# Cybersecurity Maturity Model Certification Guidance

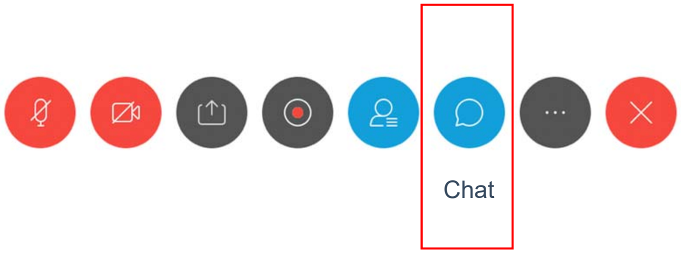
Kevin W. Cornwell, CPA, CISA, CITP
Associate Director of Technology Consulting

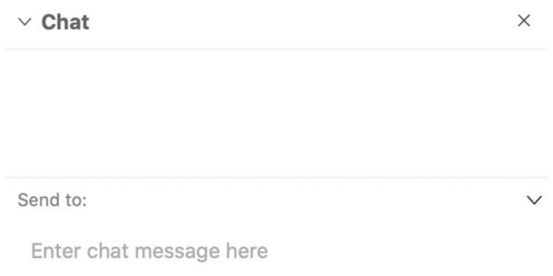
DEANDORTON

# Welcome!

## Questions?

- Use the Chat window throughout the presentation – questions will be addressed at the end





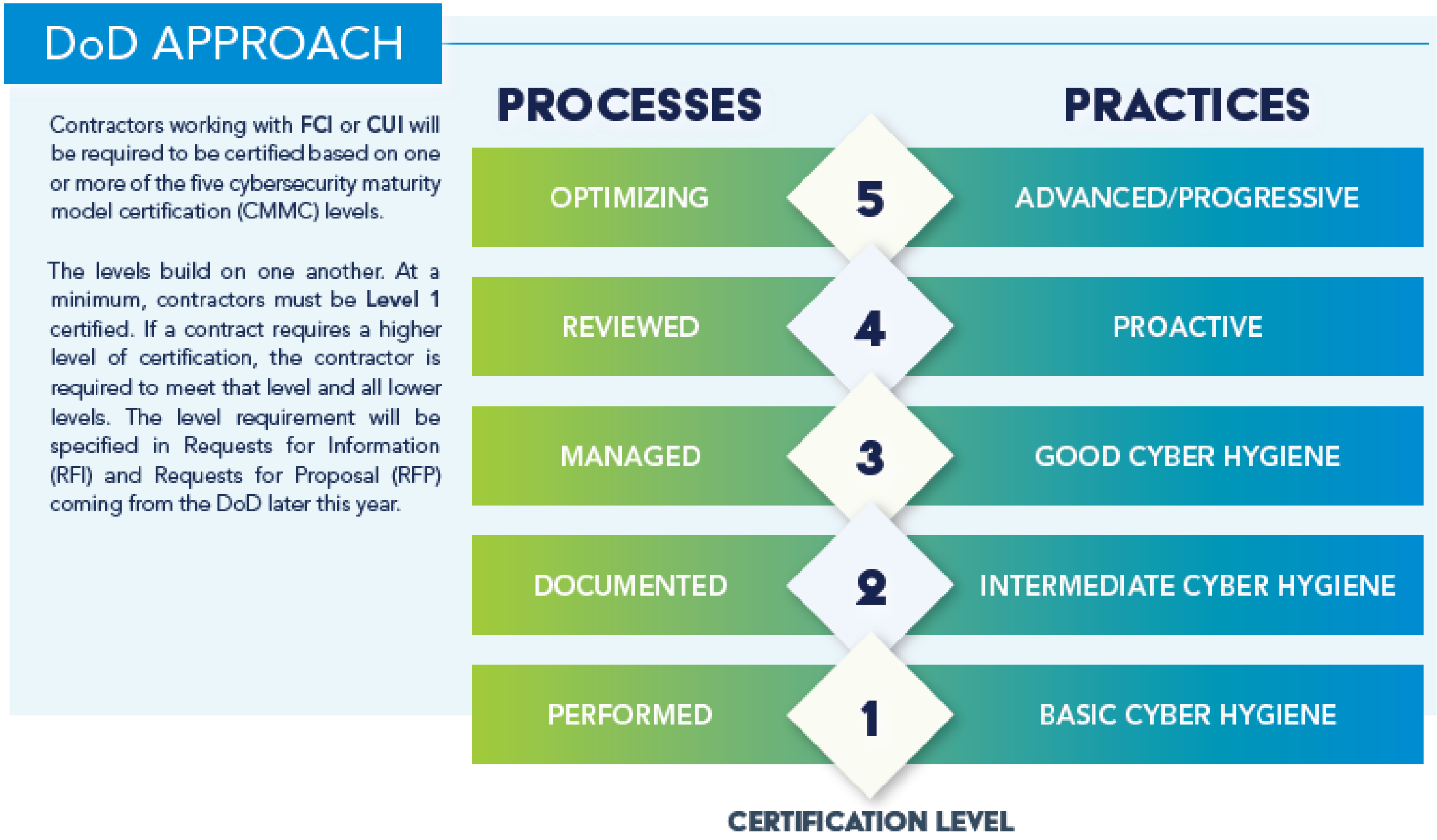
# Agenda

1. Background
2. Explanation of the certification process
3. Timeline
4. Recent developments
5. What can you do?

# Background

- NIST 800-171 not a one size fits all framework
- CMMC is NIST 800-171 segmented into levels*
- CMMC Objectives
  - Protect CUI and FCI
  - Identify shell companies
- Every DoD control will have a CMMC level requirement
- Applies to
  - Prime contractors
  - First-tier subcontractors

# Levels



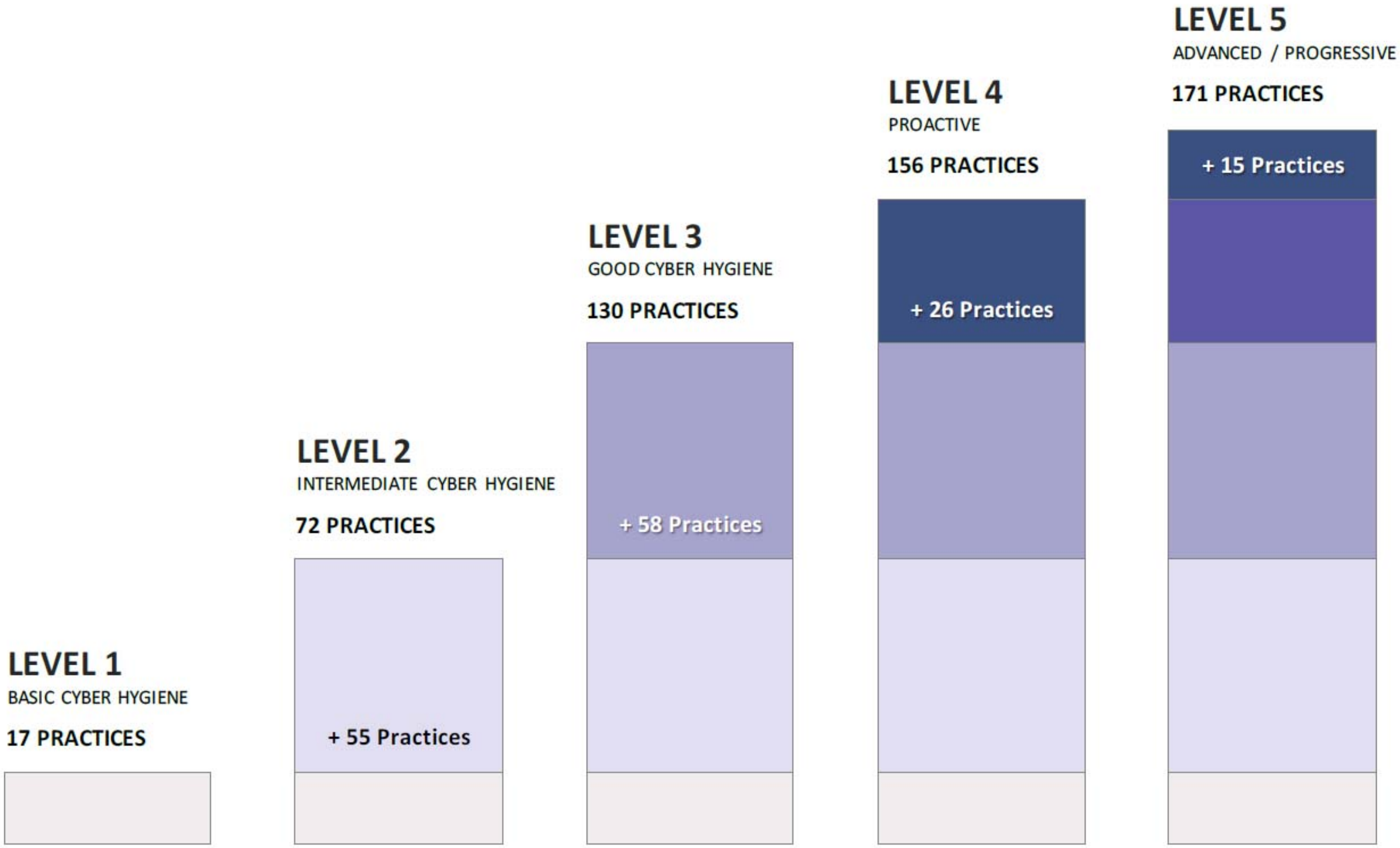
## DoD APPROACH

Contractors working with **FCI** or **CUI** will be required to be certified based on one or more of the five cybersecurity maturity model certification (CMMC) levels.

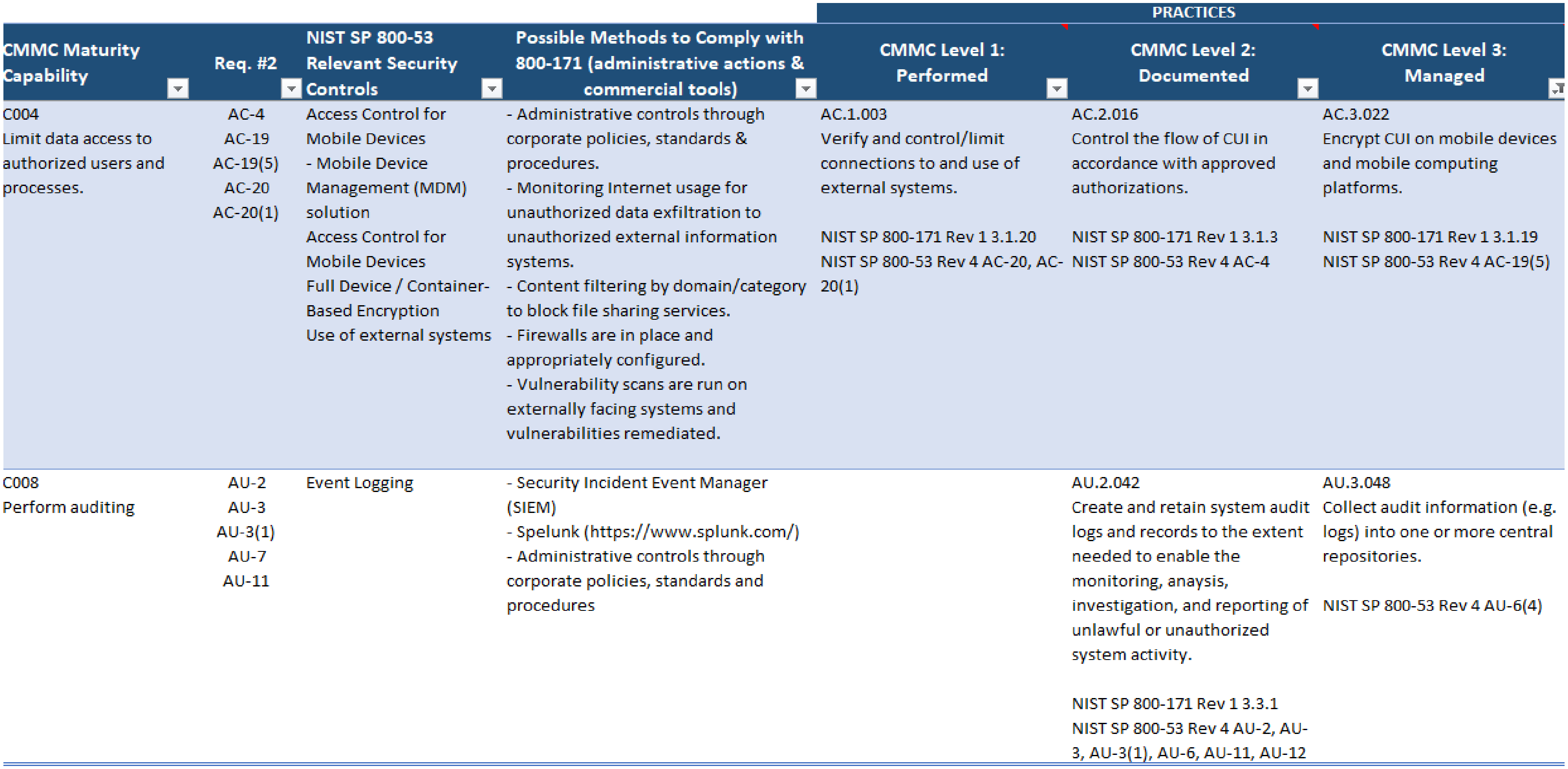
The levels build on one another. At a minimum, contractors must be **Level 1** certified. If a contract requires a higher level of certification, the contractor is required to meet that level and all lower levels. The level requirement will be specified in Requests for Information (RFI) and Requests for Proposal (RFP) coming from the DoD later this year.

| PROCESSES | CERTIFICATION LEVEL | PRACTICES |
|---|---|---|
| OPTIMIZING | 5 | ADVANCED/PROGRESSIVE |
| REVIEWED | 4 | PROACTIVE |
| MANAGED | 3 | GOOD CYBER HYGIENE |
| DOCUMENTED | 2 | INTERMEDIATE CYBER HYGIENE |
| PERFORMED | 1 | BASIC CYBER HYGIENE |

# Practices

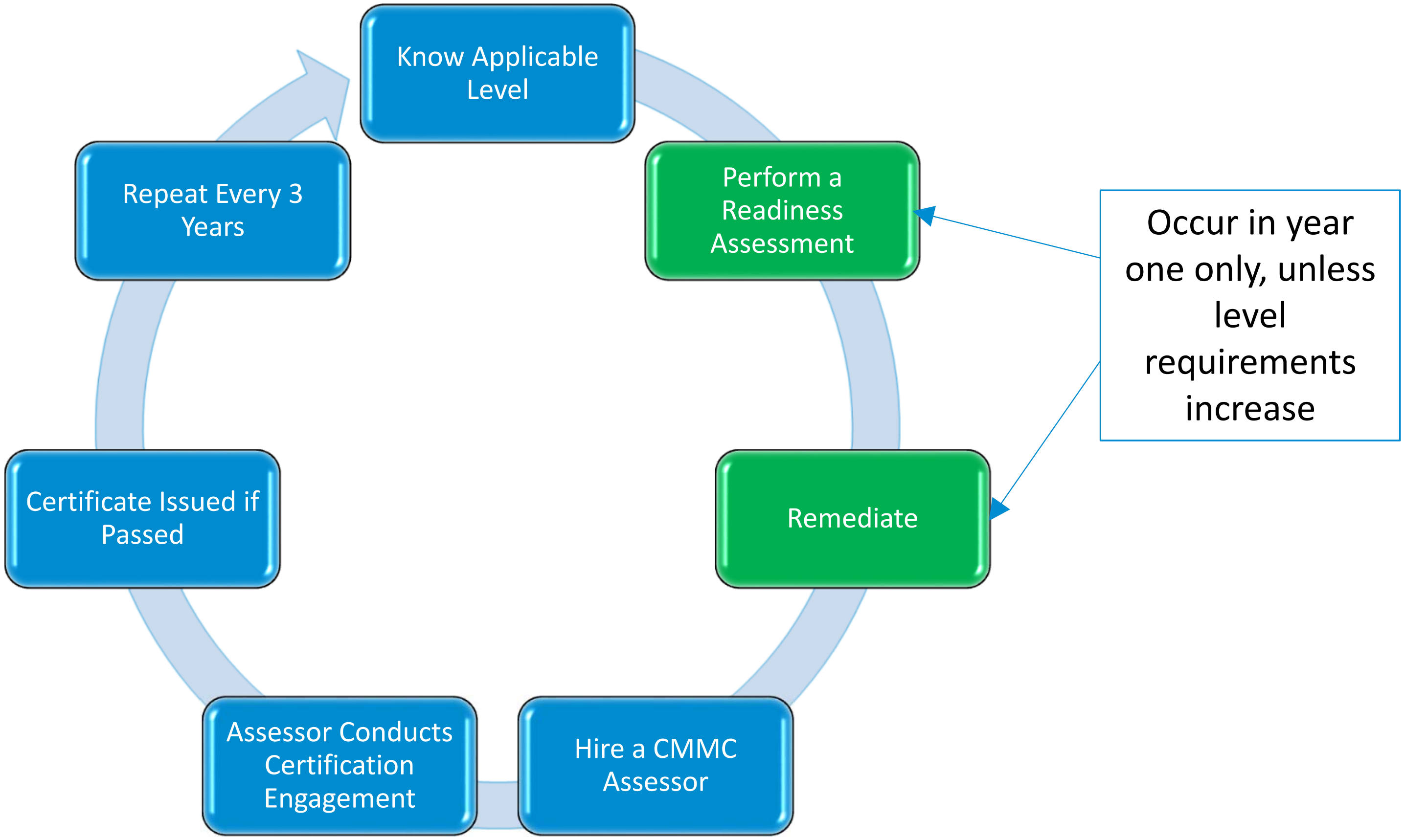

LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
+ 55 Practices
LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
+ 58 Practices
LEVEL 4
PROACTIVE
156 PRACTICES
+ 26 Practices
LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
+ 15 Practices

# Practices (Controls)



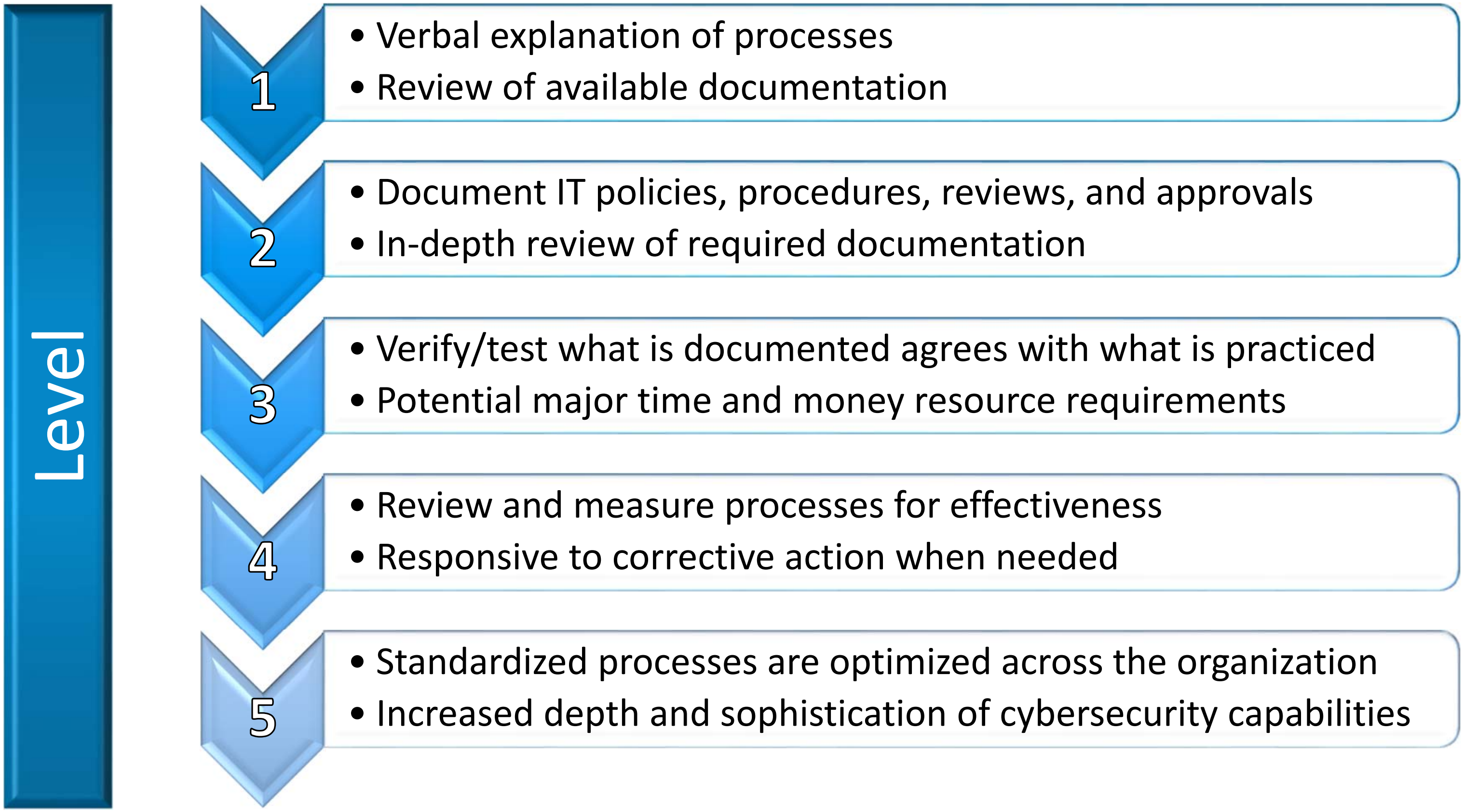
| | | | | PRACTICES | | |
|---|---|---|---|---|---|---|
| CMMC Maturity Capability | Req. #2 | NIST SP 800-53 Relevant Security Controls | Possible Methods to Comply with 800-171 (administrative actions & commercial tools) | CMMC Level 1: Performed | CMMC Level 2: Documented | CMMC Level 3: Managed |
| C004<br>Limit data access to authorized users and processes. | AC-4<br>AC-19<br>AC-19(5)<br>AC-20<br>AC-20(1) | Access Control for Mobile Devices<br>- Mobile Device Management (MDM) solution<br>Access Control for Mobile Devices<br>Full Device / Container-Based Encryption<br>Use of external systems | - Administrative controls through corporate policies, standards & procedures.<br>- Monitoring Internet usage for unauthorized data exfiltration to unauthorized external information systems.<br>- Content filtering by domain/category to block file sharing services.<br>- Firewalls are in place and appropriately configured.<br>- Vulnerability scans are run on externally facing systems and vulnerabilities remediated. | AC.1.003<br>Verify and control/limit connections to and use of external systems.<br><br>NIST SP 800-171 Rev 1 3.1.20<br>NIST SP 800-53 Rev 4 AC-20, AC-20(1) | AC.2.016<br>Control the flow of CUI in accordance with approved authorizations.<br><br>NIST SP 800-171 Rev 1 3.1.3<br>NIST SP 800-53 Rev 4 AC-4 | AC.3.022<br>Encrypt CUI on mobile devices and mobile computing platforms.<br><br>NIST SP 800-171 Rev 1 3.1.19<br>NIST SP 800-53 Rev 4 AC-19(5) |
| C008<br>Perform auditing | AU-2<br>AU-3<br>AU-3(1)<br>AU-7<br>AU-11 | Event Logging | - Security Incident Event Manager (SIEM)<br>- Spelunk (https://www.splunk.com/)<br>- Administrative controls through corporate policies, standards and procedures | | AU.2.042<br>Create and retain system audit logs and records to the extent needed to enable the monitoring, anaysis, investigation, and reporting of unlawful or unauthorized system activity.<br><br>NIST SP 800-171 Rev 1 3.3.1<br>NIST SP 800-53 Rev 4 AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12 | AU.3.048<br>Collect audit information (e.g. logs) into one or more central repositories.<br><br>NIST SP 800-53 Rev 4 AU-6(4) |

# Process


Know Applicable Level
Perform a Readiness Assessment
Remediate
Hire a CMMC Assessor
Assessor Conducts Certification Engagement
Certificate Issued if Passed
Repeat Every 3 Years

Occur in year one only, unless level requirements increase

# Expectations



Level

1
- Verbal explanation of processes
- Review of available documentation

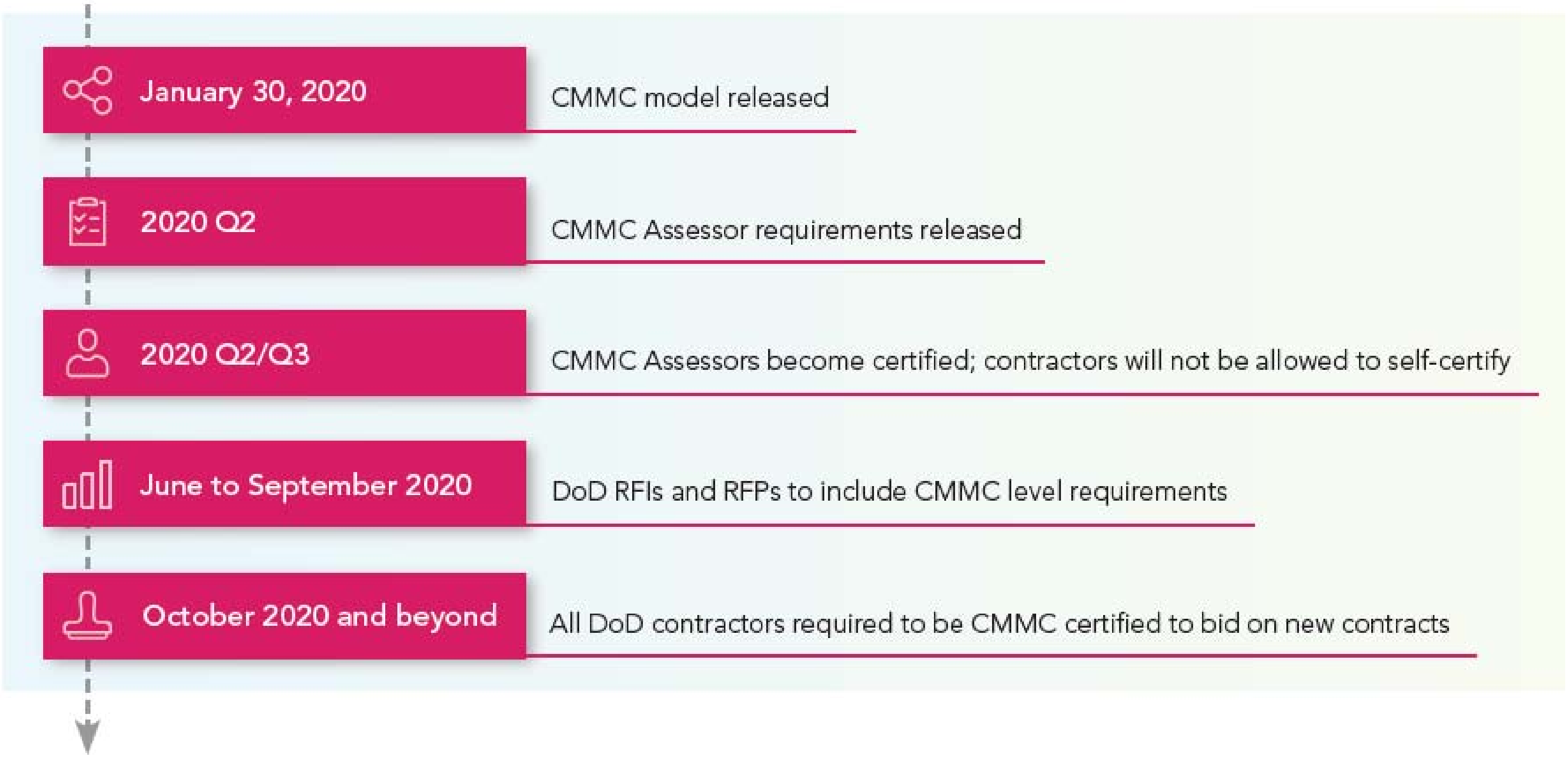
2
- Document IT policies, procedures, reviews, and approvals
- In-depth review of required documentation

3
- Verify/test what is documented agrees with what is practiced
- Potential major time and money resource requirements

4
- Review and measure processes for effectiveness
- Responsive to corrective action when needed

5
- Standardized processes are optimized across the organization
- Increased depth and sophistication of cybersecurity capabilities

# Timing



| | |
|---|---|
| January 30, 2020 | CMMC model released |
| 2020 Q2 | CMMC Assessor requirements released |
| 2020 Q2/Q3 | CMMC Assessors become certified; contractors will not be allowed to self-certify |
| June to September 2020 | DoD RFIs and RFPs to include CMMC level requirements |
| October 2020 and beyond | All DoD contractors required to be CMMC certified to bid on new contracts |

# Recent Developments

Version 1.00 Released January 30, 2020

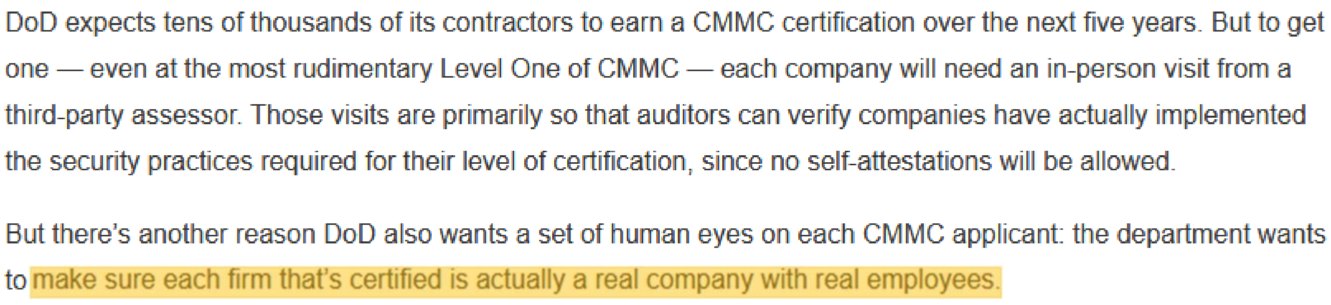
Public Briefings, Main Model, & Appendices

# Recent Developments

Version 1.02 Released March 18, 2020

Administrative corrections only

# Recent Developments



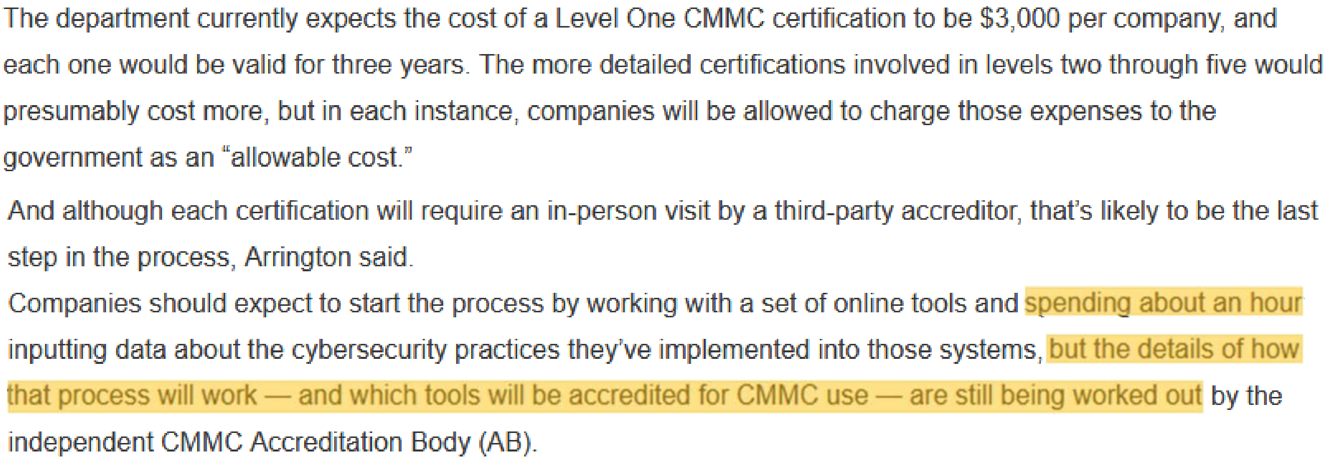
DoD expects tens of thousands of its contractors to earn a CMMC certification over the next five years. But to get one — even at the most rudimentary Level One of CMMC — each company will need an in-person visit from a third-party assessor. Those visits are primarily so that auditors can verify companies have actually implemented the security practices required for their level of certification, since no self-attestations will be allowed.

But there's another reason DoD also wants a set of human eyes on each CMMC applicant: the department wants to make sure each firm that's certified is actually a real company with real employees.

Katie Arrington is the special assistant to the Assistant Secretary of Defense for Acquisition for Cyber in the Office of the Under Secretary of Acquisition and Sustainment in DoD.

Verify Your Organization is Real
Released May 2020

# Recent Developments



The department currently expects the cost of a Level One CMMC certification to be $3,000 per company, and each one would be valid for three years. The more detailed certifications involved in levels two through five would presumably cost more, but in each instance, companies will be allowed to charge those expenses to the government as an "allowable cost."

And although each certification will require an in-person visit by a third-party accreditor, that's likely to be the last step in the process, Arrington said.

Companies should expect to start the process by working with a set of online tools and spending about an hour inputting data about the cybersecurity practices they've implemented into those systems, but the details of how that process will work — and which tools will be accredited for CMMC use — are still being worked out by the independent CMMC Accreditation Body (AB).

Katie Arrington is the special assistant to the Assistant Secretary of Defense for Acquisition for Cyber in the Office of the Under Secretary of Acquisition and Sustainment in DoD.

## Level 1 Cost Expectations Released May 2020

# Recent Developments

CMMC
ACCREDITATION BODY
Cybersecurity Maturity Model Certification

Assessor Training and Certification Process
Released June 2020

# What Can You Do?

- Prime Contractors – contact your regular source for DoD contracts and request CMMC level expectations
- First-tier Contractors – contact the prime contractor and request CMMC level expectations

You will need at least CMMC Level 1 Certification.
There will be no scenarios without at least Level 1.*

# What Can You Do?

## All Levels

- Perform a readiness assessment
  - Self assessment
  - Utilize a third party
- Remediation
- This is NOT a certification

# What Can You Do?

Not
Certified
Yet

## Readiness Assessment Level 1

- A self assessment is a realistic option
  - CMMC Appendices v1.02 should be used
  - The “spending about an hour” is not realistic
- Remediation – days, weeks, or a month
  - Very unlikely to involve major expenditures

# What Can You Do?

Not Certified Yet

## Readiness Assessment Level 2

- A self assessment may be a realistic option
  - CMMC documentation on practices should be used
  - Moderate to strong skillset in policy & procedure development needed
- Remediation – 30 to 45 days
  - Find a NIST 800-171 policy & procedure template
  - Modify template to your environment and improve processes as needed

# What Can You Do?

Not Certified Yet

## Readiness Assessment Level 3

- Utilize a third party
  - Level 3 is very technical, for example we use a combination of IT compliance auditors and cybersecurity experts for level 3 readiness assessments
- Remediation – 1 to 3 months
  - First level where remediation can potentially have major costs to remediate

# What Can You Do?

Not Certified Yet

## Readiness Assessment Level 4

- Utilize a third party
- Remediation – 3 to 9 months
  - May involve significant expenditures

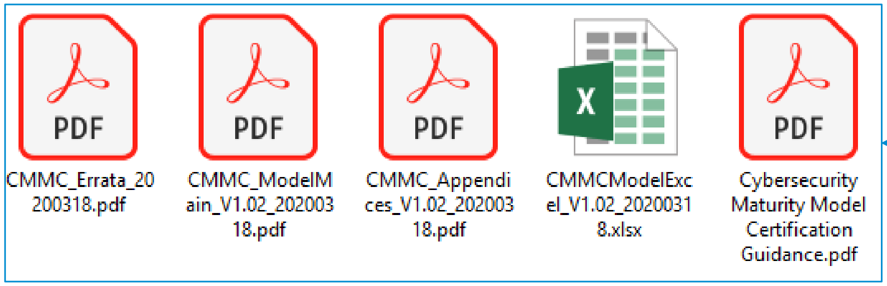
# What Can You Do?

Not Certified Yet

## Readiness Assessment Level 5

- Utilize a third party
- Remediation – 9 months to 1 year+
  - May involve significant expenditures

# Resources



CMMC_Errata_20200318.pdf

CMMC_ModelMain_V1.02_20200318.pdf

CMMC_Appendices_V1.02_20200318.pdf

CMMCModelExcel_V1.02_20200318.xlsx

Cybersecurity Maturity Model Certification Guidance.pdf

Files will be available for all participants

https://www.acq.osd.mil/cmmc/index.html

# Questions?

DEANDORTON

# Thank you

## Kevin W. Cornwell, CPA, CISA, CITP

Associate Director of Technology Consulting

kcornwell@ddaftech.com | 502.566.1011

DEANDORTON