Welcome ITPS!

ITPS Special Briefing
An Introduction to CMMC

Robert Smith
Systemwide IT Policy Director

Special Guests:
Baker Tilly

Speakers

Matt Gilbert

Principal

CISA, CRISC

matt.gilbert@bakertilly.com

Mike Cullen

Director

CISA, CISSP, CIPP/US

mike.cullen@bakertilly.com

Disclaimer

- The following sections are “best available” information/status on a rapidly evolving topic.
- This is **NOT** formal guidance. This information is intended for education, awareness and to start important conversations.
- In some cases rule making, legislation, intra-agency discussions, executive action or community feedback may change UC responsibilities.
- OGC may identify alternative approaches.
- The intent of this briefing is to inform, so that the possible impact of CMMC is considered when developing Location and Unit plans.
- **Baker Tilly** is our guest – they are not giving guidance.

Outline

- Introduction to CMMC
- CMMC at a Glance
- Legal Ramifications
- Location Impacts
- Discussion
- Questions
- Addition Material

Introduction to CMMC

Caveat: DoD and the CMMC Accreditation Board are clarifying and adapting as they go. Some positons are changing. There are open questions.

Third parties are speculating and contradicting DoD statements.

This material is "best available."

What is CMMC?

- Capability Maturity Model Certification (CMMC)
- In this case, as applied to cybersecurity.
- DoD says:
  - Security is foundational
    - Should not be traded along with cost, schedule, and performance moving forward.
  - Require enhanced protection within the supply chain.
  - DoD stakeholders
    - University Affiliated Research Centers (UARCs)
    - Federally Funded Research and Development Centers (FFRDC)
    - Industry
    - Collectively – Defense Industrial Base (DIB)

What is CMMC?

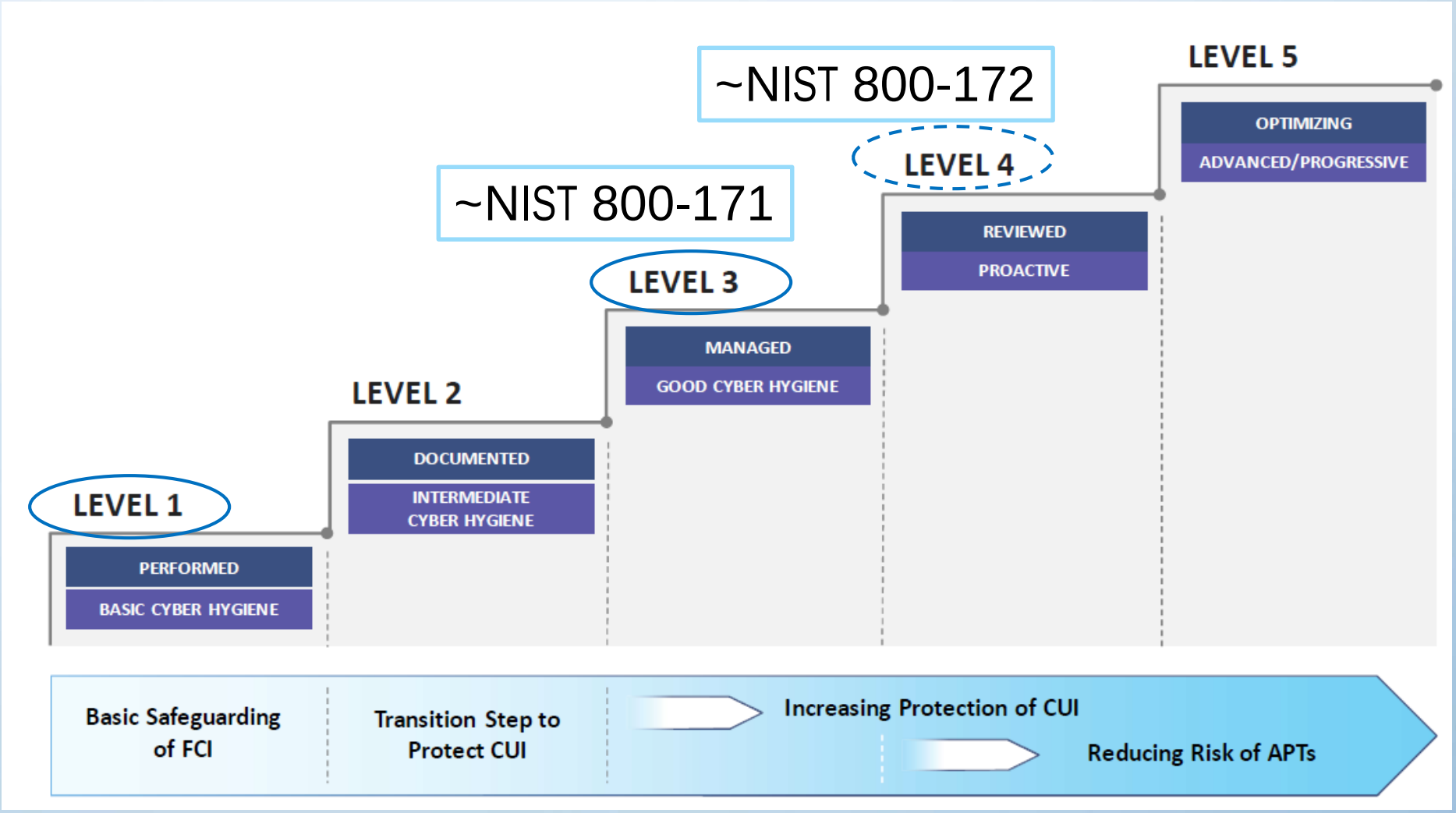
- A framework built on:
  - Maturity processes
  - Cybersecurity best practices
  - v1.02 is the current version, 1.0 released in January 2020
- Applies to:
  - Federal Contract Information (FCI)
  - Controlled Unclassified Information (CUI)
- Appears in:
  - Contracts
  - Grants are **NOT** part of the initial roll-out
- Certification lasts for 3 years.
- Certified by "**Certified Third-Party Assessor Organization**" – C3PAO
- Phased in over 5 years
  - 7,500 organizations certified in 2021

A fundamental shift

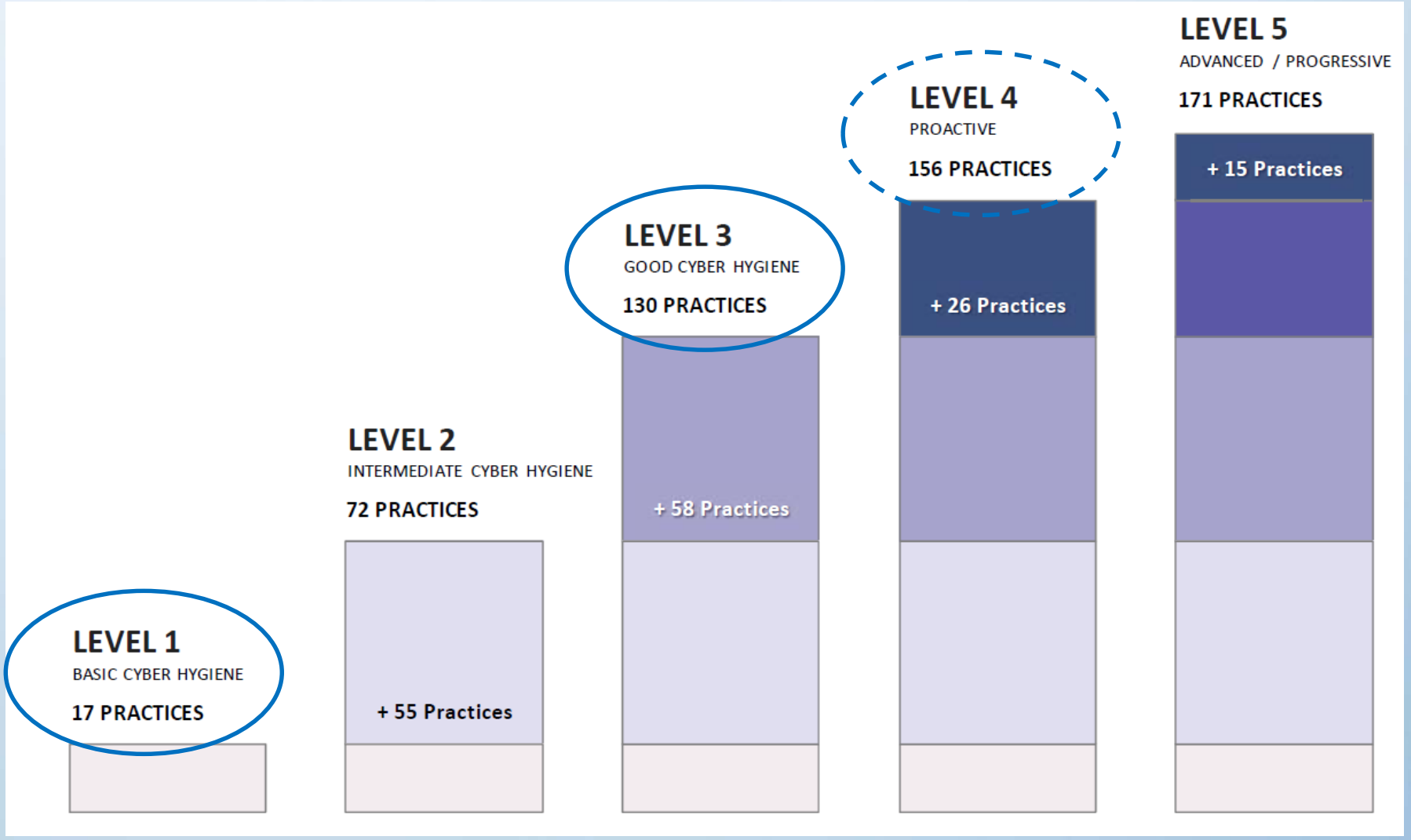
- Before
  - No perceived cyber impact to research funding.
  - Self certification, time to fix gaps, lax/non-existent enforcement, no consequences.
- 2021 and beyond
  - Cyber is a gate to seeking contracts/grants(?).
    - Starting November 2020 and progressing to 2026.
    - Rule making is not complete, no FAR clauses either
  - Certification required.
    - No POAMs (**P**lan **o**f **A**ction, **M**ilestones).
  - Stated objective to hold contractors and subcontractors liable/accountable.
    - Using contracts and the False Claims Act (FCA.)

CMMC Program at a Glance

CMMC Levels and Associated Focus



CMMC Practices (control groups) by Level

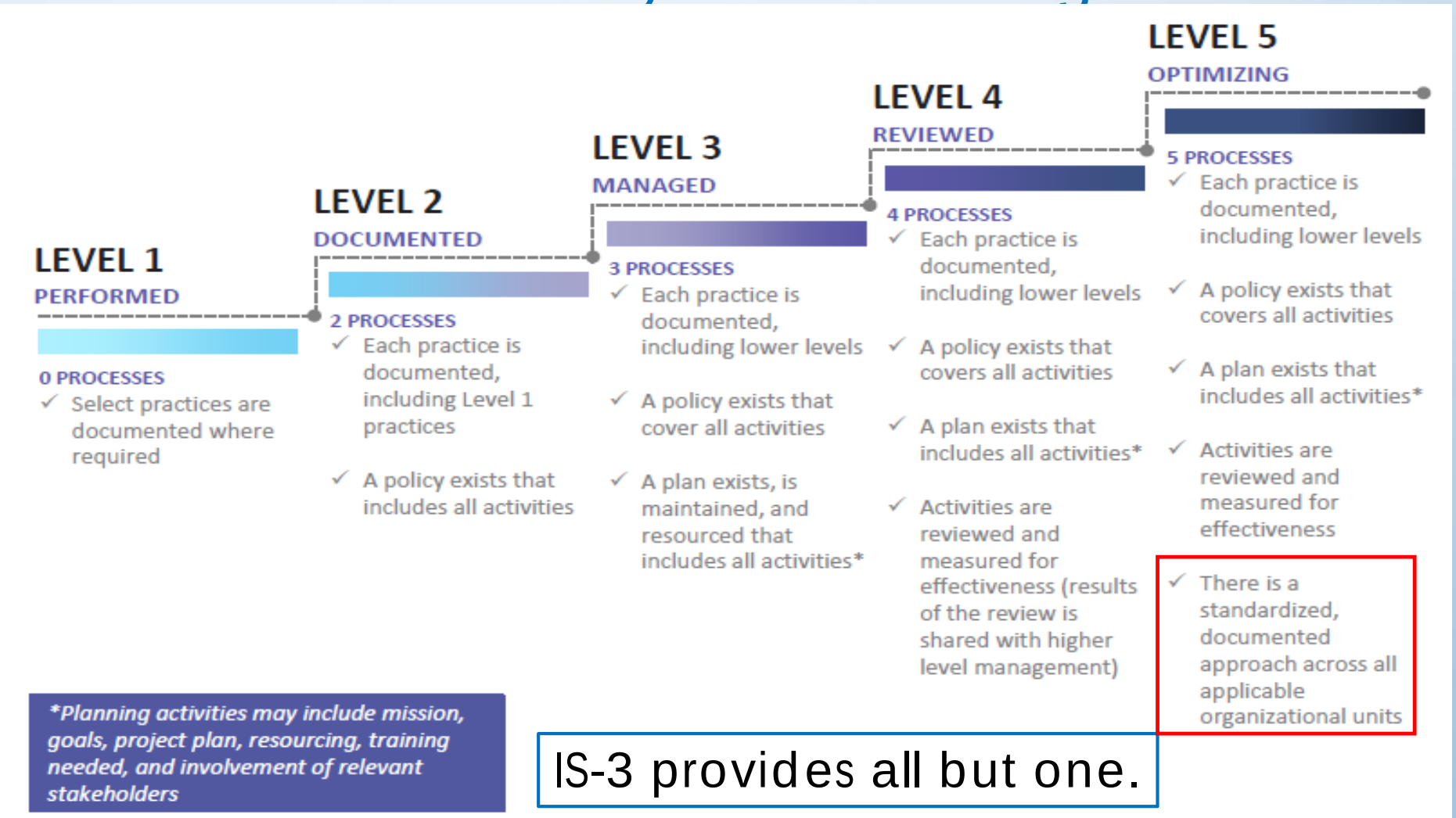


Practice example

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C002 Control internal system access	AC.1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 1 3.1.2 • CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11 • NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CERT RMM v1.2 TM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17	AC.2.007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 1 3.1.5 • CIS Controls v7.1 14.6 • NIST CSF v1.1 PR.AC-4 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 AC-6, AC-6(1), AC-6(5) • UK NCSC Cyber Essentials	AC.3.017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 1 3.1.4 • NIST CSF v1.1 PR.AC-4 • NIST SP 800-53 Rev 4 AC-5

One “Practice” may require many controls

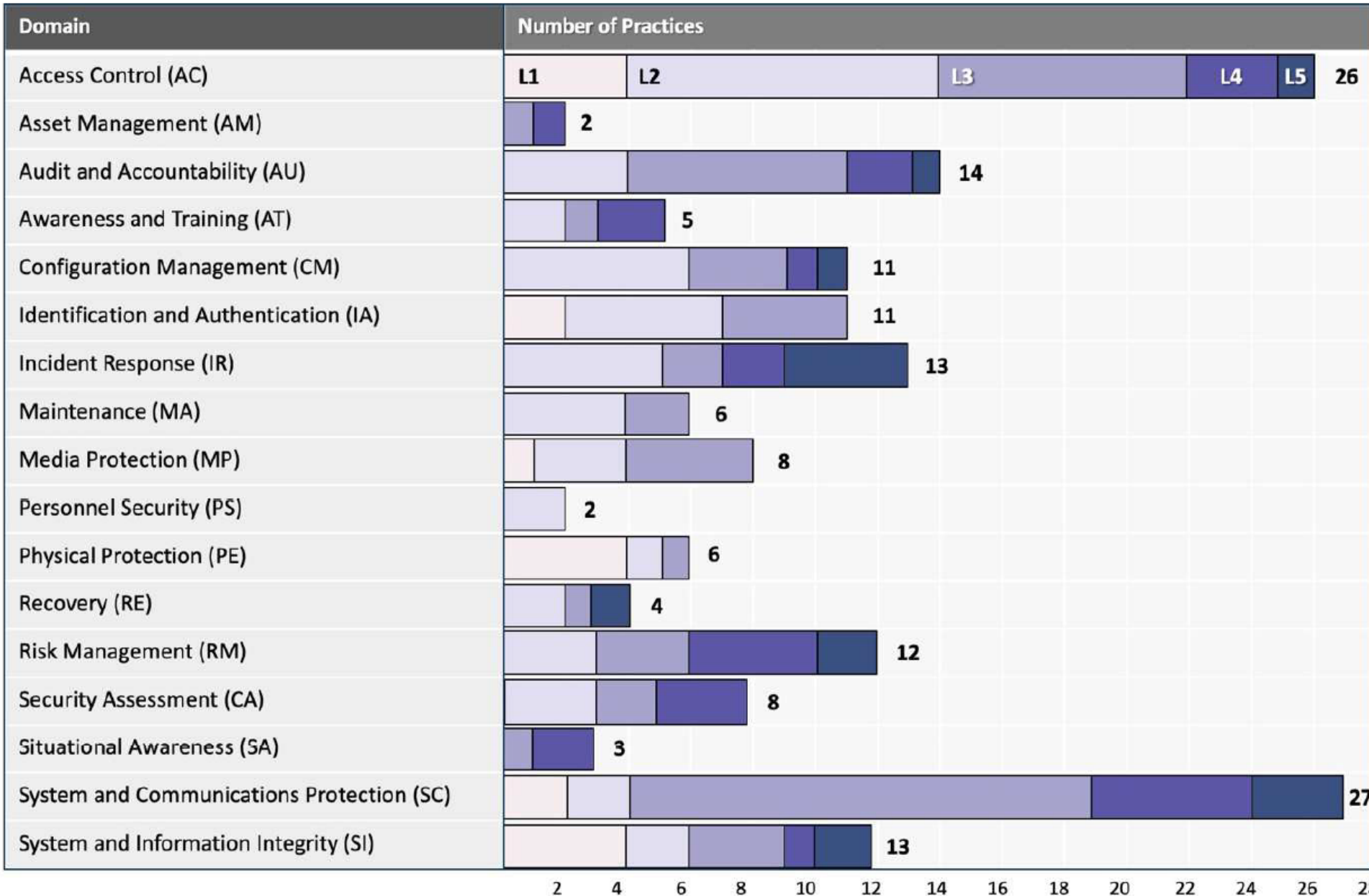
CMMC Maturity Process Progression



IS-3 provides all but one.

The 17 CMMC Domains

CMMC Domains and Practices



Why Higher Education Cares

A possible risk to research funding

- CMMC applies to all entities contracting (or subcontracting) with DoD.
- Current Controlled Unclassified Information (CUI) Defense Federal Acquisition Regulations (DFARs) clause is "based on trust."
  - CMMC is intended to add "a verification component."
  - CMMC goes further to establish requirements for every entity that contracts with the DoD.
    - Sometimes called the "Defense Industrial Base," or DIB (the DIB).
- 3rd party certification is required to receive an award.
- Implementing compliant certified programs may be costly and take years.

DoD Funding at UC (March 2020)

FY 2019 Department of Defense Grant and Contract Funding by Campus

Campus	Total Grants	Total Grant $	Total Contracts	Total Contract $	Total $
UCB	142	$36,019,276	21	$13,775,070	$49,794,346
UCD	68	$27,258,224	39	$6,744,425	$34,002,649
UCI	49	$13,245,682	35	$6,527,313	$19,772,995
LBNL	2	-$1,298	75	$8,225,870	$8,224,572
UCLA	180	$54,708,777	55	$22,520,696	$77,229,473
UCM	12	$1,840,751	0	$0	$1,840,751
UCR	41	$12,530,638	37	$5,625,533	$18,156,171
UCSD	230	$89,045,012	108	$29,791,531	$118,836,543
UCSF	50	$30,227,597	44	$36,353,220	$66,580,817
UCSB	61	$22,901,504	83	$32,766,628	$55,668,132
UCSC	29	$3,973,640	3	$739,176	$4,712,816
TOTAL	500	$163,069,462	864	$291,749,803	$454,819,265

Source: UCOP Research Office Tracking Database

How UC may see CMMC

- DoD → UC
  - DoD → UC n → UC n+1
- DoD → Prime → UC
  - DoD → Prime → Sub → UC
  - Etc.
- DoD → Some R1 → UC
- DoD → UC → Some R1
- Etc.

These can be complex if data is transferred or access shared.

Starting with <u>contracts</u> → Grants in the future.

Legal Ramifications

Legal Ramifications

- UC must ensure:
  - Systems used in connection with research are compliant with DFAR provisions, including CMMC.
  - Any statements of compliance, from RFP through litigation, must accurately reflect performance.

- Failure to comply can be legally actionable:
  - As fraud (FCA) - Recent settlements have exceeded $8M.
  - Suspension of and disqualification from future awards.
  - Breach of contract.

Location Impacts

Location preparedness

- Locations are challenged by CUI
  - Only two Locations have NIST 800-171 enclaves*:
    - San Diego Supercomputer Center and UC Davis
  - NIST 800-171 is similar to CMMC L3
    - We can learn from these experiences.
- Active UC CMMC programs
  - Only UCSD has a formal program with dates for CMMC.

* Enclaves are demonstrably separated environments with different features or capabilities.

What we think today

There are questions and unknowns

- CMMC will apply to each **Location** accepting DoD contracts
  - Certification requirements follow the data!
- However, there are questions and varying answers coming from different people.
  - Is there special treatment for research?
  - How to scope the environment and services?
- **The most important question relates to what is certified**:
  - The organization at L1and then the research lab at the CMMC Level of the data; or
  - Just the isolated and well segmented lab?
- No DoD intent to treat any organization differently regardless of:
  - Size.
  - Financial standing.
  - COVID-19 impact.

Discussion

Possible next steps

Clarity on enclaves vs. whole organization certification is key!

- Form a multi-Location workgroup
  - Office of Research, Research IT and Security
  - Focus on a needs assessment and proposed plans
- Assess the risk to research
  - Strategy: Build and leverage CMMC capability to be more competitive → increase research funding
- Prepare Location leadership
- Consider some systemwide cooperation
  - CMMC center of excellence
  - Shared enclaves and/or common architectures
  - Contracting for single UC wide C3PAO

Internal stakeholder concerns

- NIST 800-171 challenge generally, similar but separate (other federal agencies' CUI)
- CMMC investment
  - Audits/certification require ongoing resources (staff, budget, time).
  - Frictionless tools/resources to support research.
  - Enclaves are expensive to build and operate.
    - If certifications is by enclave, there could be a wide range – few to > 100 by Location
- Unified approach
  - Cross Location collaboration is difficult as priorities change, so ITLC commitment is key.
- Other agencies may follow.


fedscoop

TECH | DEFENSE | ACQUISITION | WATCH

ACQUISITION

CMMC requirements show up in GSA's STARS III contract

UC related groups tracking CMMC:

- Inside UC
  - ITSC
  - Vice Chancellors of Research
  - Research Policy Office
  - Research Compliance
  - OGC
  - Export Control Workgroup
  - UC Academic Computing Committee (Senate Subcommittee)
- Outside UC
  - EDUCAUSE
  - Council on Government Relations (COGR)
  - Association of American Universities (AAU)
  - Association of Public and Land-grant Universities (APLU)
  - Higher Education/DIB focused law firms

Scoping mistakes

bakertilly
now, for tomorrow.

- What CMMC level
- Where is the FCI and CUI
- What assets impacted
- How to handle my third party providers
- Where is the boundary
- How to leverage creative scope options
- How to demonstrate compliance

Proactive steps to take now

bakertilly
now, for tomorrow.

Inventory all existing DoD work (e.g., contracts, grants) at the institution and determine existing cybersecurity requirements for that work

Inventory all systems at the institution that collect, store and process data related to DoD work, both FCI and CUI

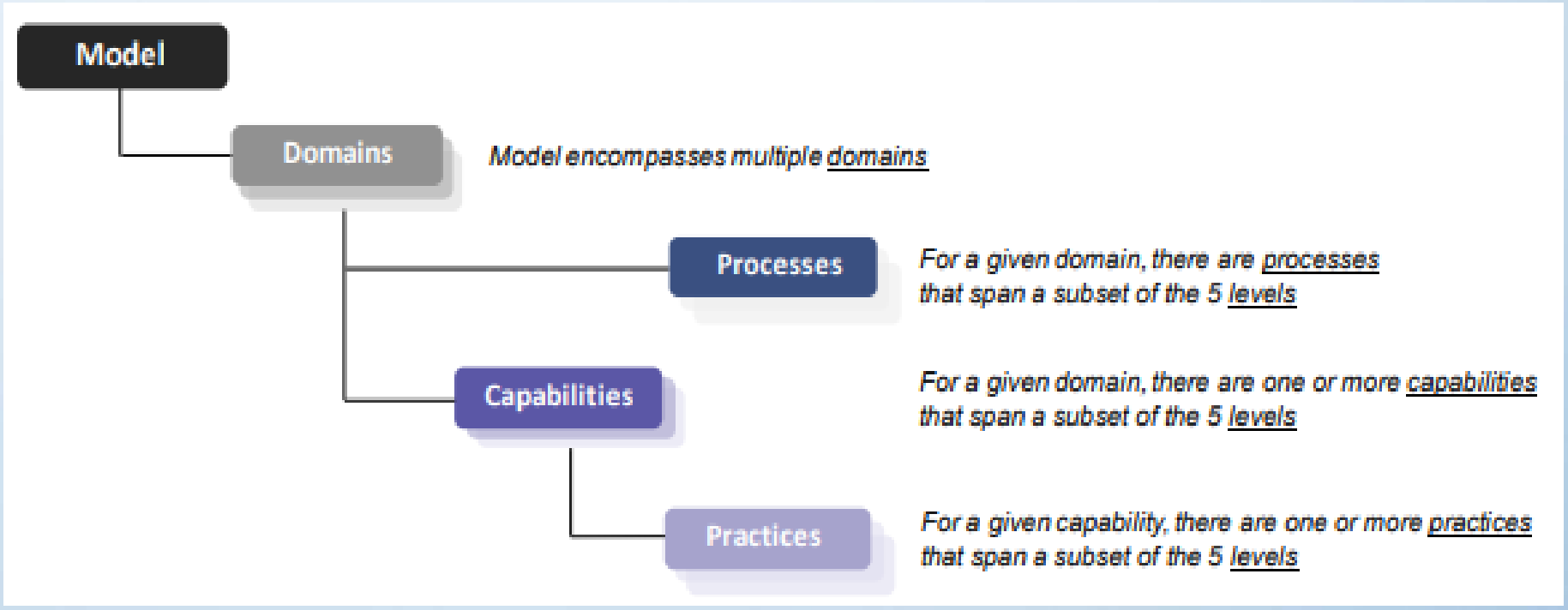
Conduct a readiness assessment, using a third party, on your ability to meet the CMMC practices based on the existing DoD work and systems

Create a remediation plan to address any identified gaps, then refine your scoping and implement new practices

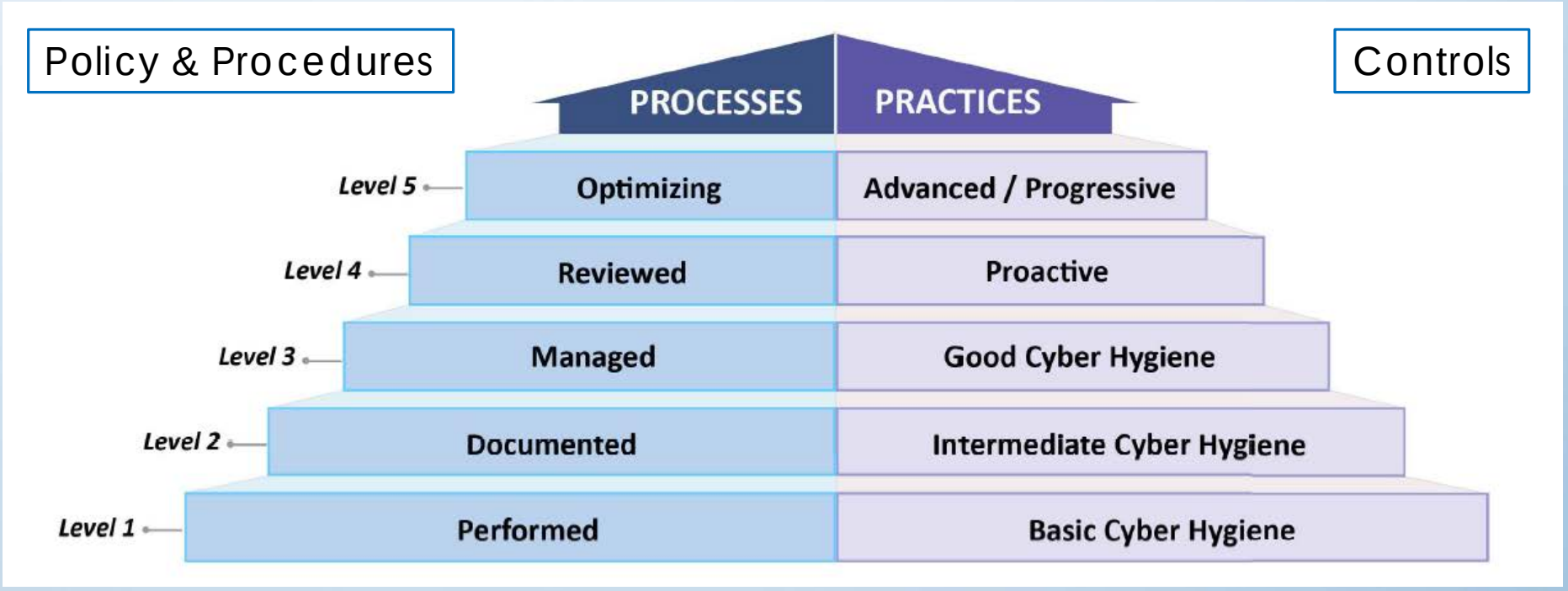
Questions?

Additional Material

CMMC Hierarchical View



CMMC Structure



Certification Roadmap in 10 Steps