CACI Supplier Series

Understanding the CMMC Requirements

CACI
EVER VIGILANT

EXPERTISE and **TECHNOLOGY** For National Security

DISCLAIMER

This presentation is for informational purposes and intended to assist CACI Suppliers understand current and emerging cyber security requirements.

CACI does not endorse or recommend any one vendor. When in doubt, Suppliers should seek qualified support to ensure regulatory/contractual requirements are properly implemented.

Presentation Overview

- CACI cybersecurity supplier expectations
- Unclassified cybersecurity compliance overview
- Supplier resources
- FAQ's
- Q&A (All)

Your Presenters

Amanda Christian | SVP, Subcontracts and Procurement | amchristian@caci.com

Leads the Subcontracts and Procurement Department at CACI that purchases goods and services with an approximate spend of $2B per year.

President Elect - *National Contract Management Association (NCMA)*

Dr. Joanna Patterson | Executive Director, Risk Management | SupplierComplianceCS@caci.com

Enterprise Risk Management, Supply Chain Risk Management, Cyber SCRM, Counterfeit Parts, Hazardous Materials, Business Continuity

Led successful ML5 appraisals for CMMI for Services and Development under the v1.3 model. Participated in a CMMI for Development appraisal for v2.0 – CMMI Associate, Six Sigma Black Belt

Successful external certifications - ISO 27001, ISO 9001, ISO 28000 (retired), and ISO 20000

CACI SB Profile

Active Subcontractors	%
Small	76%
w/Socioeconomic Status	
WOSB	17%
SDB	15%
HUBZone	4%
VOSB	21%
SDVOSB	13%
Large	**24%**
Total	**100%**

Supplier Expectations

CACI
EVER VIGILANT

Work proactively to understand and meet CMMC standards, so we can continue to partner and grow business.

Provide documentation in P2P Supplier Portal to ensure the required CMMC levels are obtained for the work solicited.

Maintain compliance with DFARS 7012 and CMMC level initially achieved. Enhance the CMMC level as business needs require.

Unclassified Compliance Tracks

CACI
EVER VIGILANT

FAR 52.204-21 - - - - - - - - - - - - - - -

- ✓ Basic safeguarding
- ✓ Not specific to CUI
- ✓ Introduced - 2016
- ✓ Supplier flow down
- ✓ No attestation / audits

DFARS 252.204-7012 - - - -

- ✓ Specific to DoD
- ✓ Introduced - 2017
- ✓ Specific to CUI handling
- ✓ Subject to DCMA audits
- ✓ 110 security controls
- ✓ Supplier flow down
- ✓ POA&M allowed
- ✓ Attestations / SPRS / Contract

Annex 16 - - - -

- ✓ Specific to Navy "critical" programs
- ✓ Adds additional security controls
- ✓ Adds onsite SSP review
- ✓ Enhanced forensics requirements
- ✓ 5% penalty - deficiency notice

Unclassified Compliance Tracks

CACI
EVER VIGILANT

NIST 800-172

- ✓ Replaces Annex 16
- ✓ Per DoD 1-2% of contracts
- ✓ Not just for the Navy – all DoD critical programs – high value assets
- ✓ 32 enhanced security controls
- ✓ Very labor intensive
- ✓ Pending release

CMMC

- ✓ Specific to DoD (currently)
- ✓ Five maturity levels
- ✓ Commercial
- ✓ Not specific to CUI
- ✓ Can be edited at will (new controls)

CMMC – A Deeper Dive

CACI
EVER VIGILANT

- Commercial certification created **for** the DoD
  - Carnegie Mellon University, Johns Hopkins APL
- Final version released January 2020
- Not limited to projects handling CUI
  - Federal Contract Information = FCI
- Multi-level certification meant to measure cyber posture
- Phased roll-out starting December 2020
  - Year 1 = 15 contracts / Year 2 = 75 contracts / Year 3 = 250 contracts / Year 4 = 325 contracts / Year 5 = 475 contracts

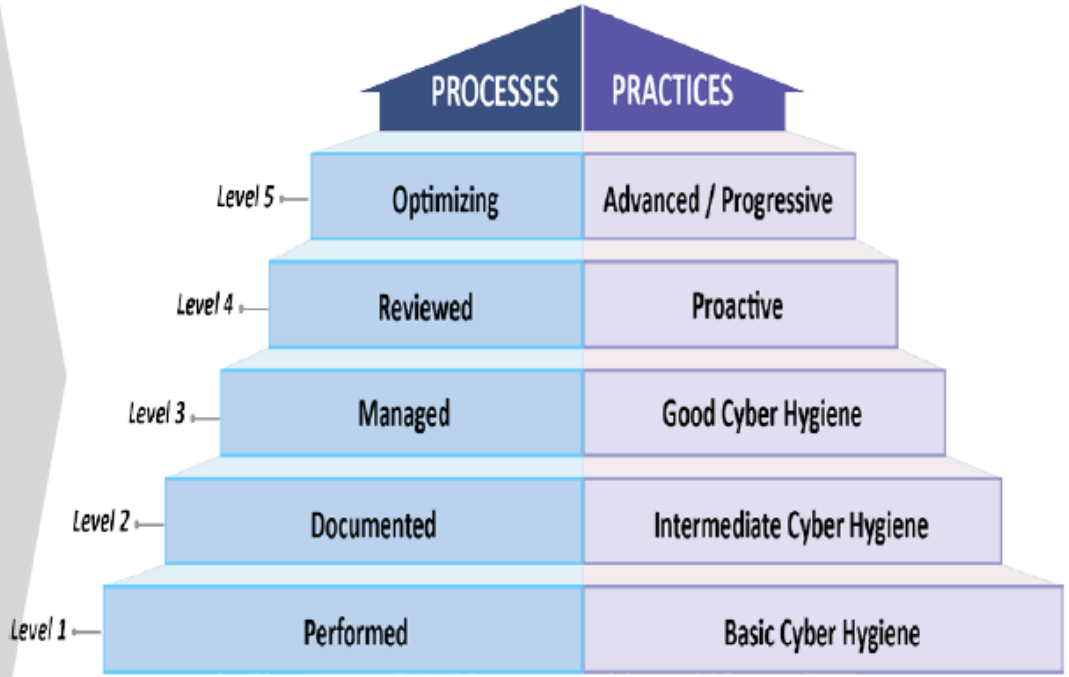
CMMC – A Deeper Dive

CACI
EVER VIGILANT

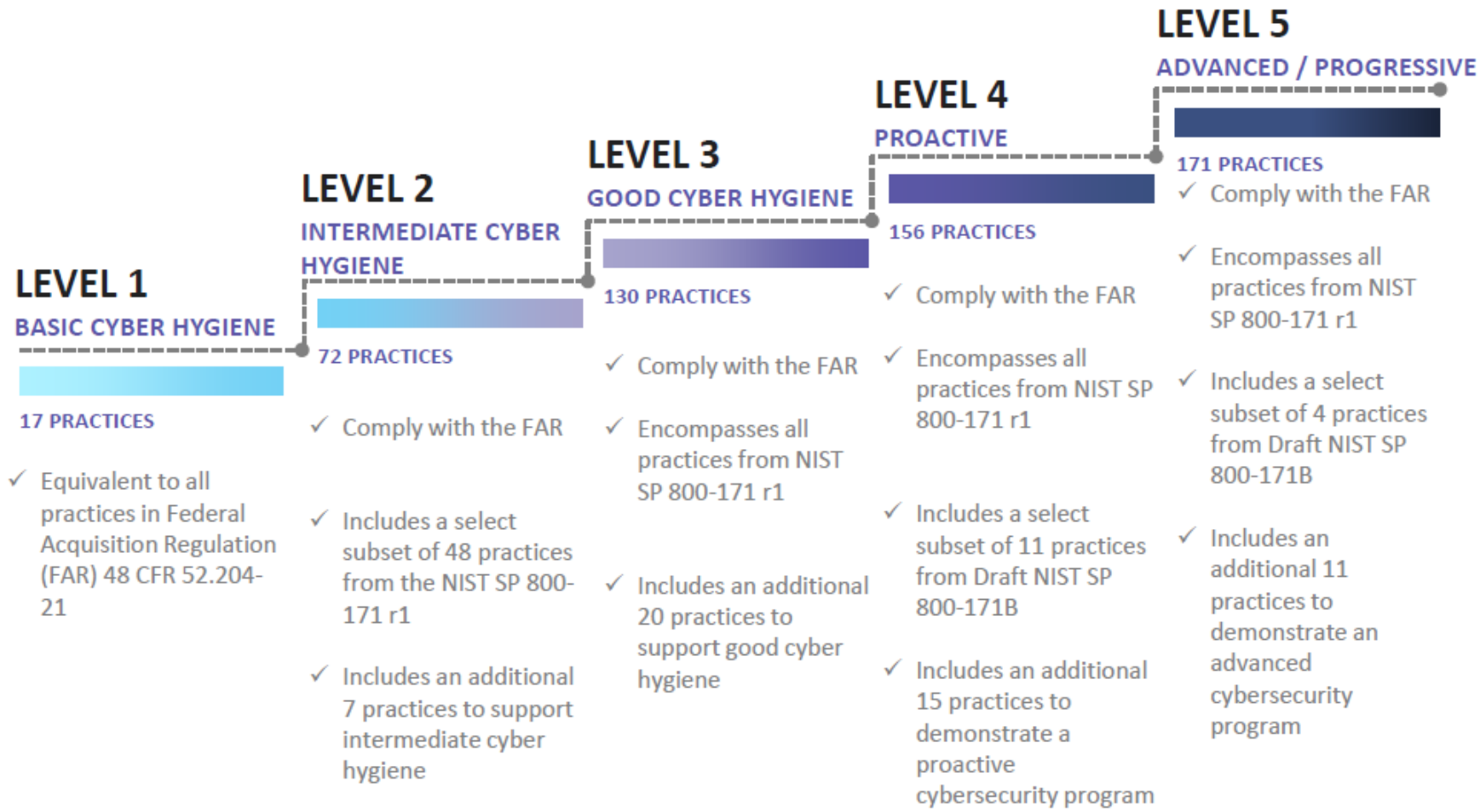
17 Capability Domains (v1.0)

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



CMMC – A Deeper Dive



Considerations

- The CMMC AB / DoD has not released how “scoping” will take place
  - The DoD has said, several times, that it is very likely that a company will hold several certifications based on location/project needs
- Little time between RFP and award for a SB to “level up” if needed
- No plan of action and milestones (POA&M) allowed
- No one size fits all categorization model for planning
- Truly up for interpretation by the person writing the RFP
- It is important to think about your current subcontractor partners and how this may impact them

Recent Regulatory Updates

CACI
EVER VIGILANT

As of 11/30/2020

- **252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements**
  - Offerors shall have a current assessment (3 years or less (less time can be specified in the solicitation)
  - Offerors shall verify score in DoD SPRS Supplier Performance Risk System for basic, medium and high assessments
    - If no assessment score, then an offeror can email a self-assessed basic assessment to navy.mil email address
- **252.204-7020 NIST SP 800-171 DoD Assessment Requirements** *Assessment and Subcontractor language duplicated from 7019 & 7020 or vice versa*
  - Clause applicable to covered contractor information systems that are required to comply with the 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting & NIST 800-171, of this contract.
  - The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment
- **252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement**
  - Contractor ensures that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor

Recommended Next Steps

CACI
EVER VIGILANT

- If you are handling CUI – ensure you are compliant with the DFARS 252.204-7012
- Enter your basic assessment score in SPRS
- Review your contracts to assess which ones call out CUI (or CUI categories)
  - This will help "estimate" potential CMMC levels
- Familiarize yourself with the CMMC
- Review the CMMC and assess any gaps that you may have up to level 3
  - What do you need to budget for going forward?
  - What policies/procedures are you lacking?
  - Create a project plan to identify timelines to remediate big issues
  - Talk to your partners/customers – gauge their knowledge of the CMMC and what level they may be considering

Small Business Resources

DFARS 252.204-7012	*NDIA CMMC Resources*
NIST 800-171	*NIST Small Business Cyber Corner*
CMMC Model	*NDISAC Cyber Assist*
CMMC AB	*NARA CUI Categories*
NIST 800-172	*SPRS*
DCMA Self-Assessment	*DFARS Case 2019-D041*
Project Spectrum	*NIST Manufacturing Extension Partnership*
Annex 16	*FAR 52.204-21*

FAQ

- *I heard I have until 2025 to get CMMC certified…*
  - The CMMC will be a phased roll out that goes through 2025. That does not mean your company will not have to obtain a CMMC certification prior to that date. Your company will need to be certified to the required level of each contract you work on that contains the requirement. Realistically, that could be 2021.
- *I have ISO 27001, that should guarantee me CMMC ML 3….*
  - ISO 27001 is a valuable information security framework, but it does not include all the controls in NIST 800-171 or CMMC ML 3. Companies should perform a gap analysis to identify controls that may still need to be implemented or enhanced.
- *Some Primes are telling me I have to a CMMC ML 3, even though there are no contracts released with the CMMC requirement…*
  - Some Primes are reviewing their current contracts and assessing what data their subs handle and making assumptions of potential CMMC maturity level requirements. The DoD did state that CMMC ML 3 is the minimum level needed to handle CUI, so if you are handling CUI it can reasonably assumed you will need a CMMC ML 3.

FAQ

- *I do not use my information system to store or transmit any Government data. I only use Government or CACI assets. This does not apply to me.*
  - There are ways to manage data access for non-compliant companies with the DFARS 252.204-7012. This typically involves issuing a CACI managed, or Government managed asset that is compliant with the DFARS 252.204-7012. This is a short-term solution until the supplier is compliant. In the future, the Government has indicated all suppliers must have, at minimum, a CMMC ML 1. CACI cannot waive these requirements.
- *I provide commercial off the shelf items (COTS) – does this apply to me?*
  - No – definition of COTS
- *Is this flowed down for purchases below the micro-threshold?*
  - No – definition of micro-threshold
- *Can CACI assist me with my DFARS 252.204-7012?*
  - Unfortunately, no. Each information system is unique.
- *Can CACI assist me with SPRS access?*
  - Unfortunately, no. Please contact the SPRS helpdesk: webptsmh@navy.mil or (207) 438-1690

SPRS Info

- *What is my location code?*
  - Contractors should use their CAGE code
  - SPRS Guide Link

Phone:

Commercial: (207) 438-1690
DSN: 684-1690

Email: webptsmh@navy.mil

Questions?
SupplierComplianceCS@caci.com

CACI
EVER VIGILANT

CORPORATE HEADQUARTERS
CACI International Inc
1100 North Glebe Road
Arlington, VA 22201
(703) 841-7800

www.caci.com