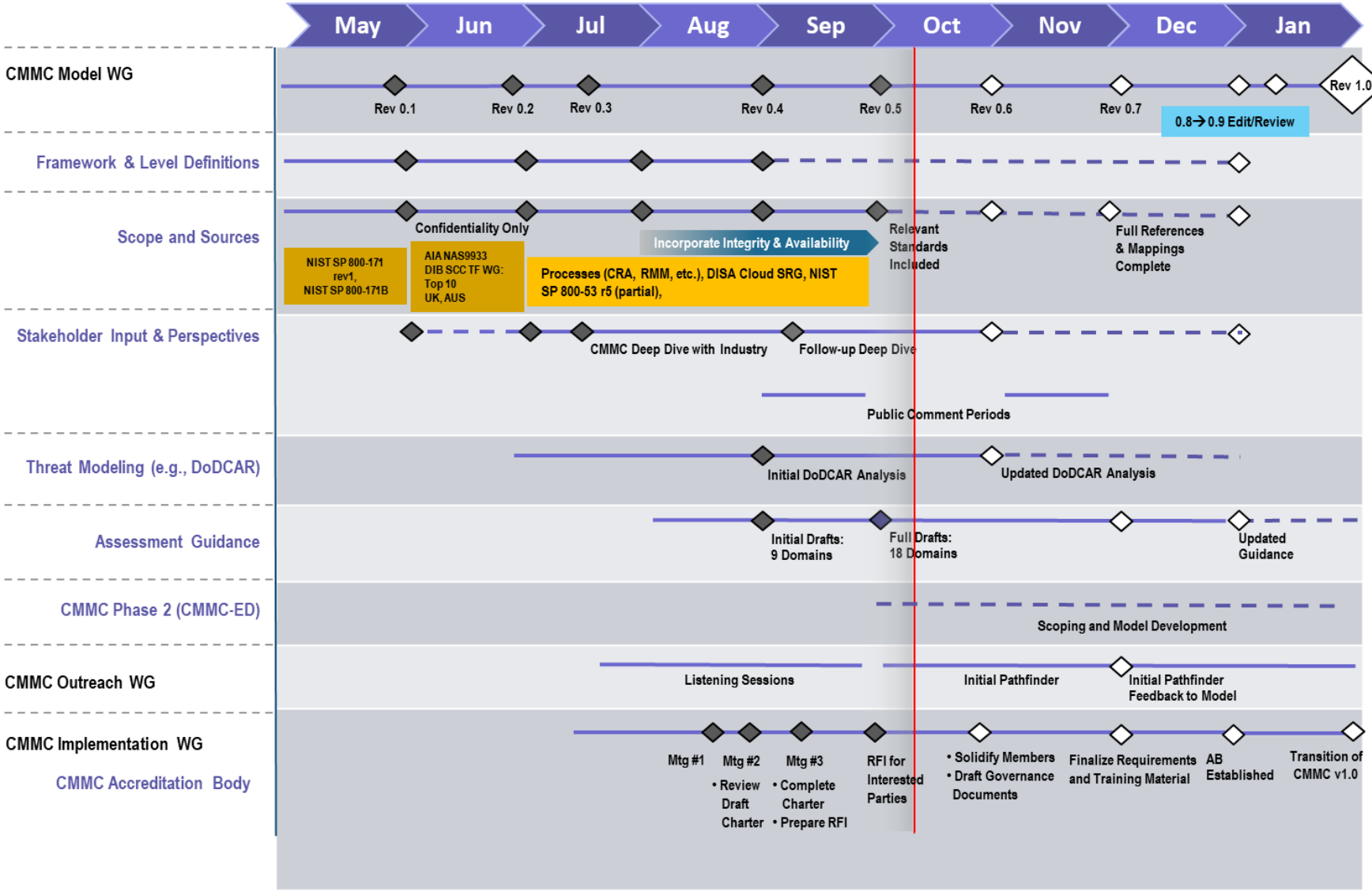
Capabilities assessed for Practice and Process maturity



Model Rev 0.4 Synopsis - Practices

	Description of Level Practices	CMMC Rev 0.3 Practices	New CMMC Rev 0.4 Material	CMMC Rev 0.4 Practices	Mapping: Controls
CMMC Level 1	Basic Cyber Hygiene	17	+18 practices	35	FAR 52
CMMC Level 2	Intermediate Cyber Hygiene	46	+69 practices	115	
CMMC Level 3	Good Cyber Hygiene	63	+28 practices	91	NIST SP 800-171 rev 1
CMMC Level 4	Proactive	10	+85 practices	95	NIST SP 800-171 rev B
CMMC Level 5	Advanced / Progressive	4	+30 practices	34	

CMMC Development Schedule



https://www.acq.osd.mil/cmmc/index.html