CLARK SCHAEFER
CONSULTING

Essential Knowledge for CMMC

Introductions

CLARK SCHAEFER
CONSULTING

Presenters

Serge Kikonda
Senior Consultant, RPA
IT Risk & Cybersecurity

Bishop Rock
Consultant
IT Risk & Cybersecurity

Moderated By

Carly Devlin
Shareholder
IT Risk & Cybersecurity

Agenda

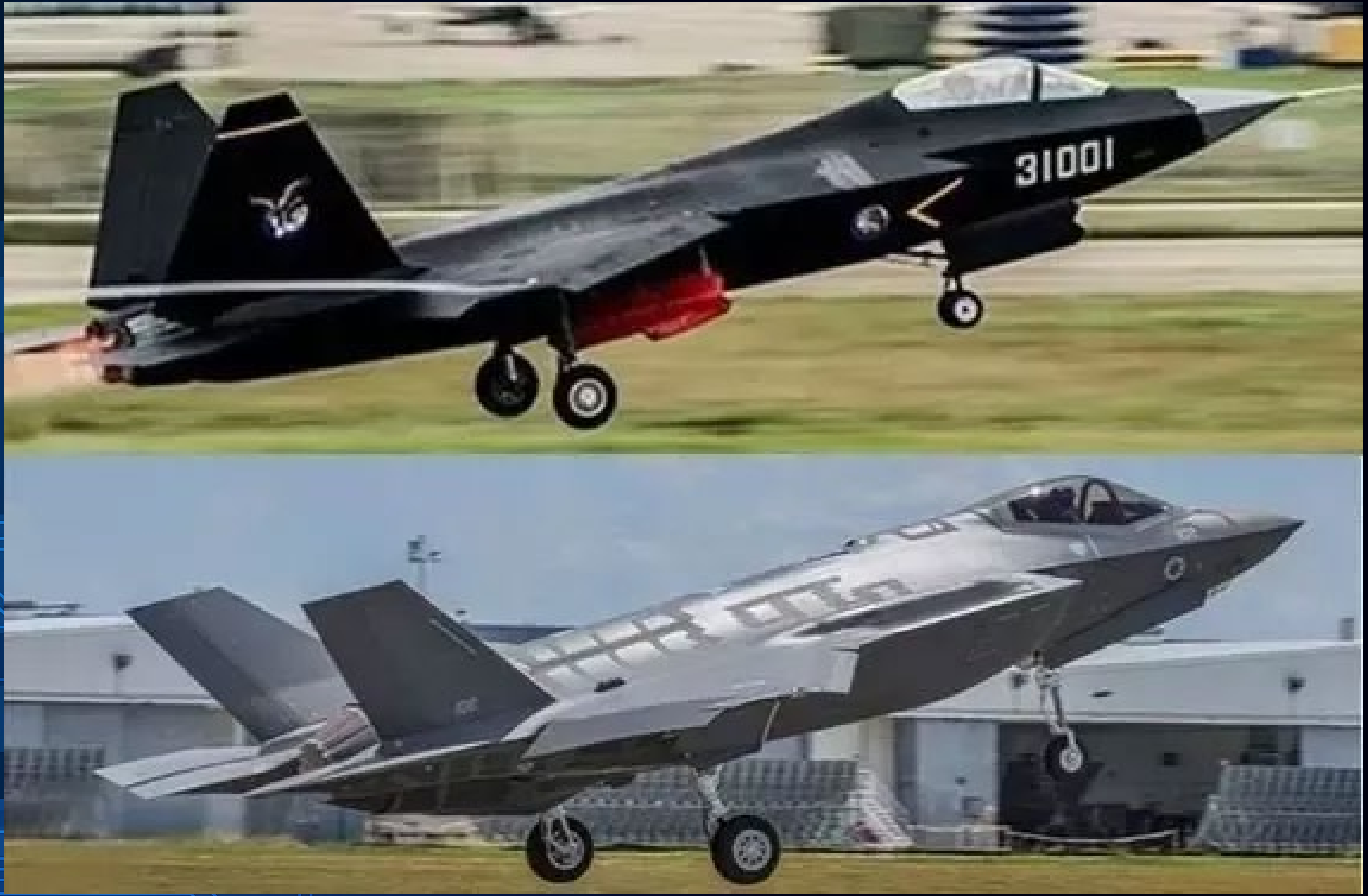
CLARK SCHAEFER CONSULTING

- Introductions
- CMMC: Origin & Objective
- CMMC Applicability
- History: The CMMC Journey
- Future: The CMMC Journey
- CMMC Compliance: Getting Started
- RPO vs C3PAO
- Deciphering the CMMC Layers
- CMMC Compliance Cost Estimates
- CMMC Assessment Insights

CMMC: Origin & Objective

- The Department of Defense (DoD) noticed that many companies that were working in the Defense Industrial Base (DIB) were not maintaining an acceptable level of cyber posture with controls.
- The information that many of these companies were meant to protect ended up in the hands of foreign adversaries.

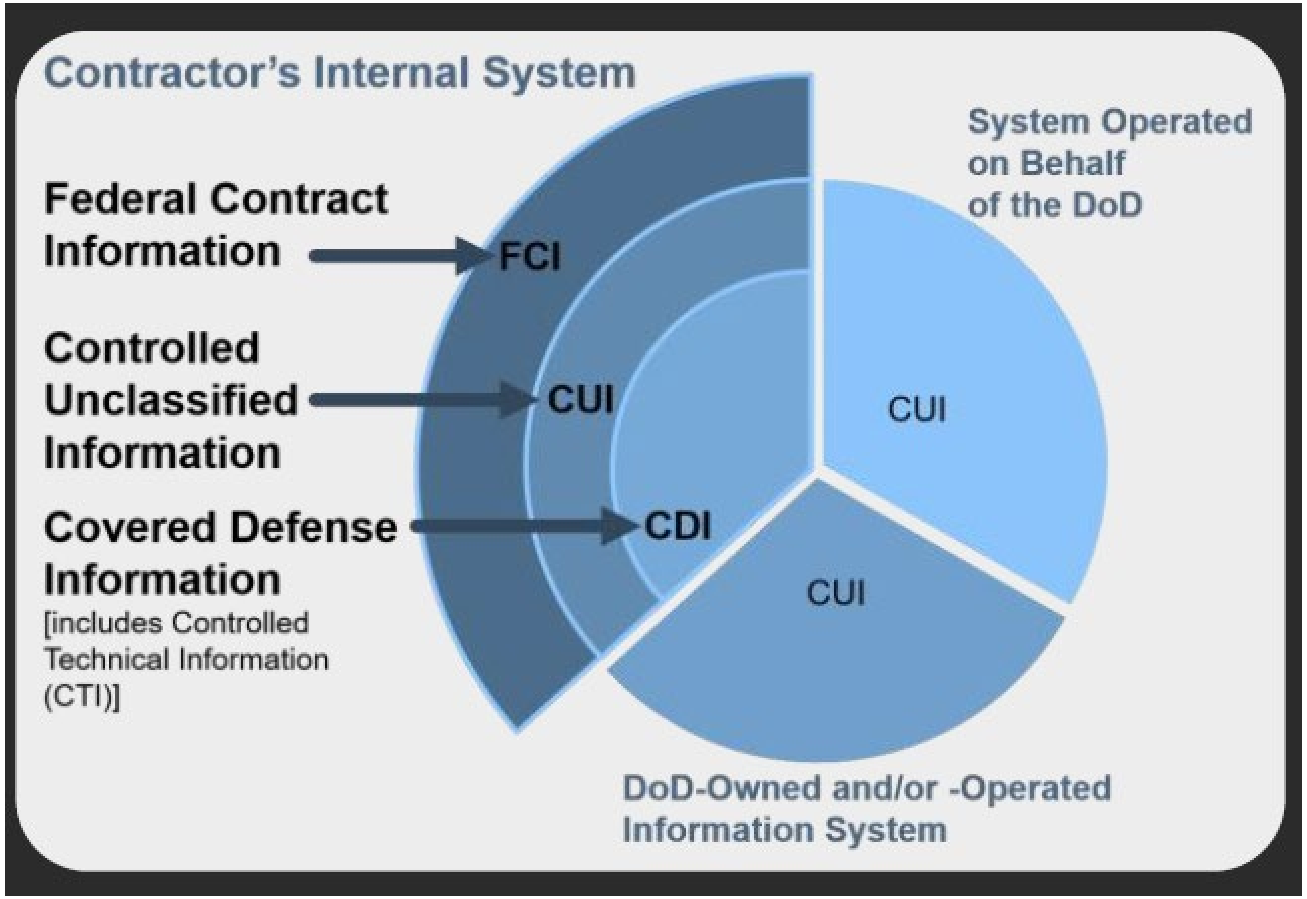
See J31 Chinese jet (Top) and American F-35 jet (Bottom) comparison



CMMC: Origin & Objective

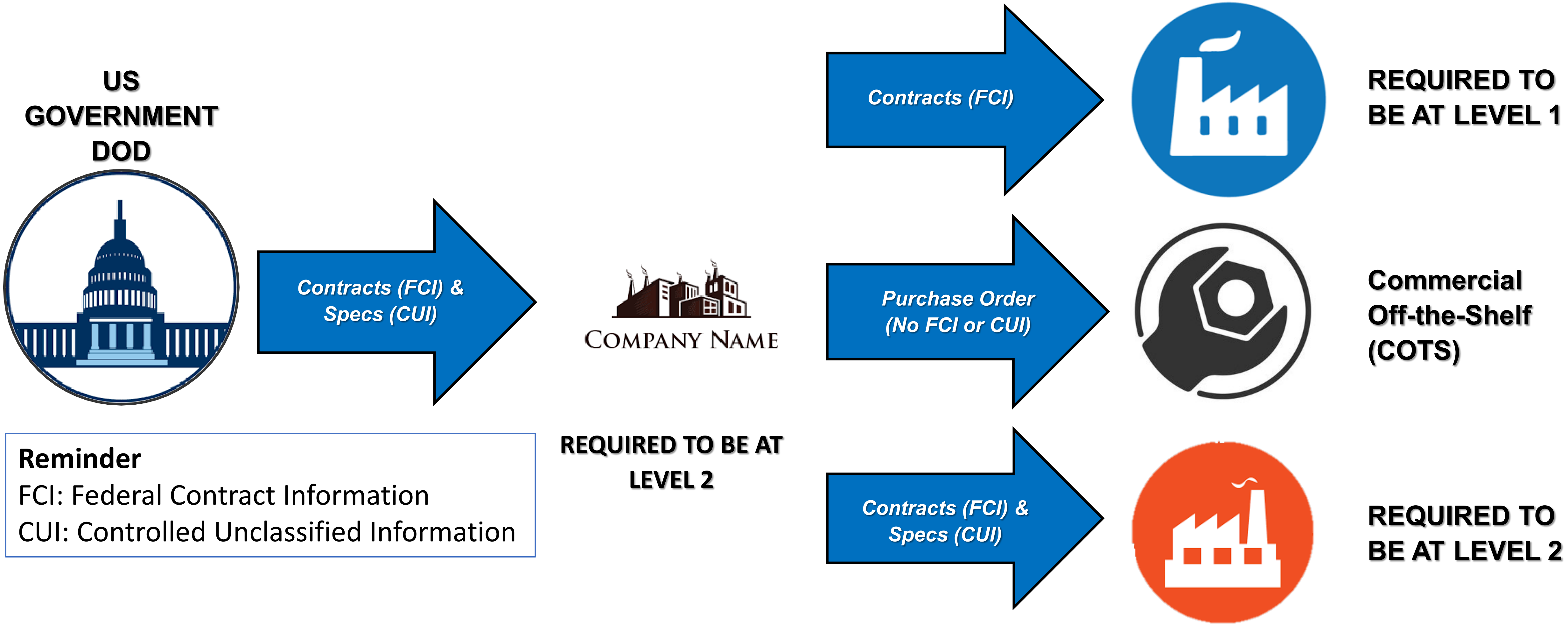
- As a result, the Cybersecurity Maturity Model Certification (CMMC) was developed by the Department of Defense (DoD).

- The objective of CMMC is to bring companies working within the Defense Industrial Base (DIB) to an acceptable level of cyber posture to protect Controlled Unclassified Information (CUI) and Covered Defense Information (CDI).



Contractor's Internal System
System Operated on Behalf of the DoD
Federal Contract Information
FCI
Controlled Unclassified Information
CUI
Covered Defense Information [includes Controlled Technical Information (CTI)]
CDI
CUI
CUI
DoD-Owned and/or -Operated Information System

CMMC Applicability: Where does your company stand?



US GOVERNMENT DOD

Contracts (FCI) & Specs (CUI)

COMPANY NAME

REQUIRED TO BE AT LEVEL 2

Contracts (FCI)

REQUIRED TO BE AT LEVEL 1

Purchase Order (No FCI or CUI)

Commercial Off-the-Shelf (COTS)

Contracts (FCI) & Specs (CUI)

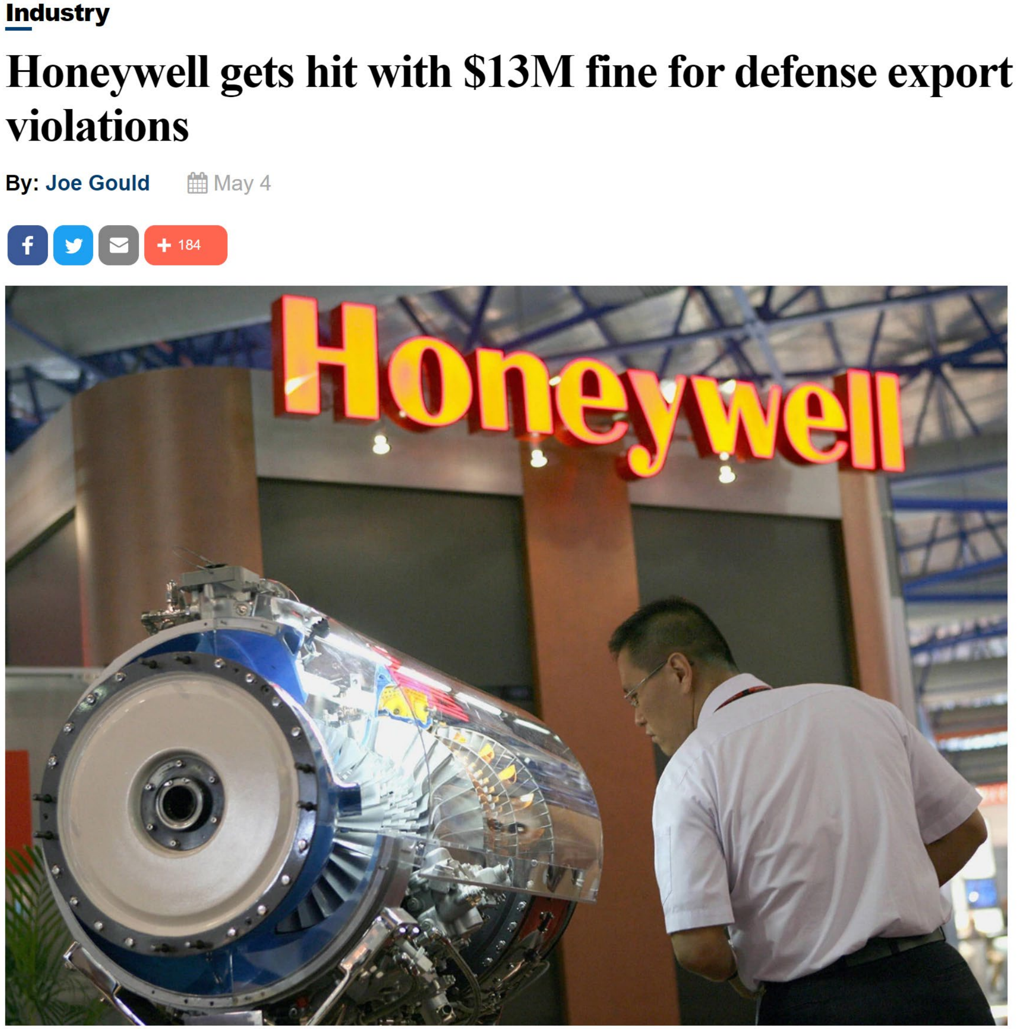
REQUIRED TO BE AT LEVEL 2

Reminder
FCI: Federal Contract Information
CUI: Controlled Unclassified Information

CMMC Applicability: Do I have to?

Cost of Noncompliance

- Potential fines
- Inability to bid or be awarded contracts
- Potential loss of current contracts



Industry

Honeywell gets hit with $13M fine for defense export violations

By: Joe Gould May 4

History: The CMMC Journey

CLARK SCHAEFER CONSULTING

START

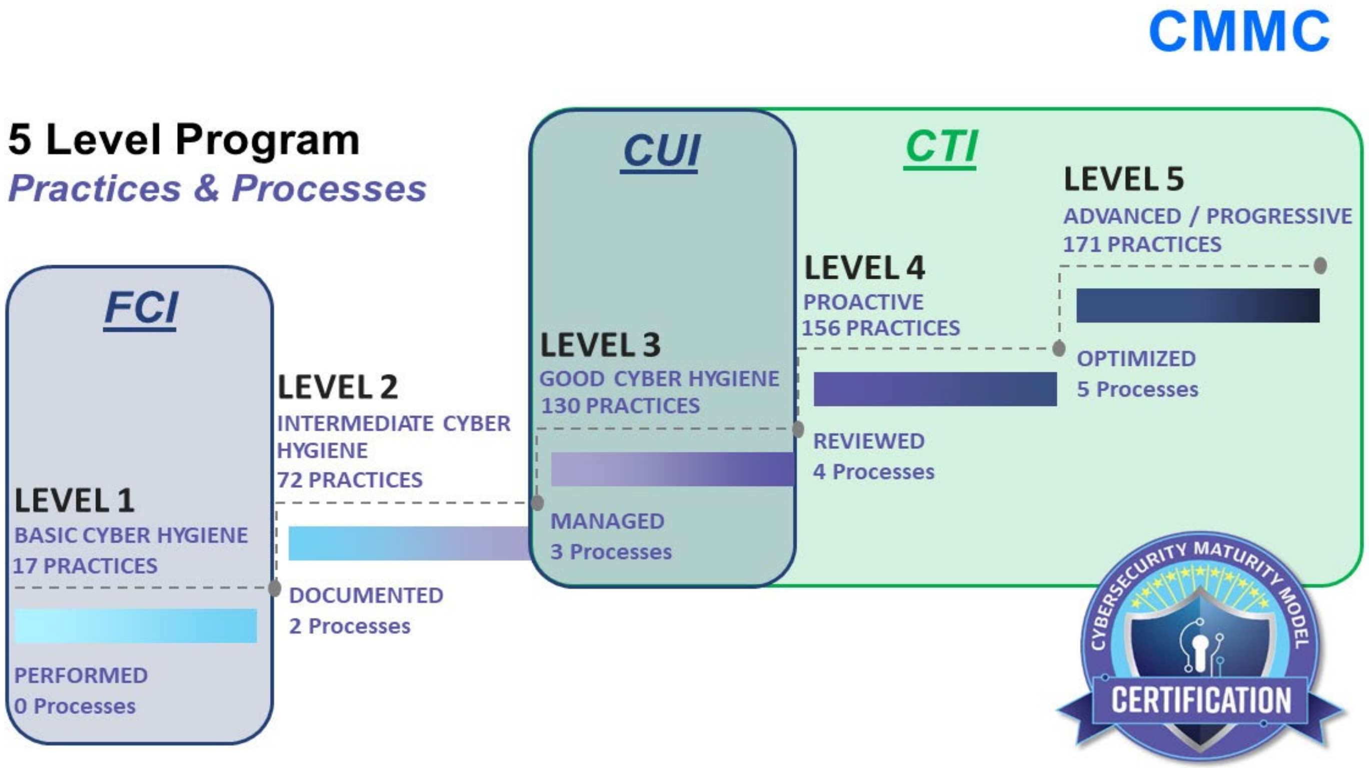
2020

NOVEMBER

INTRODUCTION OF CMMC 1.0:

3 **NEW** clauses:

- ✓ DFARS 252.704-**7019**
- ✓ DFARS 252.704-**7020**
- ✓ DFARS 252.704-**7021**



CLARK SCHAEFER CONSULTING

History: The CMMC Journey

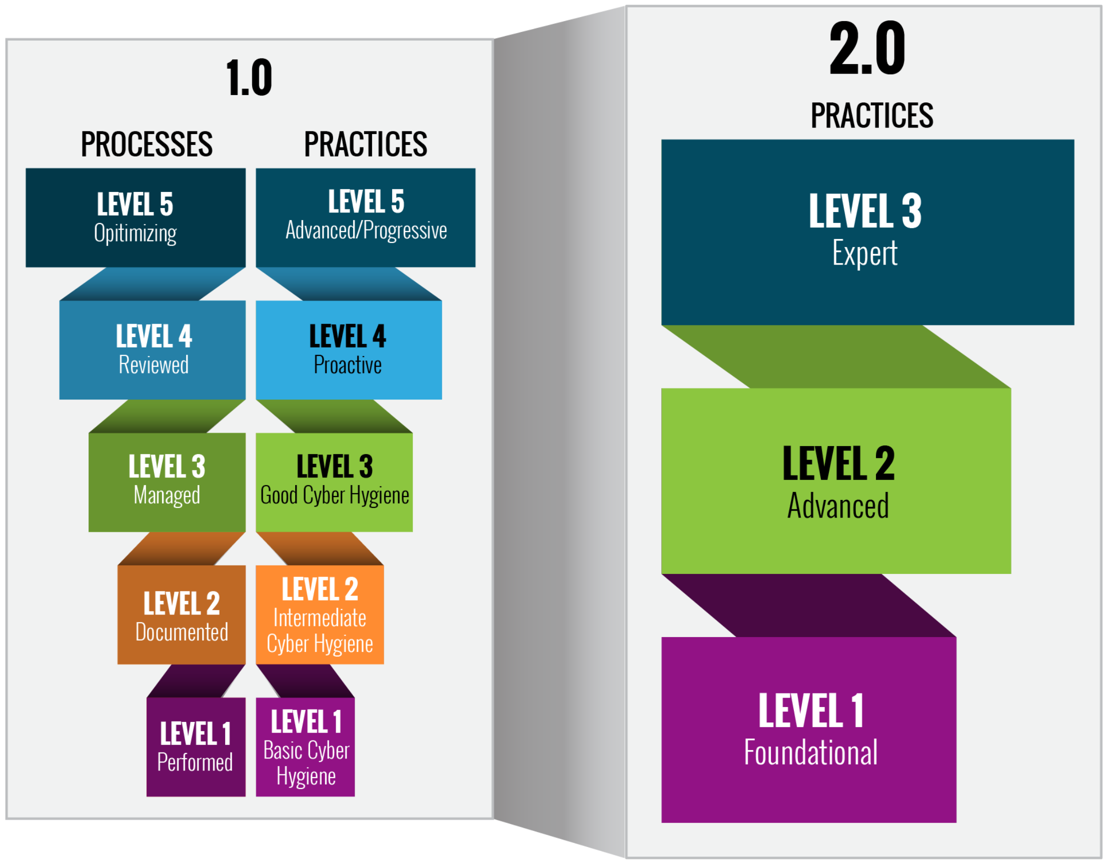
2020 → 2021

NOVEMBER NOVEMBER

INTRODUCTION OF CMMC 2.0:

- Removes Level 2 & Level 4 (from CMMC 1.0).
- Simplifies the structure and introduces key changes.

CMMC Model Structure



1.0

PROCESSES	PRACTICES
LEVEL 5 Opitimizing	LEVEL 5 Advanced/Progressive
LEVEL 4 Reviewed	LEVEL 4 Proactive
LEVEL 3 Managed	LEVEL 3 Good Cyber Hygiene
LEVEL 2 Documented	LEVEL 2 Intermediate Cyber Hygiene
LEVEL 1 Performed	LEVEL 1 Basic Cyber Hygiene

2.0

PRACTICES
LEVEL 3 Expert
LEVEL 2 Advanced
LEVEL 1 Foundational

History: The CMMC Journey

START
CYBERSECURITY MATURITY MODEL
CERTIFICATION
2.0

2020 → 2021 → 2022

NOVEMBER NOVEMBER MAY

DoD Announces Rulemaking Window:

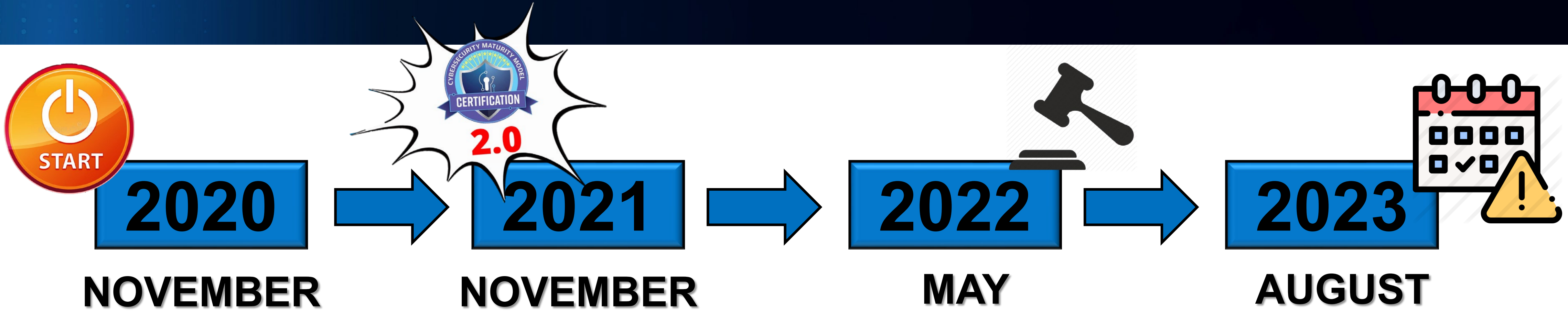
May 2023 is going to be the pivotal point for most companies within the Defense Industrial Base (DIB) who need CMMC compliance.

"May 2023 is the critical point. That's when we think we will be able to start putting the requirement in contracts…

You are probably going to see RFIs, RFPs coming out in the summer of 2023."[1]

- Stacy Bostjanick
May 9th, 2022

History: The CMMC Journey



2020 NOVEMBER → 2021 NOVEMBER → 2022 MAY → 2023 AUGUST

The end draws near!

DoD has already submitted the CMMC 2.0 rule to the Office of Information and Regulatory Affairs (OIRA).

Future: The CMMC Journey

The CMMC rule will be published as either an “Interim Final Rule” or a “Proposed Rule”.

If the rule is “proposed” then the CMMC final rule is expected to effective and in contracts between **February – April 2025**.

However, if the rule is interim final, then the CMMC final rule would be effective and in contracts in **Q1 2024**.

Future: The CMMC Journey

Better News!

- There will be a 3-year “phased-roll out” for CMMC contract clauses.
- Assuming the CMMC final rule is published in Q1 2025, all relevant DoD contracts will contain CMMC by **2028**.

CMMC Compliance: Getting Started

CLARK SCHAEFER CONSULTING

1. Team Determination - Identify internal leader and possible partner to initiate CMMC planning.
2. Scope Validation - Determine the required scope of your CMMC audit that will be pursued.
3. Assessment Planning - Create a roadmap for your CMMC journey.
4. Gap Analysis – Determine current state and what may be missing from your current environment?
5. Remediation - Remediate gaps that are found during Gap Analysis.
6. Affirmation/Self-Assessment - Validate that your controls are viable with a self-assessment.
7. CMMC Assessment – Depending on level of compliance, conduct a self-assessment or participate in CMMC Audit.

CMMC Compliance: Getting Started

- How long does it take to become compliant?
  - On average, it takes 10-18 months

- What does that mean for you?
  - You might not have that long.
  - It could be as soon as 4-5 months; OR 12-14 months depending on the rule.

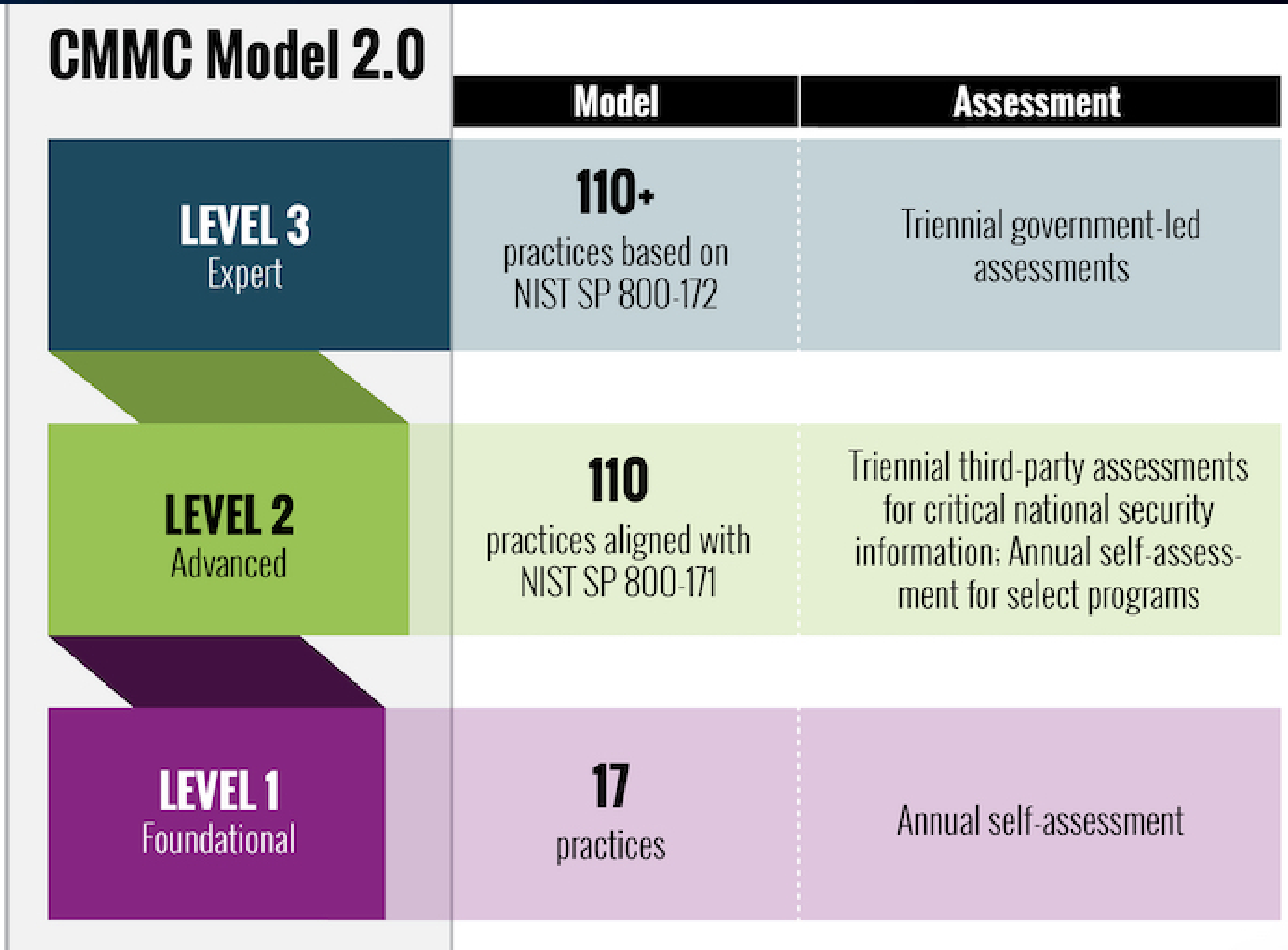
- Readiness (20%), Remediation (70%), Ongoing maintenance(10%).

CMMC Help: RPO & C3PAO

CLARK SCHAEFER CONSULTING

- Registered Provider Organization (RPO)
  - Provide pre-assessment consulting services to government contractors and other Organizations Seeking Certification (OSCs) and/or assist during assessments in the event a finding is uncovered.
- CMMC 3rd Party Assessment Organization (C3PAO)
  - A service provider organization that the CMMC Accreditation Body (CMMC-AB) has accredited and authorized to conduct CMMC audits and submits findings and certify that Organizations Seeking Certification (OSCs) comply with the CMMC 2.0 maturity level (1 through 3) to perform in any Defense Industrial Base (DIB) contract.
- An organization can be both an RPO and C3PAO. However, they cannot perform both roles for the same client. Separate entities must perform these tasks because the same entity cannot provide consulting services and then audit its own work. It is a conflict of interest.

CMMC Levels: Deciphering the Levels



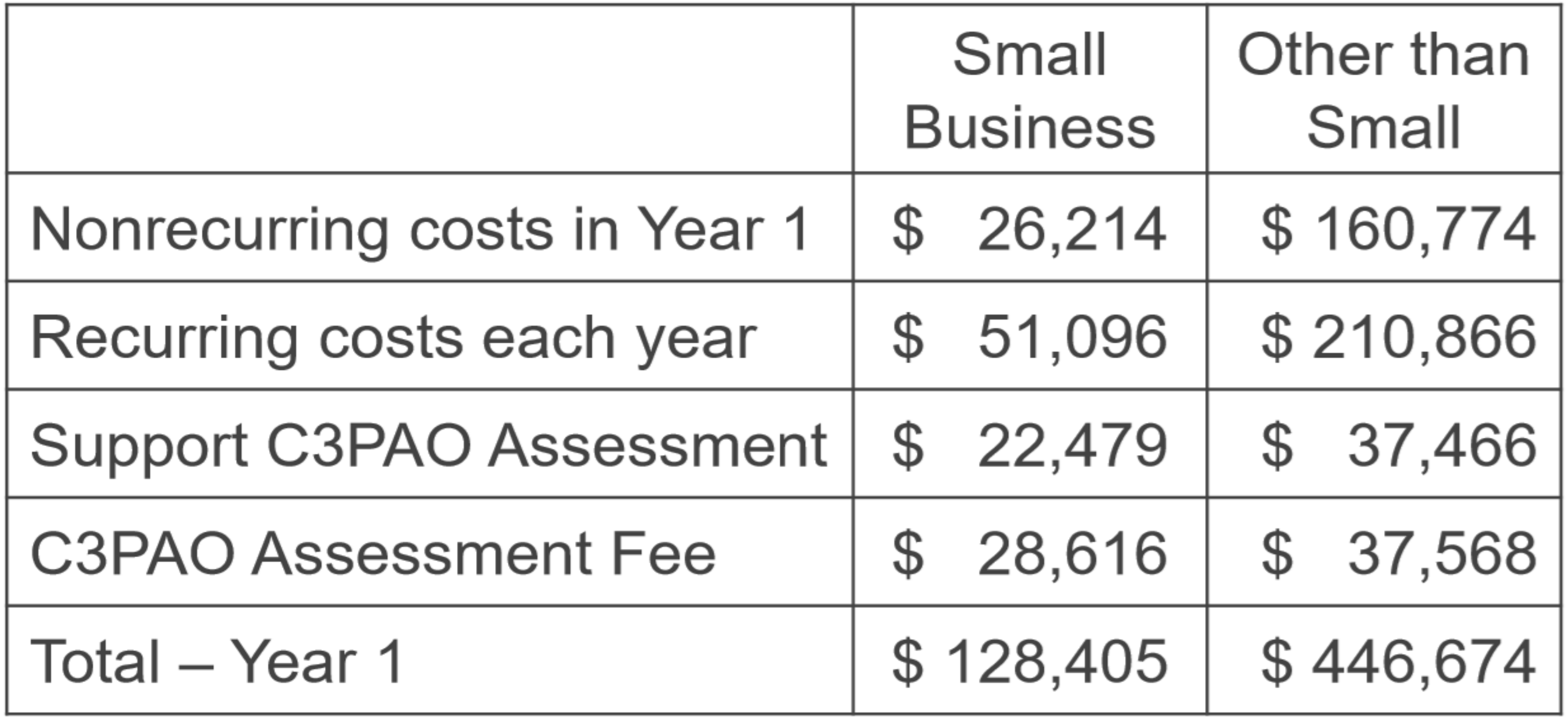
CMMC Model 2.0

	Model	Assessment
LEVEL 3 Expert	**110+** practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	**110** practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	**17** practices	Annual self-assessment

CMMC Compliance Cost Estimates

CLARK SCHAEFER
CONSULTING

* Cost estimates from 2020 *



	Small Business	Other than Small
Nonrecurring costs in Year 1	$ 26,214	$ 160,774
Recurring costs each year	$ 51,096	$ 210,866
Support C3PAO Assessment	$ 22,479	$ 37,466
C3PAO Assessment Fee	$ 28,616	$ 37,568
Total – Year 1	$ 128,405	$ 446,674

CMMC Assessment Insights

- The best thing your organization can do to prepare yourself for CMMC 2.0 is EVIDENCE GATHERING.

- The more you can PROVE, the smoother your audit will go.

- It is advantageous to work with an RPO to gather the best evidence for your audit.

Wrapping Up: Next Steps & Resource Pointers

CLARK SCHAEFER CONSULTING

1. Understand how CMMC applies to your organization
   - Check out our free survey to help with this! https://www.cshco.com/cmmc-survey/

2. Start planning your roadmap, conduct a gap analysis, and remediate
   - Clark Schaefer Consulting is a CMMC Registered Provider Organization (RPO) and can help with CMMC readiness and remediation work

If you have questions, need more information, or are ready to start your CMMC journey, check out our CMMC info page https://www.cshco.com/cmmc or contact us at cmmc@clarkschaefer.com.

Future CMMC Information

CLARK SCHAEFER
CONSULTING

- Future webinar series on CMMC by Clark Schaefer Consulting

- Keep an eye out for email communications!
  - Clark Schaefer Consulting will be sending out resources to help with your CMMC journey.

Thank you!

CLARK SCHAEFER
CONSULTING

Presenters

Serge Kikonda
Senior Consultant, RPA
IT Risk & Cybersecurity

CYBER AB
REGISTERED PRACTITIONER
ADVANCED

Bishop Rock
Consultant
IT Risk & Cybersecurity

CYBER AB
REGISTERED PRACTITIONER

Moderated By

Carly Devlin
Shareholder
IT Risk & Cybersecurity