CYBER COLLABORATION CENTER

Cybersecurity Maturity Model Certification (CMMC) Update Featuring Katie Arrington, CISO OUSD A&S

eresilience
EXPERTS IN ENCLAVES

Copyright Notice

CYBER COLLABORATION CENTER

Welcome & Introduction

DFARS 7012 Awareness Campaign

CYBER COLLABORATION CENTER

eresilience
EXPERTS IN ENCLAVES

DFARS 7012 Webinar Series

- *#1 - July 13, 2017: Cybersecurity Requirements Update for Contracts Managers*
- *#2 – August 2, 2017: Prime Contractor Responsibilities for Safeguarding Controlled Unclassified Information (CUI)*
- *#3 – August 23, 2017: Protecting Covered Defense Information (CDI) in the Cloud*
- *#4 – September 13, 2017: Strategies to Minimize Business Impacts of DFARS 7012*
- *#5 – July 18, 2018 Primer: Performing Streamlined NIST 800-171A Assessments*
- *#6 – September 5, 2018: How Changes in DFARS Cybersecurity Enforcement Can Impact Your DoD Business*
- *#7 – November 14, 2018: DFARS 7012 Cyber Incident Response Liabilities and Strategies*
- *#8 – February 6, 2019: Cybersecurity Trends for 2019 and their Impact on DoD Contracting*
- *#9 – April 17, 2019: Update on DoD Enforcement of DFARS 7012 Cybersecurity Compliance*
- *#10 July 17, 2019: Upcoming DFARS Cybersecurity Audits and 3rd Party Certifications: DCMA CPSR / NIST 800-171B / CMMC*
- **#11 – October 23, 2019: Cybersecurity Maturity Model Certification (CMMC) Update Featuring Katie Arrington, CISO OUSD A&S**

Presenters

- Katie Arrington

  Chief Information Security Officer, Office of the Under Secretary of Defense for Acquisition

- Larry Lieberman

  Cyber Evangelist, eResilience

Webinar Agenda

- Introduction
- CMMC Update by Katie Arrington, CISO OUSD (A&S)
- Summary and Conclusion
- Q&A

eresilience

EXPERTS IN ENCLAVES

Advanced DoD Cybersecurity Solutions (over 15 years)

NSA Trusted Integrator

Certified Cyber Risk and Solutions Experts

eResilience Outreach Efforts

- Educational Content for Past 10 CCC Webinars
- Next Webinar will discuss strategies to prepare for CMMC
  - Expected broadcast date TBD Mid-December
- Partnerships with Government and Industry
- Attendance at CMMC Listening Tours
- Recent eResilience CMMC Webinar August 7th
- Today's role is to facilitate, and to moderate Q&A
- Pleased to introduce Katie Arrington, CISO OUSD (A&S)

eresilience
EXPERTS IN ENCLAVES

Securing the DoD Supply Chain

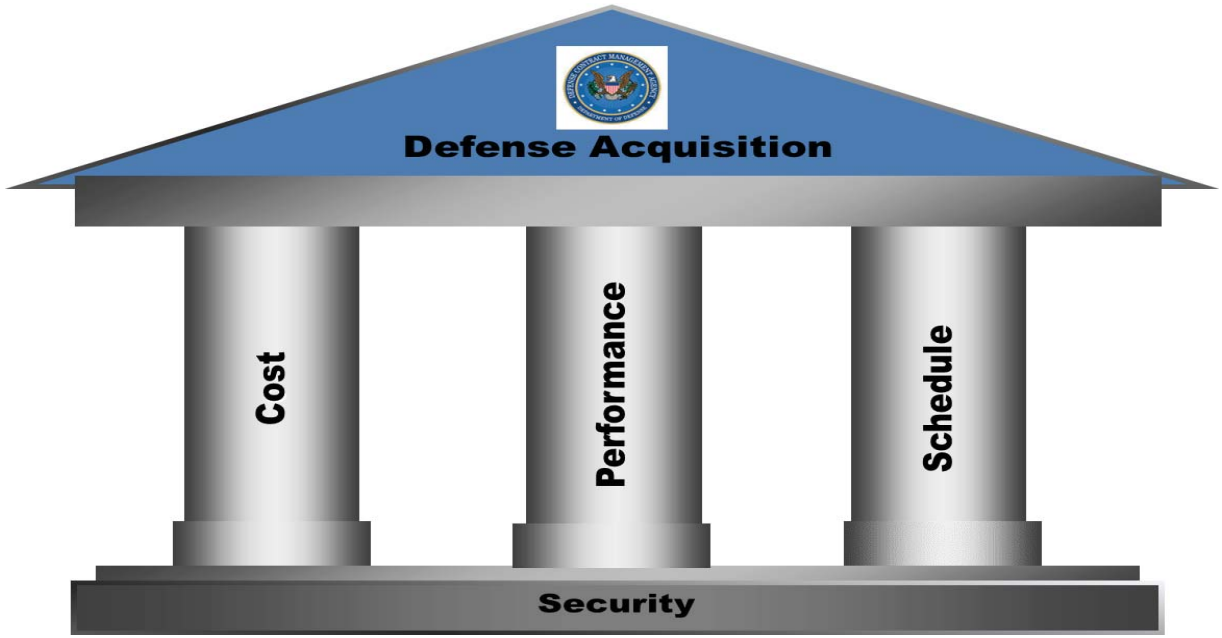
Cybersecurity Maturity Model Certification

Director Cybersecurity Maturity Model Certification

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)

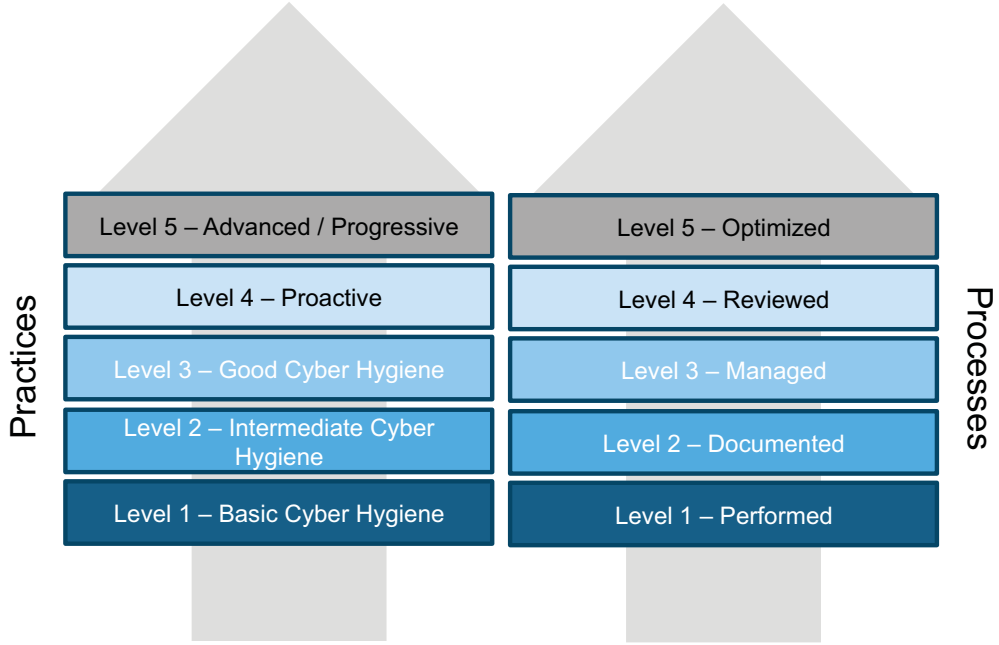
- **The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.**
- **The CMMC levels will range from basic hygiene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

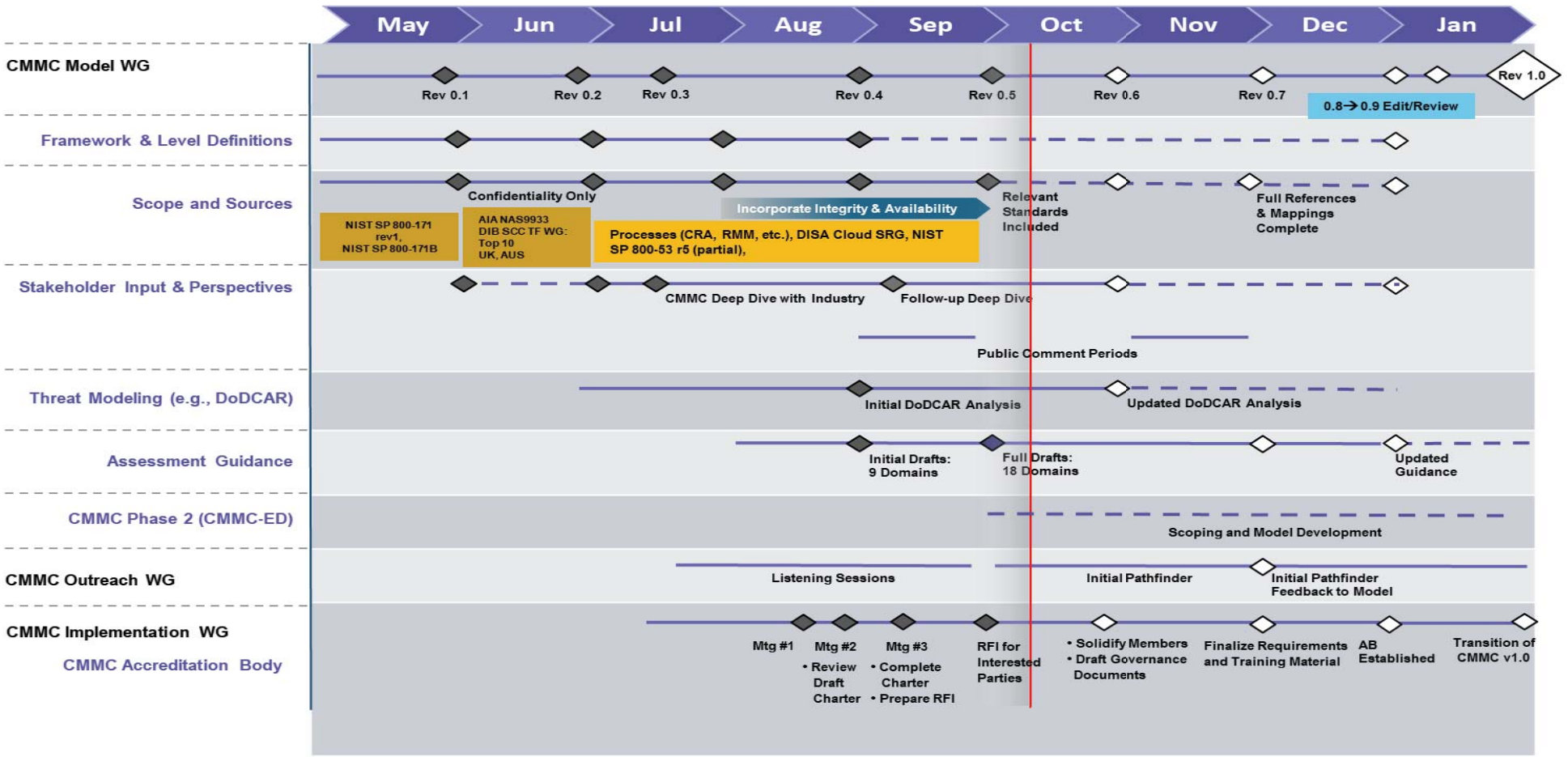
Capabilities assessed for Practice and Process maturity



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

Summary and Conclusion

- CMMC = dramatic impact on the Defense Industrial Base
- Self-Attestation model is coming to an end
- Enough hemorrhaging: Time to start implementing controls
- Don’t be caught off-guard… get suppliers prepared NOW!
- Check DoD‘s CMMC website regularly for updates
- Next Webinar will be about strategies to minimize impacts

eresilience
EXPERTS IN ENCLAVES

Questions & Answers

Reminders & Contact

- **Thanks** for attending!
- Please fill out **exit survey to request slides**
- **Next Webinar will be focused on strategies to prepare for CMMC**

Katie Arrington
https://www.acq.osd.mil/cmmc/

eResilience
Larry Lieberman
Office: 808-840-8580
info@eresilience.com

CYBER COLLABORATION CENTER

eresilience
EXPERTS IN ENCLAVES