"One Cause, One Voice"

Central Florida Chapter

NVSBC CMMC Panel Discussion

Introductions

1. NVSBC Welcome
2. Introduction of Panel Members
3. Pillars of Acquisition Program
4. CMMC Model Overview
5. CMMC Model Frameworks
6. CMMC Model Structure
7. CMMC ML Process Progression
8. CMMC ML Practice Progression
9. CMMC Practices Per Level
10. CMMC Model Source Counts
11. 5 Year Roll-Out Plan
12. Questions – Open forum Questions
13. Links

CELEBRATING 10 YEARS

Panelists

Dana Pekas
President
ISOP Solutions, Inc.

Steve Bullock
Director
ISOP Solutions, Inc.

Kyle Lai
Founder & CISO
KLC Consulting, LLC.

Amanda Gorski
CISO
SofiaITC, Inc.

Joshua Duvall
Managing Partner
Matross Edwards, LLC.

James Quilty
Board of Director
National Veteran Small Business Coalition

Jonathan Williams,
Partner
PilieroMazza, PLLC.

Pillars of Acquisition Program

CELEBRATING 10 YEARS

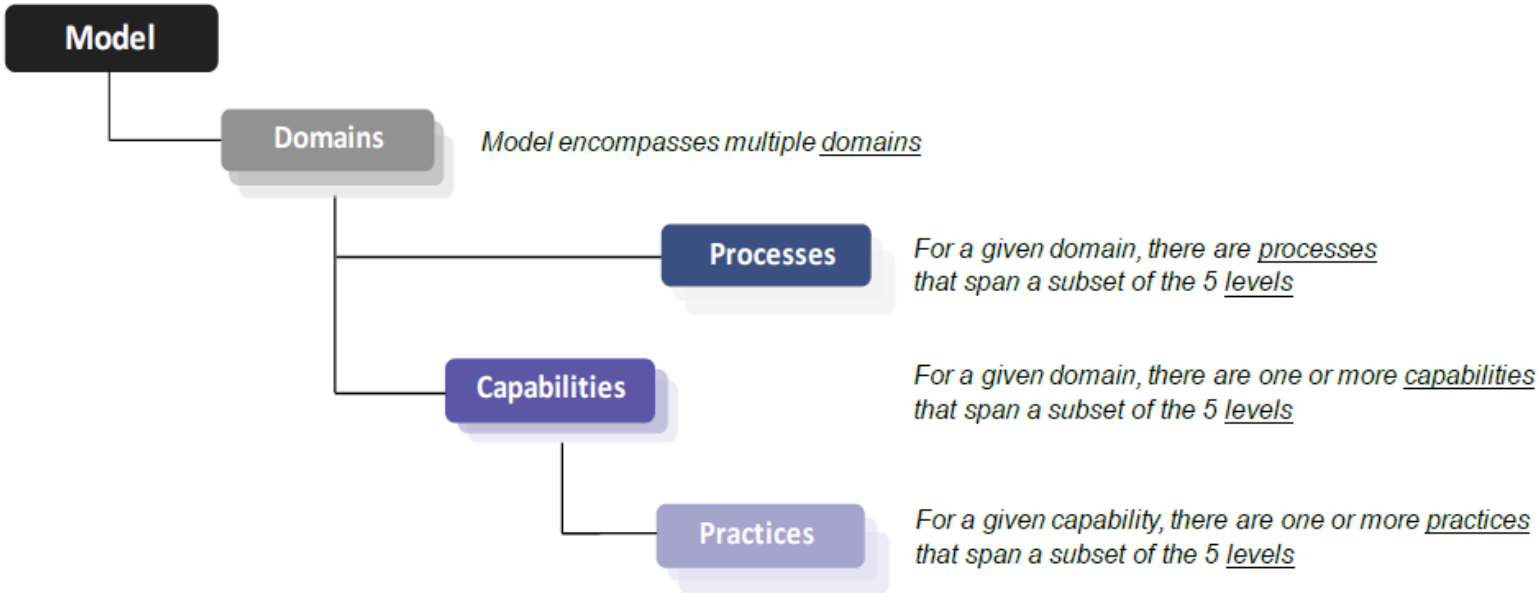
CMMC Model Overview

- **CMMC is a unified cybersecurity standard for future DoD acquisitions**
- **CMMC Model v1.0 encompasses the following:**
  - 17 capability domains; 43 capabilities
  - 5 processes across five levels to measure process maturity
  - 171 practices across five levels to measure technical capabilities

CMMC Model v1.0: Number of Practices and Processes Introduced at each Level

CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1

CMMC Model Framework



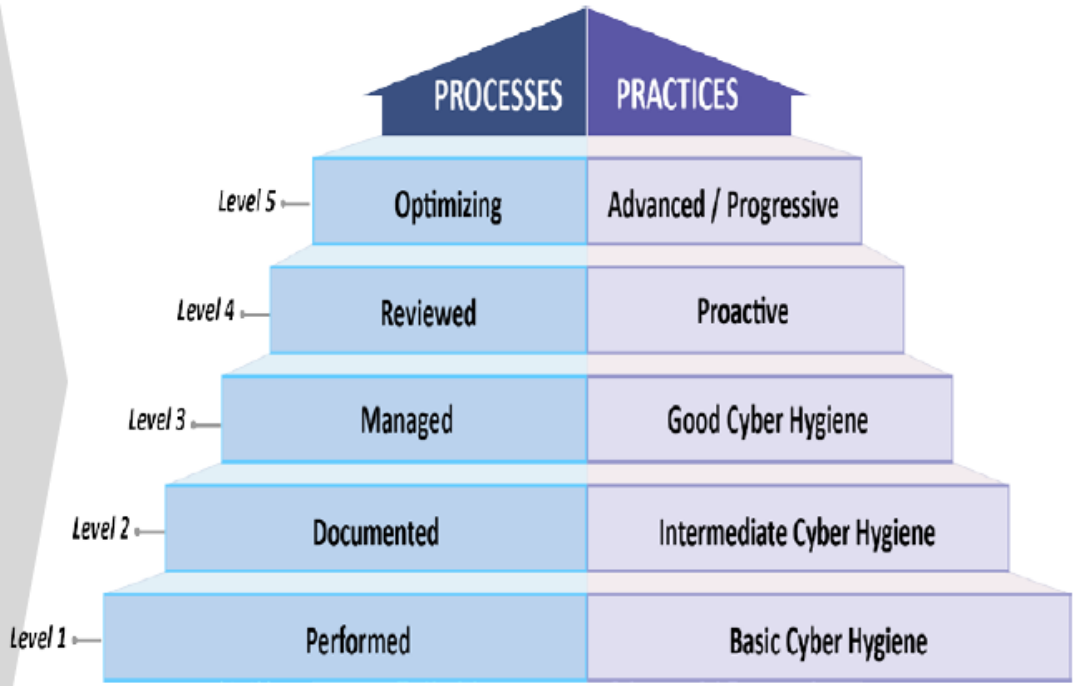
- **CMMC model framework organizes processes and cybersecurity best practices into a set of domains**
  - Process maturity or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely it is that:
    - An organization will continue to perform the activity – including under times of stress – and
    - The outcomes will be consistent, repeatable and of high quality.
  - Practices are activities performed at each level for the domain

CMMC Model Structure

17 Capability Domains (v1.0)

Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Model with 5 levels measures cybersecurity maturity

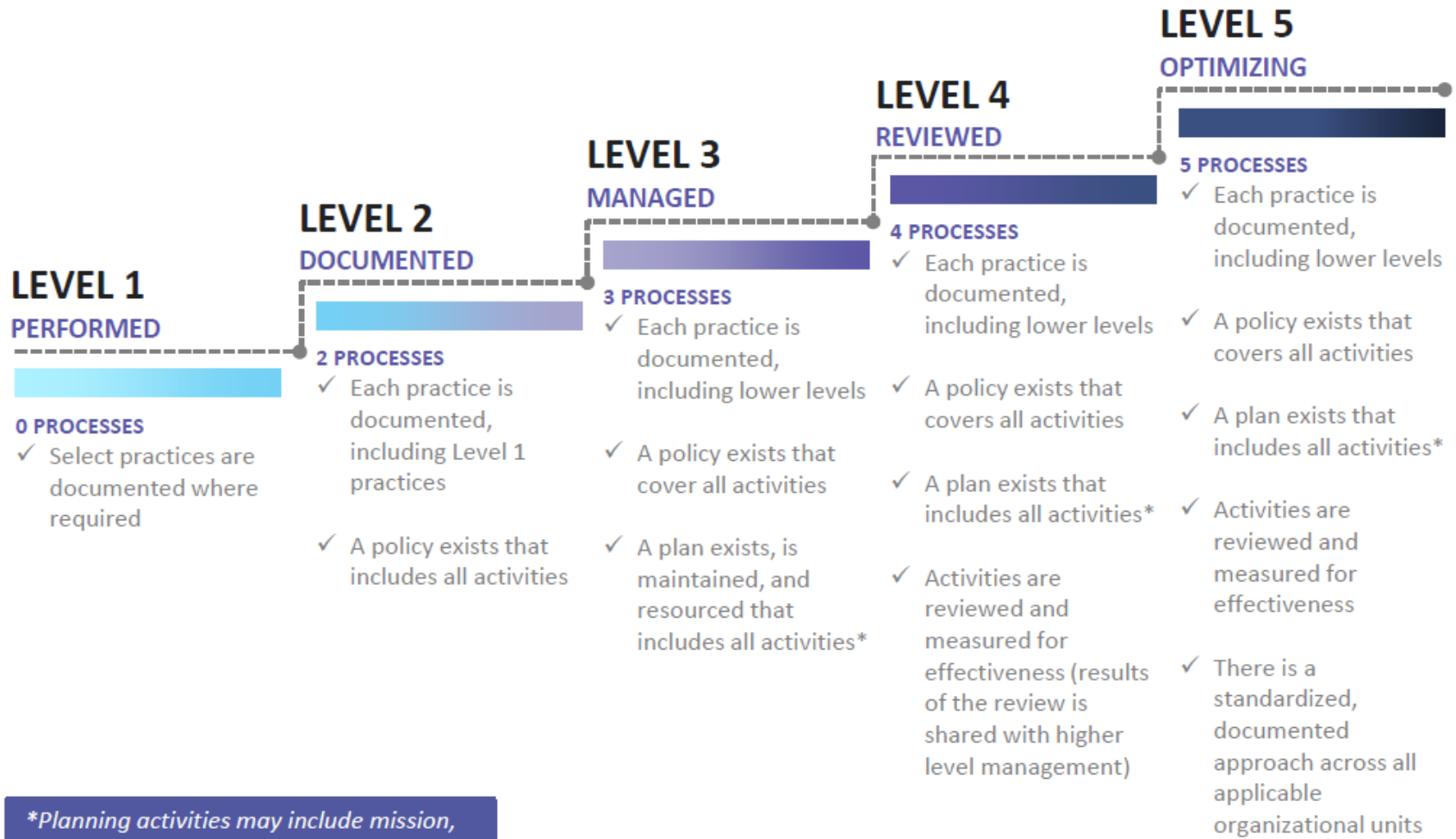


CELEBRATING 10 YEARS

CMMC Model Structure

CELEBRATING 10 YEARS

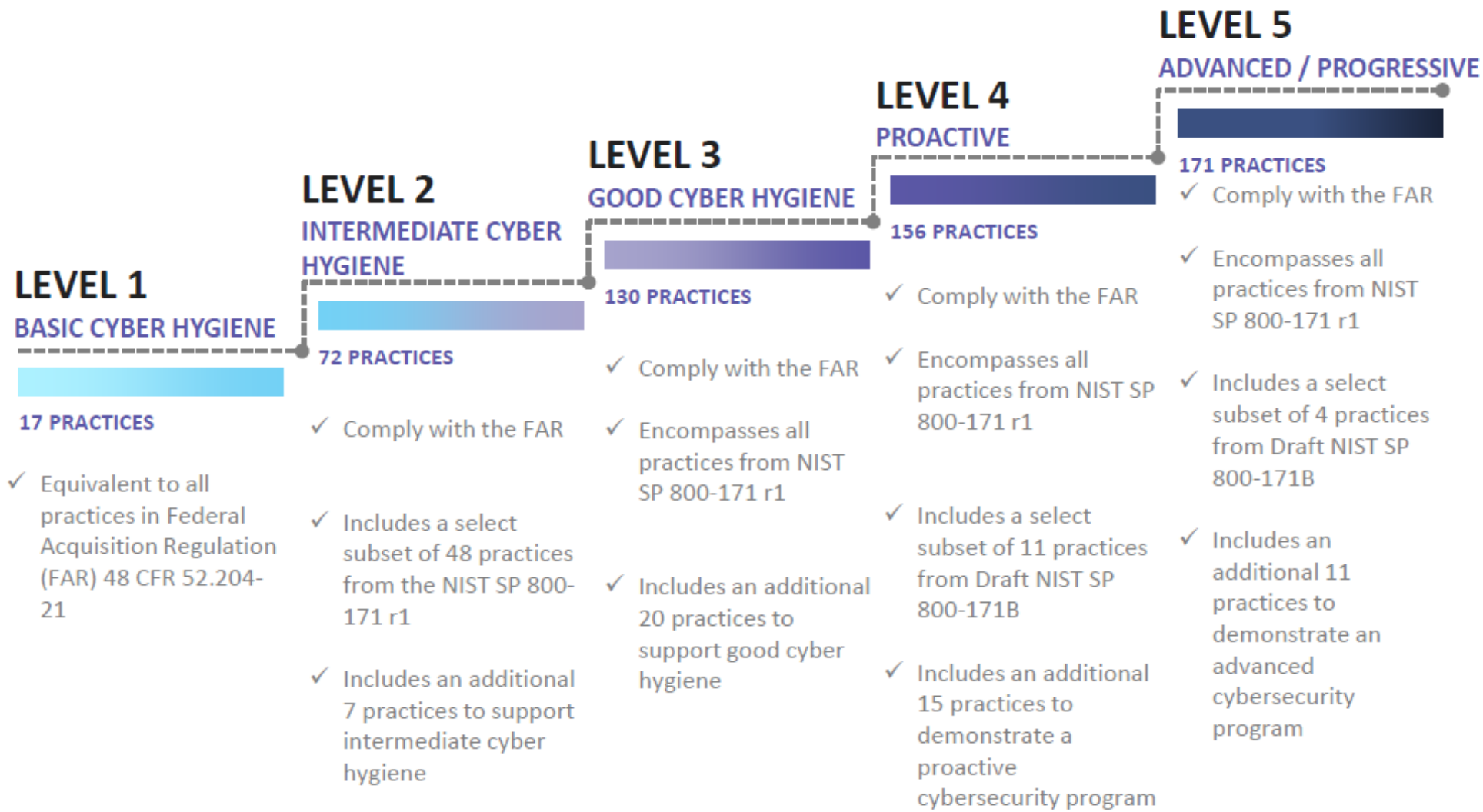
CMMC ML Process Progression



**Planning activities may include mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders*

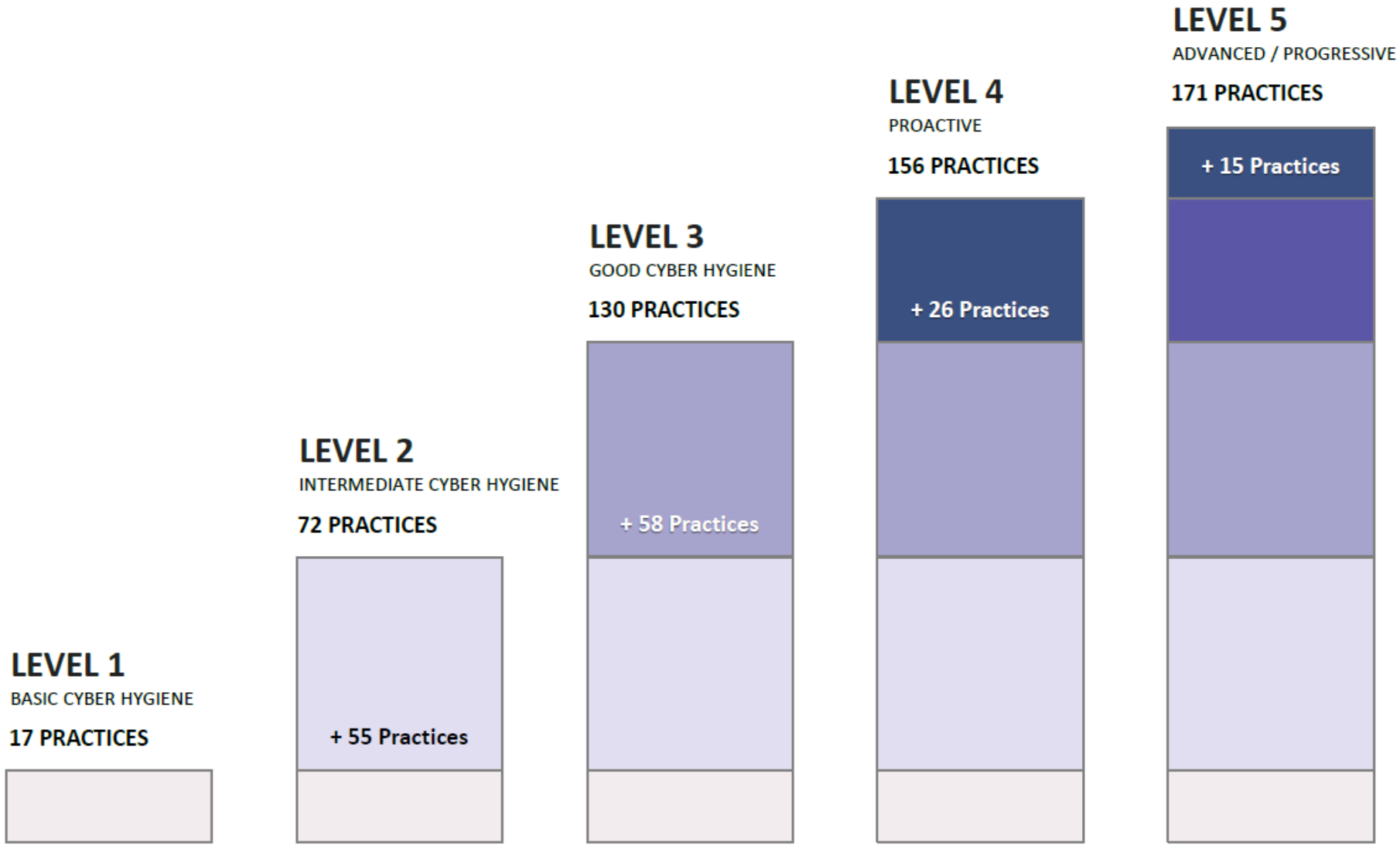
CELEBRATING 10 YEARS

CMMC ML Practice Progrssion



CELEBRATING 10 YEARS

CMMC Practices Per Level



CELEBRATING 10 YEARS

CMMC Model Source Counts

- **Model leverages multiple sources and references**
  - CMMC Level 1 only addresses practices from FAR Clause 52.204-21
  - CMMC Level 3 includes all of the practices from NIST SP 800-171r1 as well as others
  - CMMC Levels 4 and 5 incorporate a subset of the practices from Draft NIST SP 800-171B plus others
  - Additional sources, such as the UK Cyber Essentials and Australia Cyber Security Centre Essential Eight Maturity Model, were also considered and are referenced in the model

Draft CMMC Model v1.0: Number of Practices per Source

CMMC Level	Total Number Practices Introduced per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B **	Other
Level 1	17	15*	17*	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11

* Note: 15 safeguarding requirements from FAR clause 52.204-21 correspond to 17 security requirements from NIST SP 800-171r1, and in turn, 17 practices in CMMC

** Note: 18 enhanced security requirements from Draft NIST SP 800-171B have been excluded from CMMC Model v1.0

5 Year Roll-Out Plan

METHODICAL 5 YEAR ROLL-OUT

OUSD(A&S) is working with Services and Agencies to identify candidate programs for CMMC implementation during FY21-FY25 phased roll-out

Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement				
FY21	FY22	FY23	FY24	FY25
15	75	250	479	479

	Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement				
	FY21	FY22	FY23	FY24	FY25
Level 1	899	4,490	14,981	28,714	28,709
Level 2	149	749	2,497	4,786	4,785
Level 3	452	2,245	7,490	14,357	14,355
Level 4	0	8	16	24	28
Level 5	0	8	16	24	28
Total	1,500	7,500	25,000	47,905	47,905

½ of 1% of the DSC

All new DoD contracts will contain the CMMC requirement starting in FY26

CELEBRATING 10 YEARS

Questions

Open forum Questions

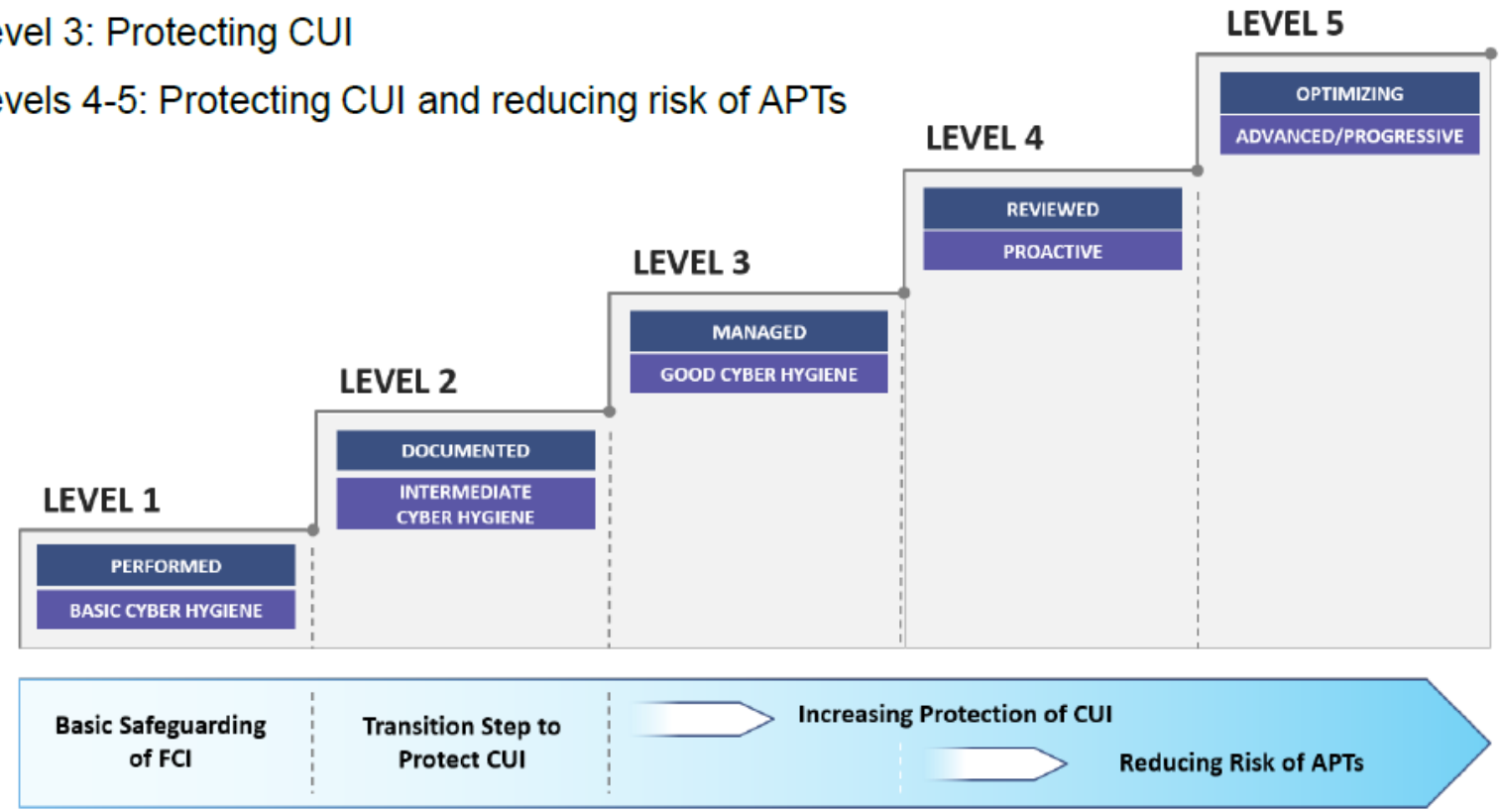
CELEBRATING 10 YEARS

Links

1. The Florida Defense Cybersecurity Training Program (F-DCTP) is working on establishing a grant program to help SMBs obtain their CMMC certifications. They are also going to each geographical region over the next year to explain their web portal for CMMS support and the grant program. https://floridajobs.org/business-growth-and-partnerships/military-community-programs/florida-defense-cybersecurity-training-program
2. Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification (CMMC) https://www.acq.osd.mil/cmmc/draft.html
3. FloridaMakes Receives Grant from the Florida Department of Economic Opportunity to Assist Florida Defense Contractors Comply with New Department of Defense Regulations https://www.floridamakes.com/news/news-releases/news/floridamakes-receives-grant-from-the-florida-department-of-economic-opportunity-to-assist-florida-defense-contractors-comply-with-new-department-of-defense-regulati.stml

CMMC Focus

- **CMMC establishes cybersecurity as a foundation for future DoD acquisitions**
- **CMMC levels align with the following focus:**
  - Level 1: Basic safeguarding of FCI
  - Level 2: Transition step to protect CUI
  - Level 3: Protecting CUI
  - Levels 4-5: Protecting CUI and reducing risk of APTs



CELEBRATING 10 YEARS

Process Maturity Level

PROCESS MATURITY (ML)

Note: The maturity processes are repeated in each domain. When being used in a specific domain, the first two characters of the identifier change from *'ML'* to the appropriate two-character domain identifier, while the rest of the identifier remains unchanged from what is shown below.

MATURITY CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
MC01 Improve [DOMAIN NAME] activities		ML.2.999 Establish a policy that includes [DOMAIN NAME]. • CERT RMM v1.2 GG2.GP1 subpractice 2	ML.3.997 Establish, maintain, and resource a plan that includes [DOMAIN NAME] • CERT RMM v1.2 GG2.GP2 • CERT RMM v1.2 GG2.GP3	ML.4.996 Review and measure [DOMAIN NAME] activities for effectiveness. • CERT RMM v1.2 GG2.GP8	ML.5.995 Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organizational units. • CERT RMM v1.2 GG3.GP1 • CERT RMM v1.2 GG3.GP2
		ML.2.998 Document the CMMC practices to implement the [DOMAIN NAME] policy. • CERT RMM v1.2 GG2.GP1 subpractice 2			

Practice – Personnel Security

PERSONNEL SECURITY (PS)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C028 Limit physical access	PE.1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. • FAR Clause 52.204-21 b.1.viii • NIST SP 800-171 Rev 1 3.10.1 • NIST CSF v1.1 PR.AC-2 • CERT RMM v1.2 KIM:SG4.SP2 • NIST SP 800-53 Rev 4 PE-2	PE.2.135 Protect and monitor the physical facility and support infrastructure for organizational systems. • NIST SP 800-171 Rev 1 3.10.2 • NIST CSF v1.1 PR.AC-2 • CERT RMM v1.2 KIM:SG4.SP2 • NIST SP 800-53 Rev 4 PE-6	PE.3.136 Enforce safeguarding measures for CUI at alternate work sites. • NIST SP 800-171 Rev 1 3.10.6 • CERT RMM v1.2 EC:SG2.SP1 • NIST SP 800-53 Rev 4 PE-17		
	PE.1.132 Escort visitors and monitor visitor activity. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 1 3.10.3 • CERT RMM v1.2 AM:SG1.SP1 • NIST SP 800-53 Rev 4 PE-3				
	PE.1.133 Maintain audit logs of physical access. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 1 3.10.4 • NIST SP 800-53 Rev 4 PE-3				
	PE.1.134 Control and manage physical access devices. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 1 3.10.5 • CERT RMM v1.2 KIM:SG4.SP2 • NIST SP 800-53 Rev 4 PE-3				

Practice – Audit & Accountability

AUDIT AND ACCOUNTABILITY (AU)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C007 Define audit requirements		AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions. • NIST SP 800-171 Rev 1 3.3.2 • CIS Controls v7.1 16.8, 16.9 • NIST CSF v1.1 DE.CM-1, DE.CM-3, DE.CM-7 • CERT RMM v1.2 MON:SG1.SP3 • NIST SP 800-53 Rev 4 AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	AU.3.045 Review and update logged events. • NIST SP 800-171 Rev 1 3.3.3 • CIS Controls v7.1 6.7 • CERT RMM v1.2 IMC:SG2.SP2 • NIST SP 800-53 Rev 4 AU-2(3)		
			AU.3.046 Alert in the event of an audit logging process failure. • NIST SP 800-171 Rev 1 3.3.4 • CIS Controls v7.1 6.7 • NIST SP 800-53 Rev 4 AU-5		
C008 Perform auditing		AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. • NIST SP 800-171 Rev 1 3.3.1 • CIS Controls v7.1 6.2 • NIST CSF v1.1. DE.CM-1, DE.CM-3, DE.CM-7 • CERT RMM v1.2 MON:SG2.SP3 • NIST SP 800-53 Rev 4 AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	AU.3.048 Collect audit information (e.g., logs) into one or more central repositories. • CMMC • CIS Controls v7.1 6.5 • CERT RMM v1.2 COMP:SG3.SP1 • NIST SP 800-53 Rev 4 AU-6(4)		AU.5.055 Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging. • CMMC • CIS Controls v7.1 6.2 • NIST SP 800-53 Rev 4 AU-12