



Securing the DoD Supply Chain

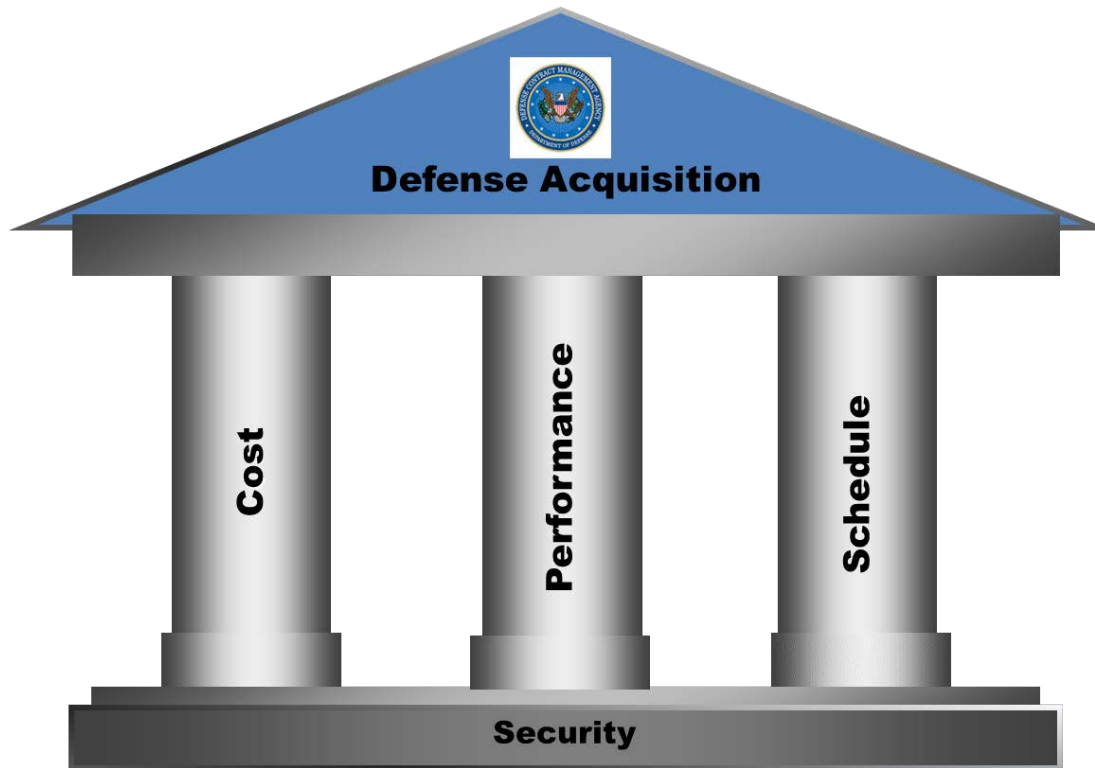
Cybersecurity Maturity Model Certification (CMMC)

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 ENVIROMENT





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 $\geq 10\%$ 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



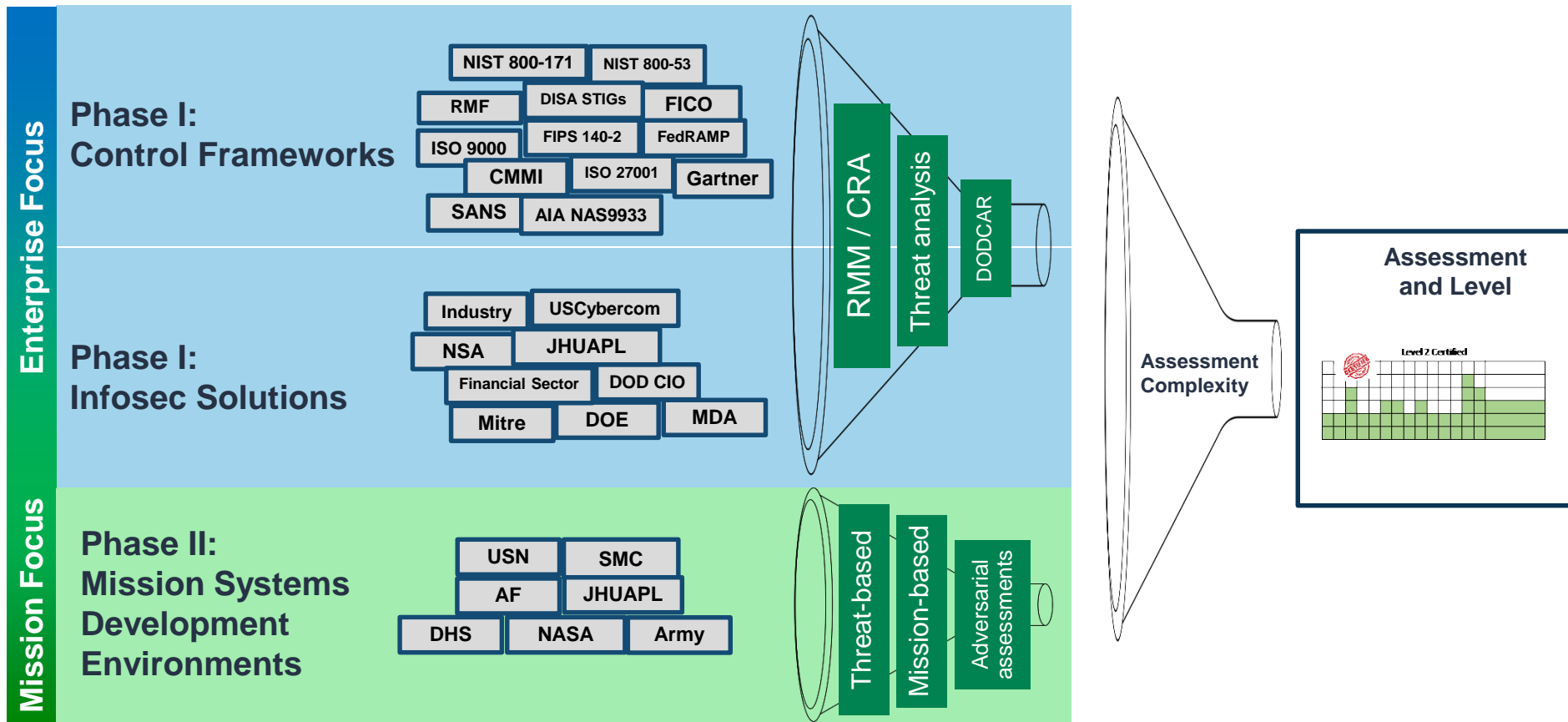
Cybersecurity Maturity Model Certification (CMMC)



- 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 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



Maturity model must be dynamic and threat informed



CMMC Phase 1: Model v0.2

	Initial Thinking	Updated Mapping of NIST SP 800-171 rev1	Initial Mapping of Draft NIST SP 800-171 revB
CMMC Level 5	Advanced / Progressive		4 security controls
CMMC Level 4	Proactive		26 security controls
CMMC Level 3	Good Cyber Hygiene	47 security controls	
CMMC Level 2	Intermediate Cyber Hygiene	46 security controls	
CMMC Level 1	Basic Cyber Hygiene	17 security controls	

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

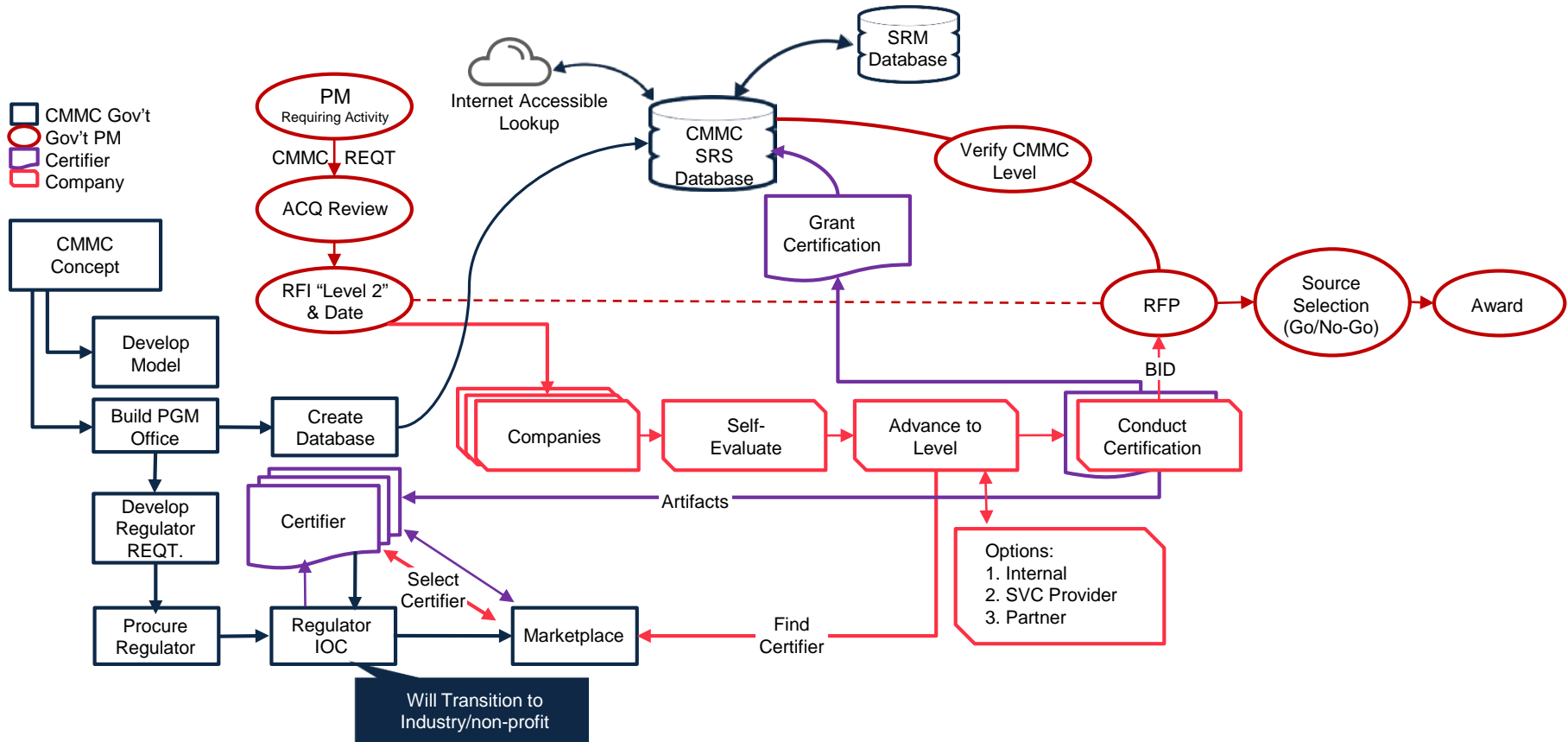


	Initial Thinking	Initial Mapping: Practices (Controls)	Initial Mapping: Processes
CMMC Level 5	Advanced / Progressive	Draft NIST SP 800-171B	CMM derived sources (pending)
CMMC Level 4	Proactive		
CMMC Level 3	Good Cyber Hygiene	NIST SP 800-171 rev1	
CMMC Level 2	Intermediate Cyber Hygiene	Additional references reviewed: <ul style="list-style-type: none">• DIB SCC TF WG Top 10• AIA NAS 9933• UK Cyber Essentials• AUS Essential Eight• Other	
CMMC Level 1	Basic Cyber Hygiene		

The draft CMMC model will continue to evolve and improve based on inputs and joint work with industry and DoD stakeholders

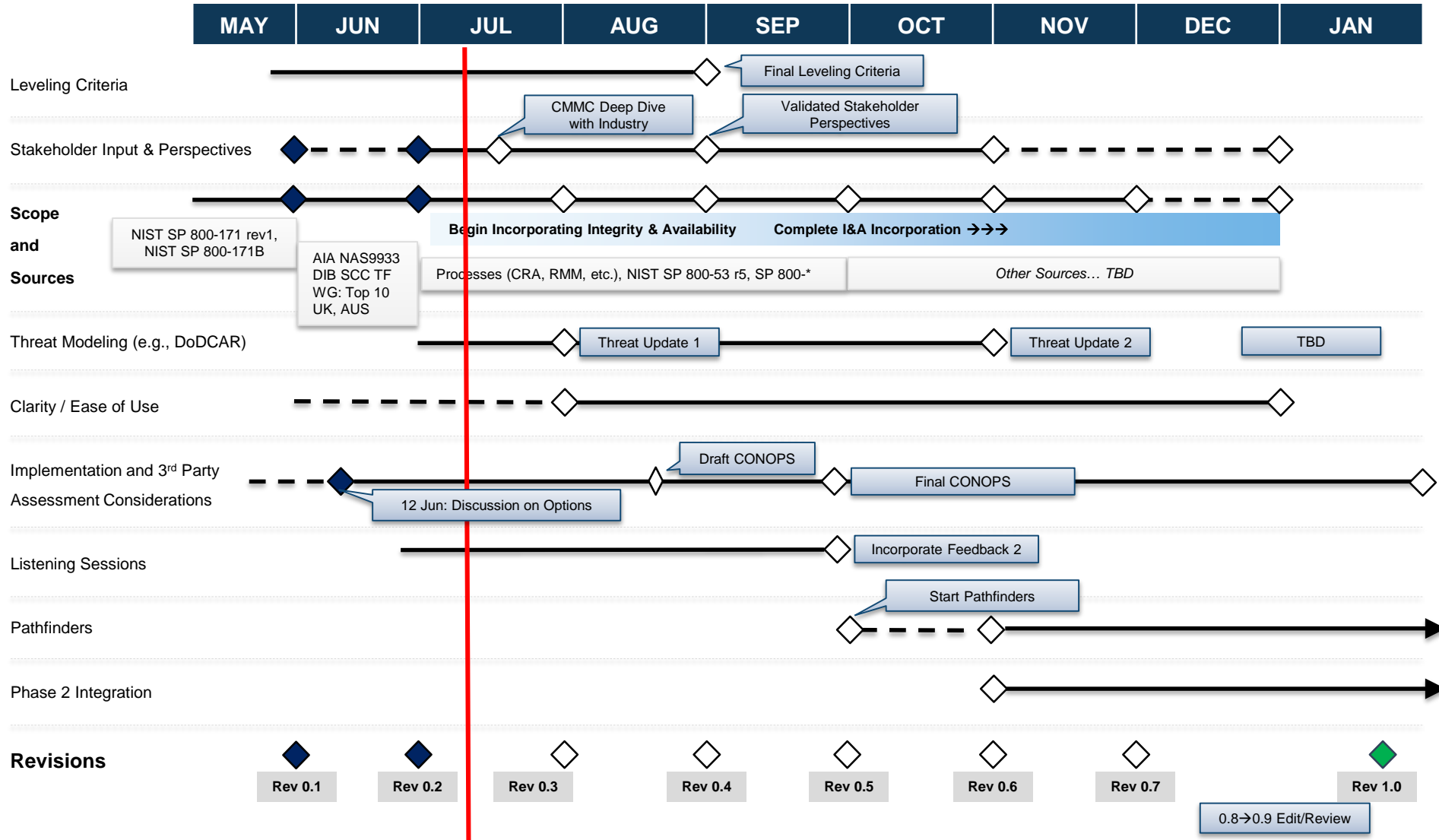


Implementation (Pre-Award)





Draft CMMC Model Development Schedule





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