# Securing the DoD Supply Chain

## Cybersecurity Maturity Model Certification (CMMC)

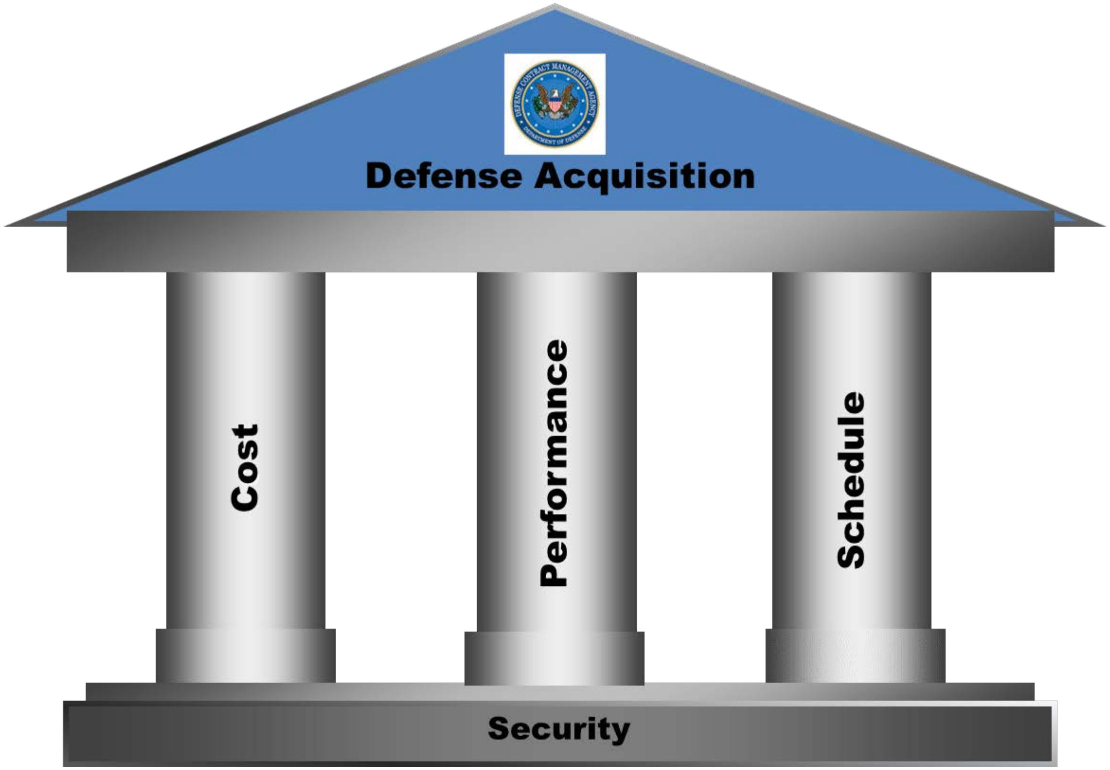
**July 15, 2019**

**Ms. Katie Arrington**
**HQE Cyber for ASD (A)**

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

## Cost, Schedule, Performance

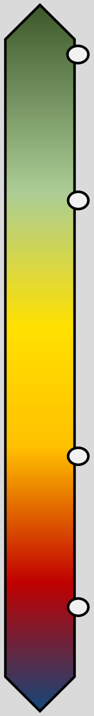
**ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT**



# 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 ≥ 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".**

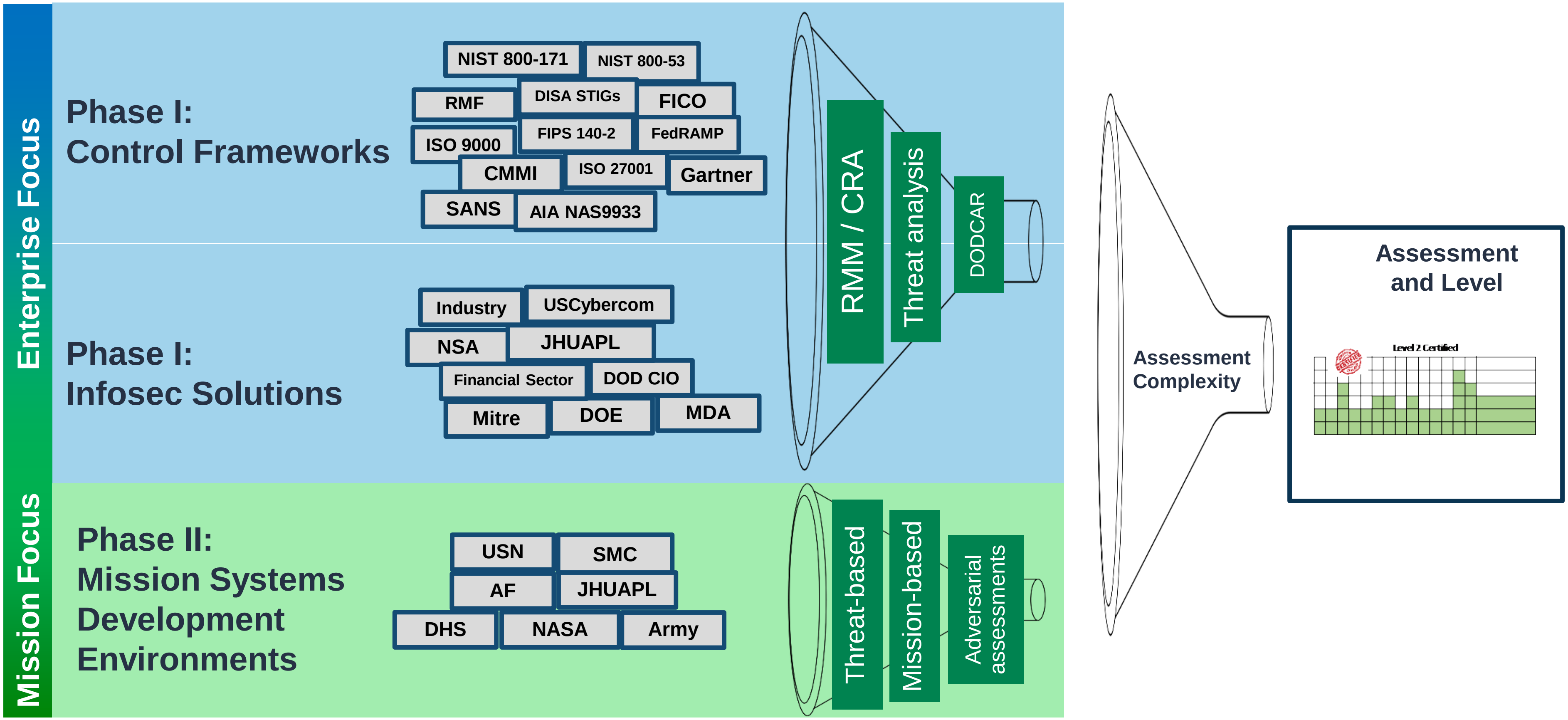
- **The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.**

- **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



Enterprise Focus

Phase I:
Control Frameworks

NIST 800-171 · NIST 800-53 · RMF · DISA STIGs · FICO · ISO 9000 · FIPS 140-2 · FedRAMP · CMMI · ISO 27001 · Gartner · SANS · AIA NAS9933

Phase I:
Infosec Solutions

Industry · USCybercom · NSA · JHUAPL · Financial Sector · DOD CIO · Mitre · DOE · MDA

RMM / CRA · Threat analysis · DODCAR

Mission Focus

Phase II:
Mission Systems Development Environments

USN · SMC · AF · JHUAPL · DHS · NASA · Army

Threat-based · Mission-based · Adversarial assessments

Assessment Complexity

Assessment and Level

Maturity model must be dynamic and threat informed

# CMMC Phase 1: Model v0.2

| | Initial Thinking | CMMC v0.2:<br>Updated Mapping of<br>NIST SP 800-171 rev1 | CMMC v0.1:<br>Initial Mapping of<br>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:**

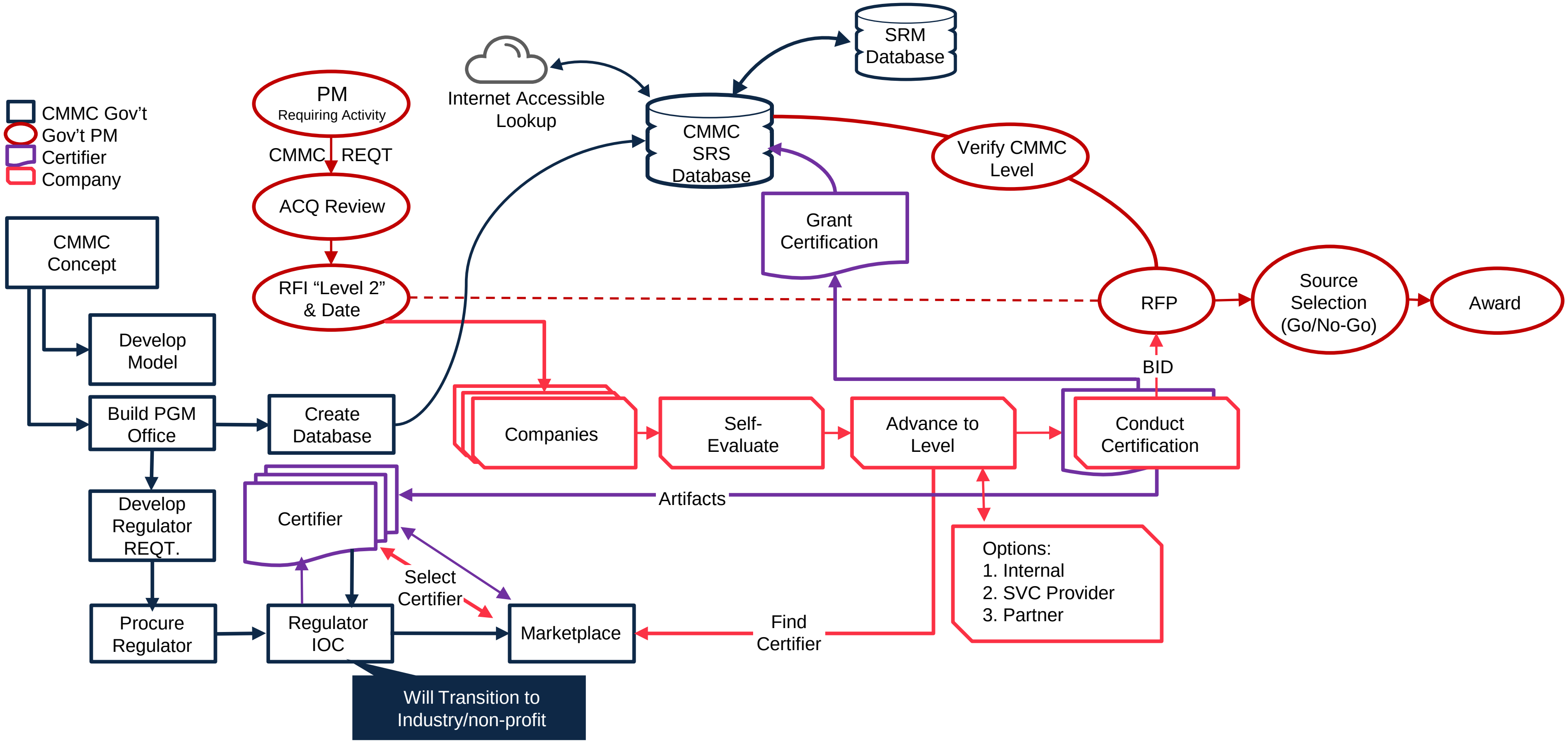
- Number of controls per level will change in future revisions of CMMC model
- Leveling criteria is still in flux and will therefore shift controls across levels

# Draft CMMC Model v0.2

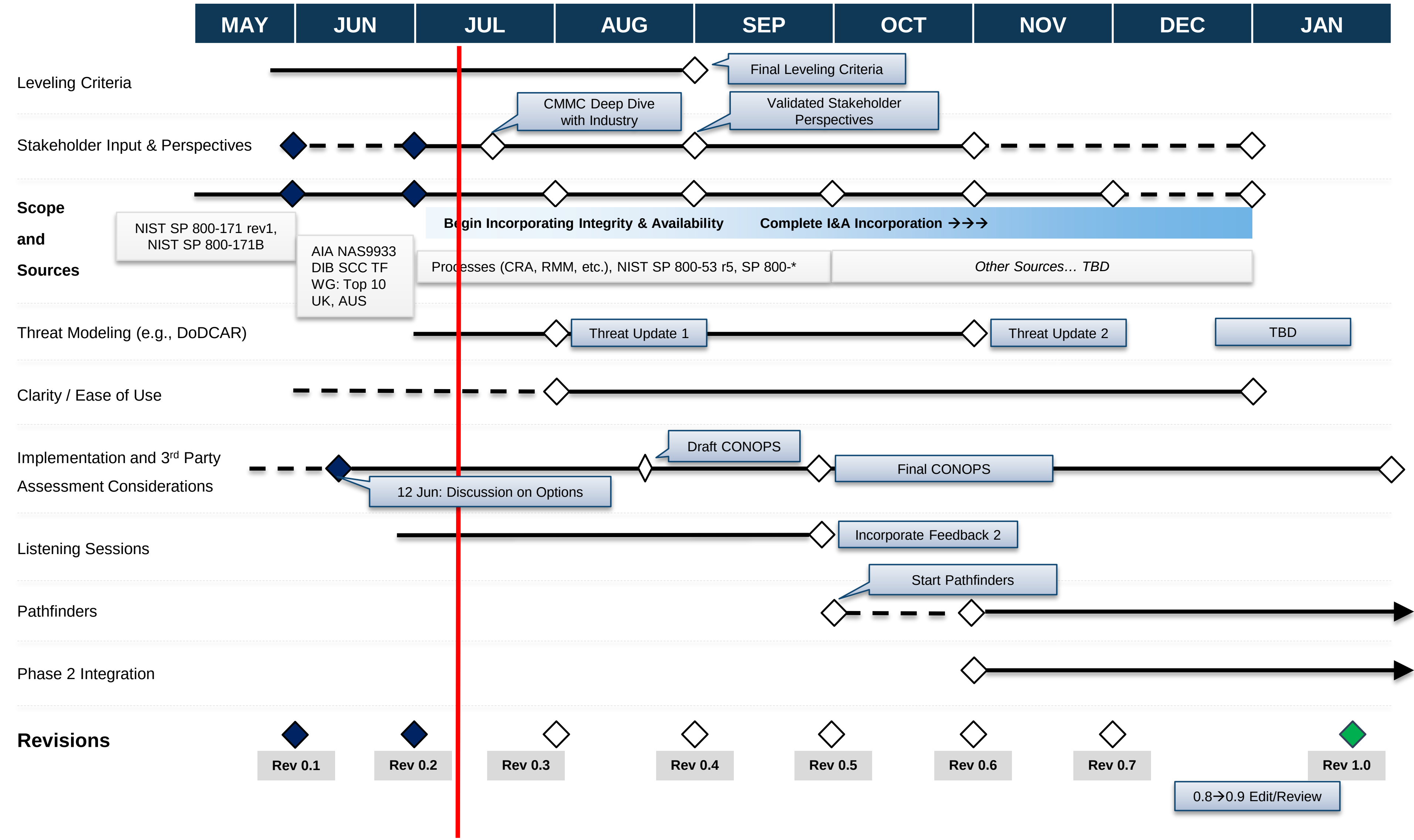
| | Initial Thinking | Initial Mapping: Practices (Controls) | Initial Mapping: Processes |
|---|---|---|---|
| **CMMC Level 5** | Advanced / Progressive | Draft NIST SP 800-171B | CMM derived sources (pending) |
| **CMMC Level 4** | Proactive | | |
| **CMMC Level 3** | Good Cyber Hygiene | NIST SP 800-171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



MAY JUN JUL AUG SEP OCT NOV DEC JAN

Leveling Criteria

Final Leveling Criteria

Stakeholder Input & Perspectives

CMMC Deep Dive with Industry

Validated Stakeholder Perspectives

**Scope and Sources**

NIST SP 800-171 rev1, NIST SP 800-171B

AIA NAS9933
DIB SCC TF
WG: Top 10
UK, AUS

**Begin Incorporating Integrity & Availability** **Complete I&A Incorporation →→→**

Processes (CRA, RMM, etc.), NIST SP 800-53 r5, SP 800-*

*Other Sources… TBD*

Threat Modeling (e.g., DoDCAR)

Threat Update 1

Threat Update 2

TBD

Clarity / Ease of Use

Implementation and 3rd Party Assessment Considerations

Draft CONOPS

Final CONOPS

12 Jun: Discussion on Options

Listening Sessions

Incorporate Feedback 2

Pathfinders

Start Pathfinders

Phase 2 Integration

**Revisions**

**Rev 0.1** **Rev 0.2** **Rev 0.3** **Rev 0.4** **Rev 0.5** **Rev 0.6** **Rev 0.7** **Rev 1.0**

0.8→0.9 Edit/Review