




CMMC '25: WHAT'S REAL, WHAT'S NOT & HOW TO KEEP YOUR CONTRACTS

SHAYLA TREADWELL, PH.D.

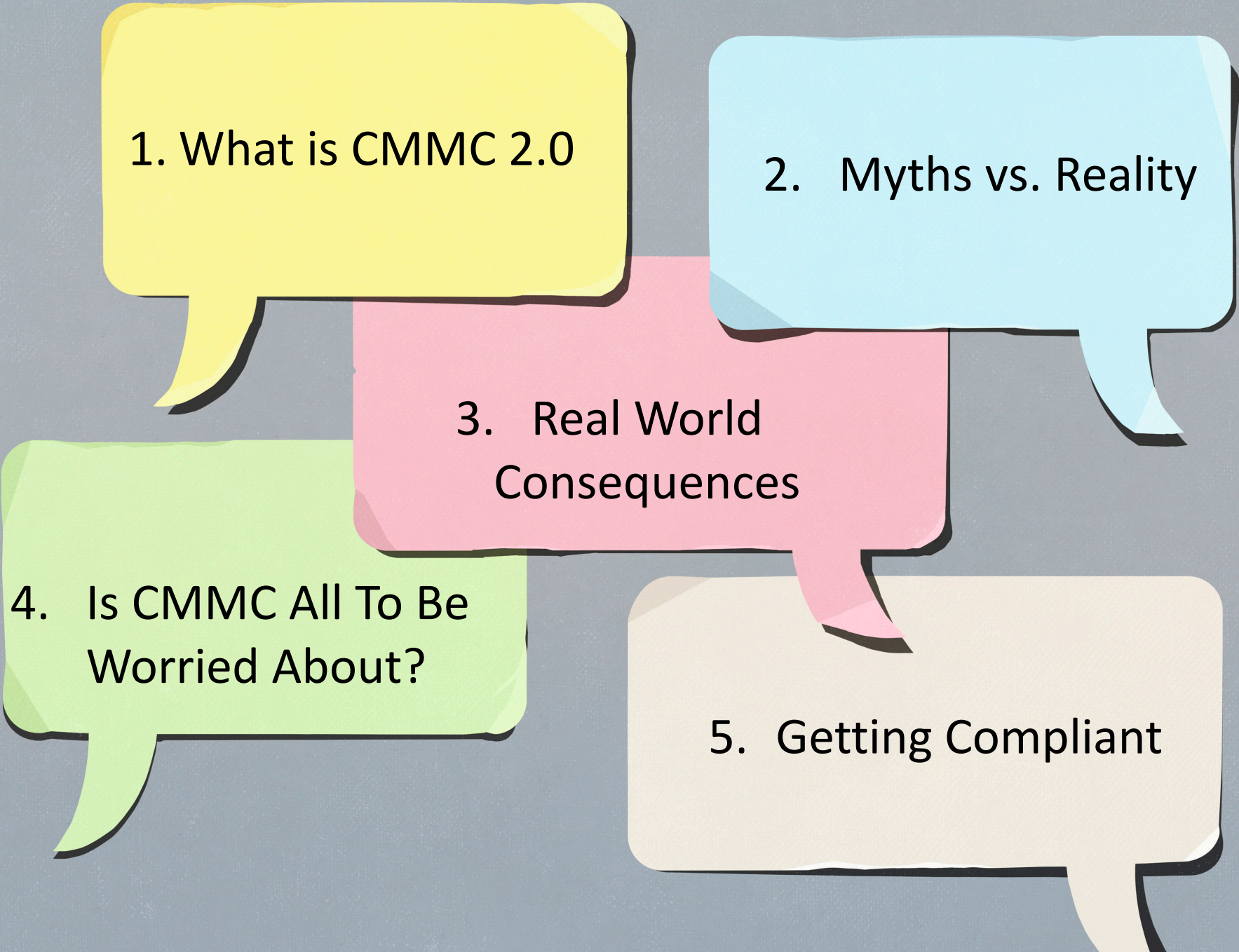
DISCLAIMER

This presentation is intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of Lumen Technologies.



- 
- CYBERSECURITY EXECUTIVE
 - GRC SME
 - AI GOVERNANCE STRATEGIST
 - ORGANIZATIONAL PSYCHOLOGIST

SHAYLA TREADWELL, Ph.D.



1. What is CMMC 2.0

2. Myths vs. Reality

3. Real World
Consequences

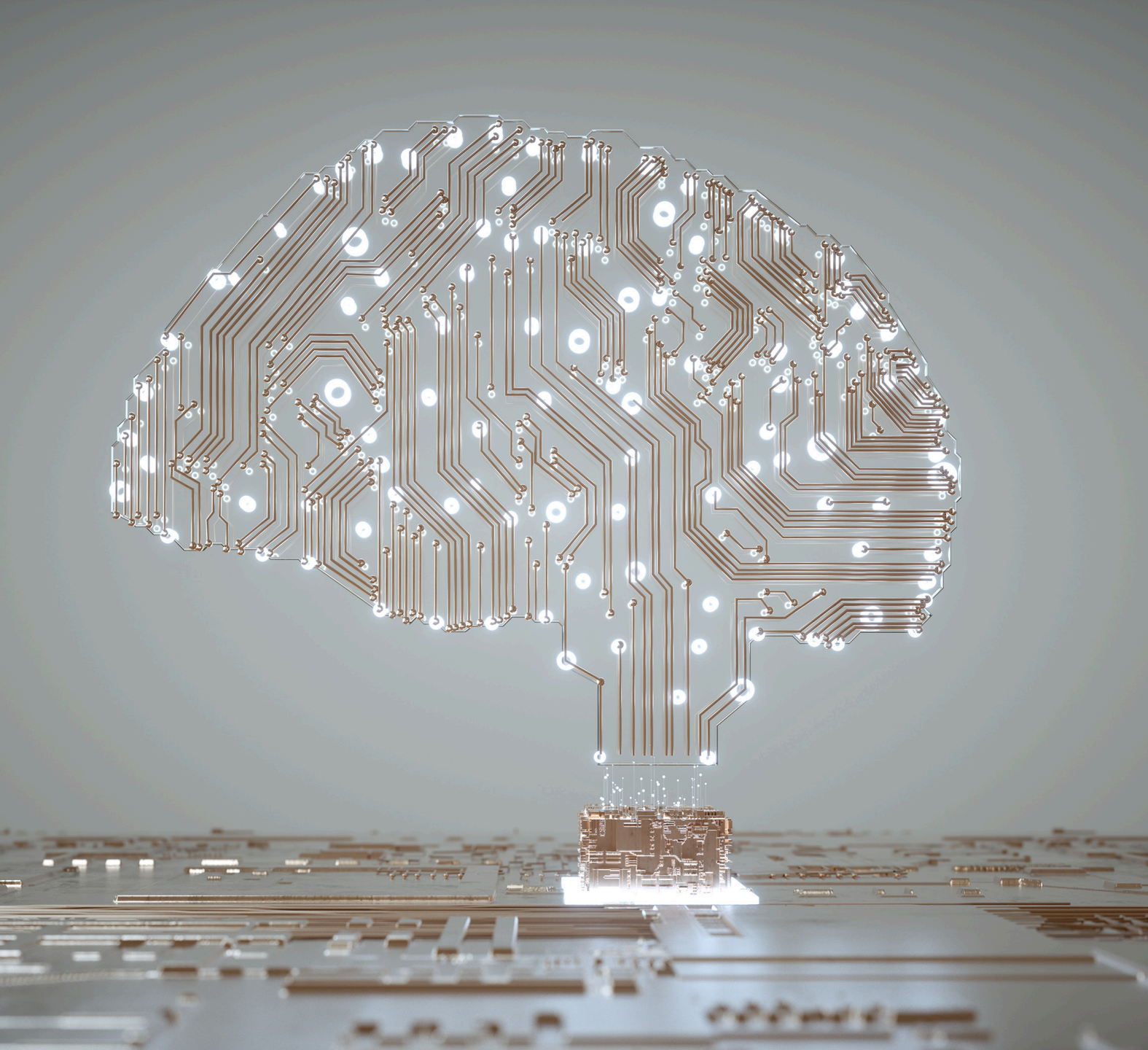
4. Is CMMC All To Be
Worried About?

5. Getting Compliant



MAKING SENSE OF THE COMPLINACE MAZE





FLASH FACE DISTORTION EFFECT (FFDE)

- A phenomenon where, when faces are rapidly alternated and viewed peripherally, they appear grotesque and exaggerated.
- Distortions seemed to be caused by the brain's heightened sensitivity to deviations from normal face templates, leading to exaggerated perceptions of those differences

SO, WHAT'S THE CONNECTION HERE...



FLASH FACE DISTORTION EFFECT

Faces appear distorted when shown quickly and without context

Your brain exaggerates differences

It's an illusion

VS




CMMC COMPLIANCE

Controls seem overwhelming when only viewed during an audit

Teams overreact to issues because they lack baseline understanding

So is thinking your SSP alone will save your contract



“Just like the Flash Face Distortion Effect tricks your eyes by isolating features without context, CMMC compliance fails when we isolate controls from the bigger security picture. It's not about what looks wrong — it's about what is missing.”



WHAT IS CMMC?

CMMC PROGRAM OVERVIEW

CMMC Model		
	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	<ul style="list-style-type: none">• DIBCAC certification assessment every 3 years• Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 R2	<ul style="list-style-type: none">• C3PAO certification assessment every 3 years, or• Self assessment every 3 years for select programs• Annual Affirmation
LEVEL 1	15 requirements aligned with FAR 52.204-21	<ul style="list-style-type: none">• Annual Self Assessment• Annual Affirmation

- The CMMC Program aligns with the DoD's existing information security requirements for the DIB.
- The program provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal systems processing controlled unclassified information.
- The FAR requires compliance with 15 security basic cybersecurity requirements. FAR clause 52.204-21 (b)(1), items (i) through (xv) identify these requirements. These security requirements map to 17 security requirements in NIST SP 800-171 R2.

CMMC AIMS TO...



Safeguard sensitive information to enable and protect the warfighter



Dynamically enhance DIB cybersecurity to meet evolving threats



Ensure accountability while minimizing barriers to compliance with DoD requirements



Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience



Maintain public trust through high professional and ethical standards

WHO MUST ADHERE TO CMMC

All DoD prime- and sub-contractors planning to bid on future contracts with with the CMMC DFARS clause

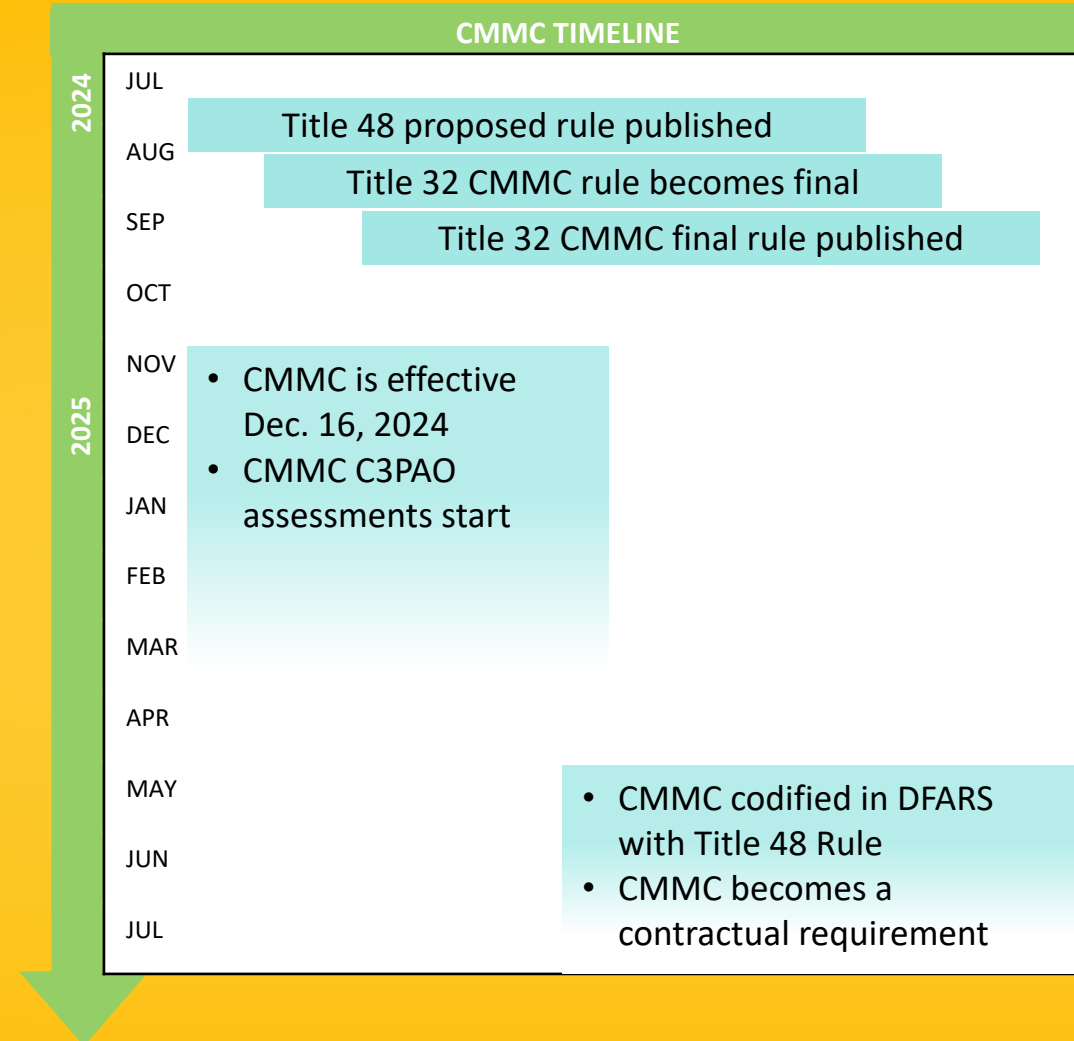


FEDERAL CONTRACT
INFORMATION (FCI)



CONTROLLED UNCLASSIFIED
INFORMATION (CUI)

CMMC TIMELINE



A photograph of two deer with large, multi-tined antlers facing each other in a grassy field. The deer are positioned on either side of the frame, with their heads and antlers meeting in the center. The background is a blurred natural setting with trees and foliage. The text "MYTH VS. RELAITY" is overlaid on the right side of the image.

MYTH VS. RELAITY



My contract will never change.
We will get a waver. We can outsource it all.
It will just get postponed indefinitely.
All companies need Level 3.




**CMMC only applies to
prime contractors.**

CMMC applies to everyone in the DIB, including subcontractors, vendors, and suppliers, if they handle Controlled Unclassified Information (CUI) or Federal Contract Information (FCI).

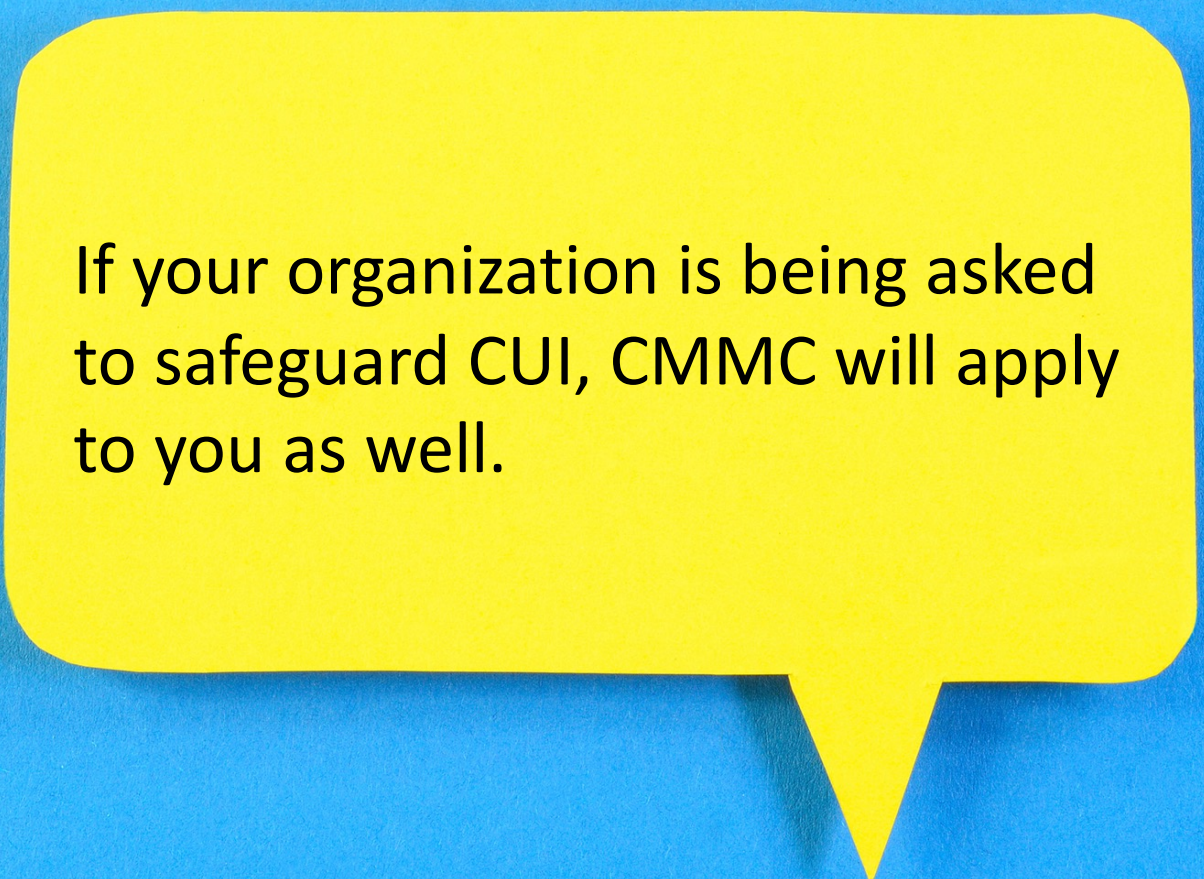


**CMMC is only about
NIST 800-171**

While NIST 800-171 is a key component of CMMC, it is not the only aspect. It's about alignment with regulation and demonstrating continuous improvement.



CMMC Level 2 only
applies to large
organizations.

A yellow speech bubble with a pointed tail at the bottom center, set against a large blue circular background. The background has a subtle texture and faint white circular patterns on the right side.

If your organization is being asked
to safeguard CUI, CMMC will apply
to you as well.



REAL WORLD CONSEQUENCES

PRESS RELEASE

Aerojet Rocketdyne Agrees to Pay \$9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts

Friday, July 8, 2022

For Immediate Release

Office of Public Affairs

IS CMMC ALL I SHOULD BE WORRIED ABOUT?



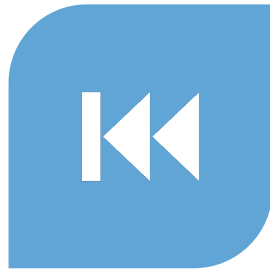
A man with a beard and a light blue shirt is shown from the chest up, looking directly at the camera with a surprised expression. His hands are outstretched to the sides, palms up. The background is a dark reddish-brown color with faint, white technical diagrams overlaid. These diagrams include concentric circles, arcs, and lines with numerical labels such as 40, 150, 160, 170, 180, 190, 200, 210, 220, 230, 240, 250, and 260. Some of the lines have arrowheads, suggesting a flow or direction. The overall aesthetic is technical and modern.

SHORT ANSWER... NO

GETTING COMPLIANT



MAKE COMPLINACE A
CULTURE



GET BACK TO THE
TEXT



KNOW AND CONTROL
YOUR DATA



GET SOME QUICK
WINS

KEY TAKEAWAYS

- **CMMC Is Real and Rising**
CMMC 2.0 is not a drill — contracts *will* require certification and audits.
- **DFARS Compliance Already Has Teeth**
Just ask Aerojet Rocketdyne — \$9M later, non-compliance isn't theoretical.
- **Spot-Check Compliance = Flash Face Illusion**
Don't just chase what looks wrong. Build a full-picture, continuous program.
- **Self-Attestation ≠ Safety**
False claims can trigger False Claims Act violations. Document, don't assume.
- **3 Steps to Safeguard Your Contracts**
Align with corporate compliance
Embed security in daily ops
Make audit-readiness a living practice



THANK YOU

Shayla Treadwell, Ph.D.

E: Shayla.Treadwell@lumen.com

<https://www.linkedin.com/in/shayla-treadwell/>