



# NIST 800-171 & CMMC: INSIGHTS FROM A C3PAO CANDIDATE COMPANY

**Kyle Lai & Scott Armstrong**

April 28, 2021

- Today's webinar is scheduled to last 45 min to 1 hour including Q&A.
- All participants will be muted to enable the speakers to present without interruption.
- A large portion of today's event is dedicated to answering pressing questions from the audience. Speakers will be answering questions that have been submitted prior to today's event.
- In case of outage, please wait for a minute and refresh the page.
- For your convenience, there is a link in the YouTube description to a glossary of commonly used terms, acronyms and initializations that will be referenced during today's webinar.
- This webinar is being recorded and will be available on-demand via the Exostar Resource Library ([www.Exostar.com/Resources](http://www.Exostar.com/Resources)) post-event as well as at this same YouTube link.
- To speak with one of our industry experts or request a copy of this slide deck, please reach out to us at [cmmc-pp@Exostar.com](mailto:cmmc-pp@Exostar.com) or use the live chat feature at [www.Exostar.com](http://www.Exostar.com).

## Introductions

### Pathway to CMMC – **Kyle Lai (25-30 minutes)**

- Where to begin: DFARS 252.204-7012, your NIST 800-171 self-assessment with Incident Response (IR) plan
- Reporting your compliance status to the DoD SPRS as required by DFARS 252.204-7019 & -7020
- Achieving full compliance with 110 controls of NIST 800-171
- The evolutionary progression to CMMC and the additional 20 controls (DFARS 252.204-7021)
- Evaluation – How do I know I'm truly in compliance?
- Duration of a C3PAO assessment & variables

### Q & A – Moderated by **Scott Armstrong (20)**

## Exit Poll

# Speakers



**Kyle Lai**  
KLC Consulting



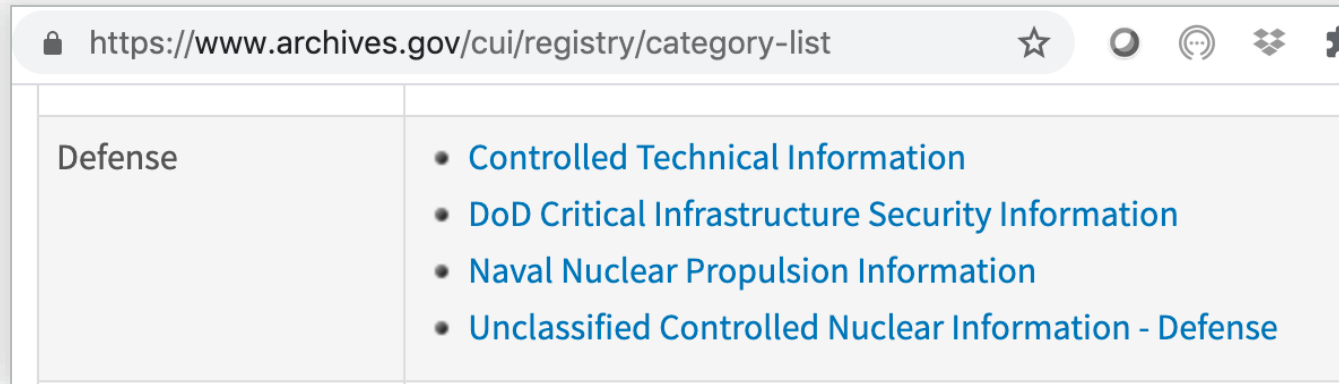
**Scott Armstrong**  
Exostar

## Controlled Unclassified Information (CUI)

Information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a **law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.**

## Federal Contract Information (FCI)

Information not intended for public release, that is provided by or generated for the U.S. Government under a contract to develop or deliver a product or service to the government, but not including information provided by the government to the public (such as on public websites).



DoD CUI Registry: <https://www.dodcui.mil/Home/DoD-CUI-Registry/>

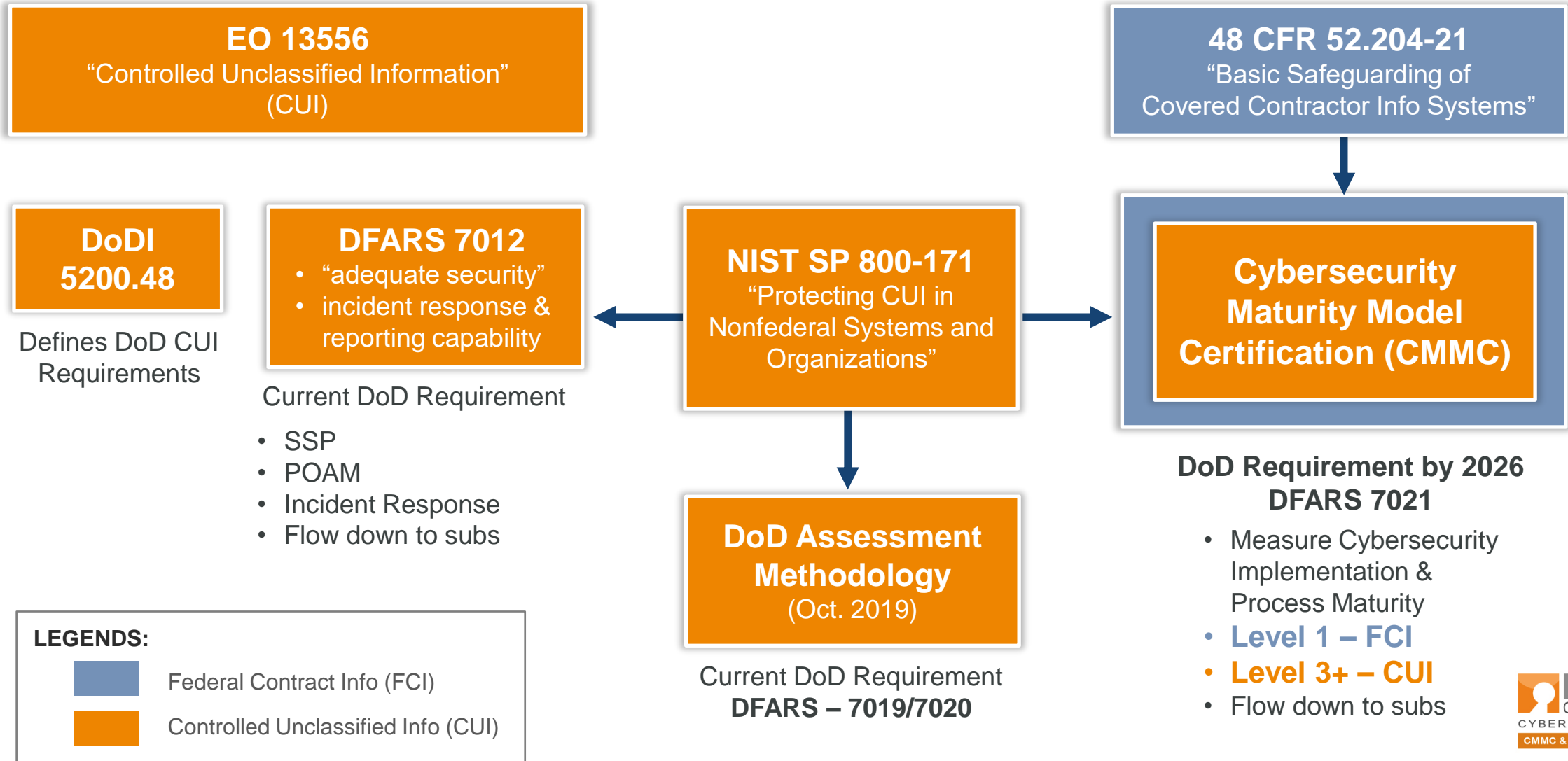
List of CUI Training: <https://www.dodcui.mil/Home/Training/>

[DoD Mandatory CUI Training](#) – Required for all DIB Contractors

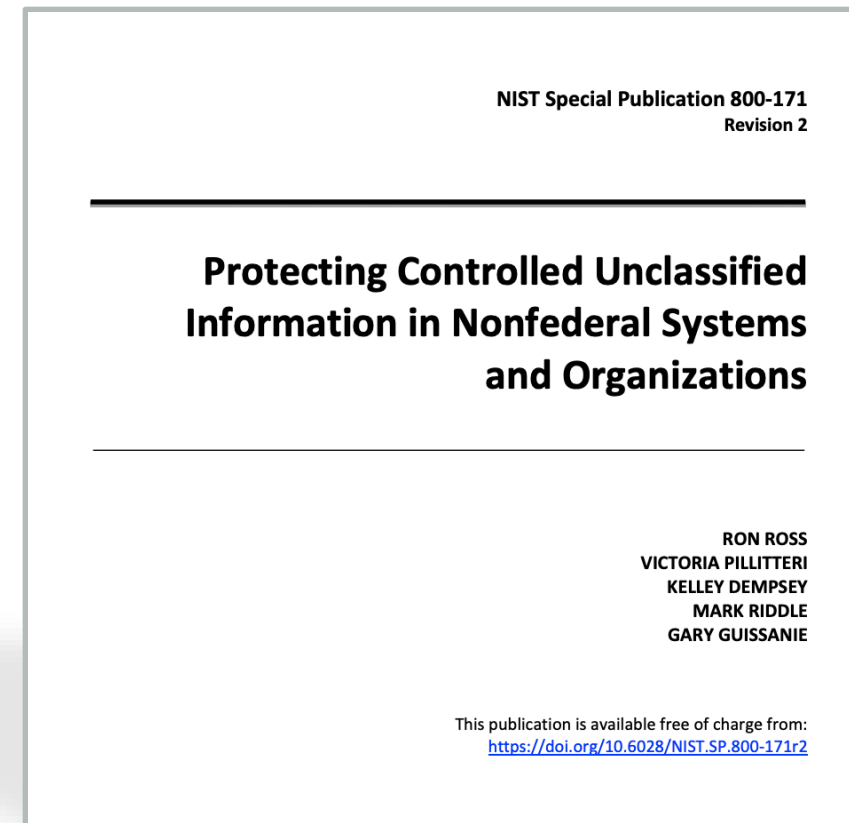
## CTI Examples:

- Research and engineering data
- Engineering drawings & lists
- Specifications
- Standards
- Process sheets
- Manuals
- Technical reports
- Computer software executable code and source code
- Conformance reports

# Regulatory Overview – CUI / FCI



- Provides security requirements for protecting CUI.
- NIST 800-171 controls apply to **U.S. Government contractors and sub-contractors**.
- If you or another company you work with has a contract with a federal agency, you must be compliant with NIST 800-171
- Self-Assessment required since December 31, 2017
- Required pursuant to DFARS 252.204-7012

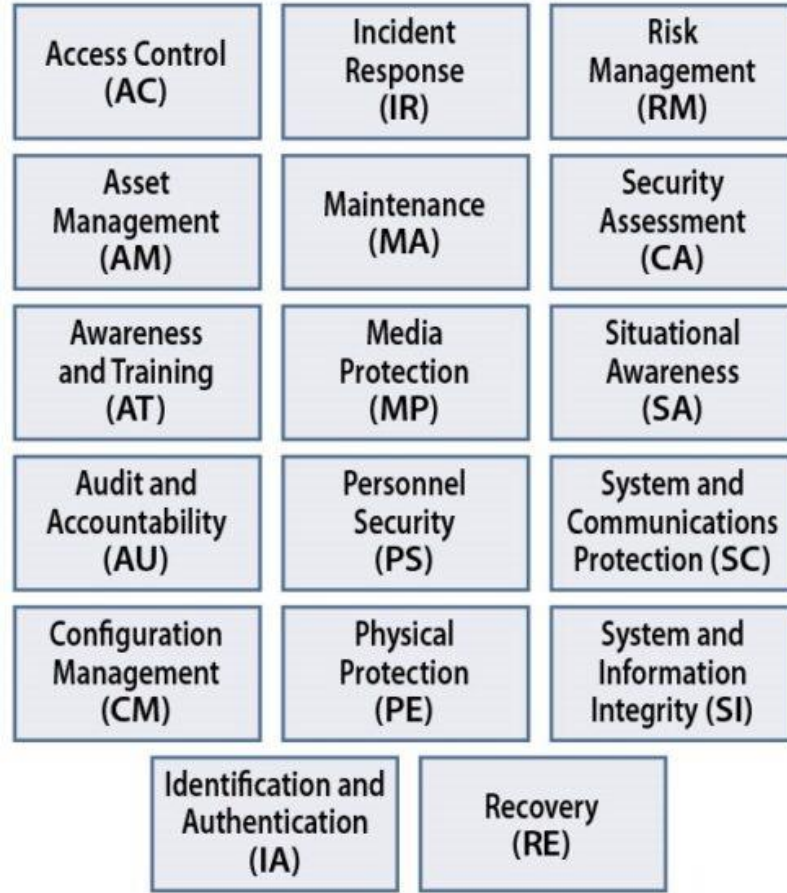




- Cybersecurity Maturity Model Certification (CMMC)
- Cybersecurity requirements from the DoD to Defense Industrial Base (DIB) companies.
- Provides increased assurance to DoD that a DIB company can **adequately protect** sensitive unclassified information and is **accountable** for information flow down to subcontractors in a multi-tier supply chain.
- 5 different maturity levels (ML1 - ML5)
- Verification of processes and practices for required maturity level
- Requires certification assessment by a CMMC Third-Party Assessment Organization (C3PAO)
- CMMC approval is granted by CMMC Accreditation Body (CMMC-AB)
- Required in select contracts during 2021 – 2025, all contracts starting in 2026.



## 17 Capability Domains (v1.0)



## CMMC Model with 5 levels measures cybersecurity maturity



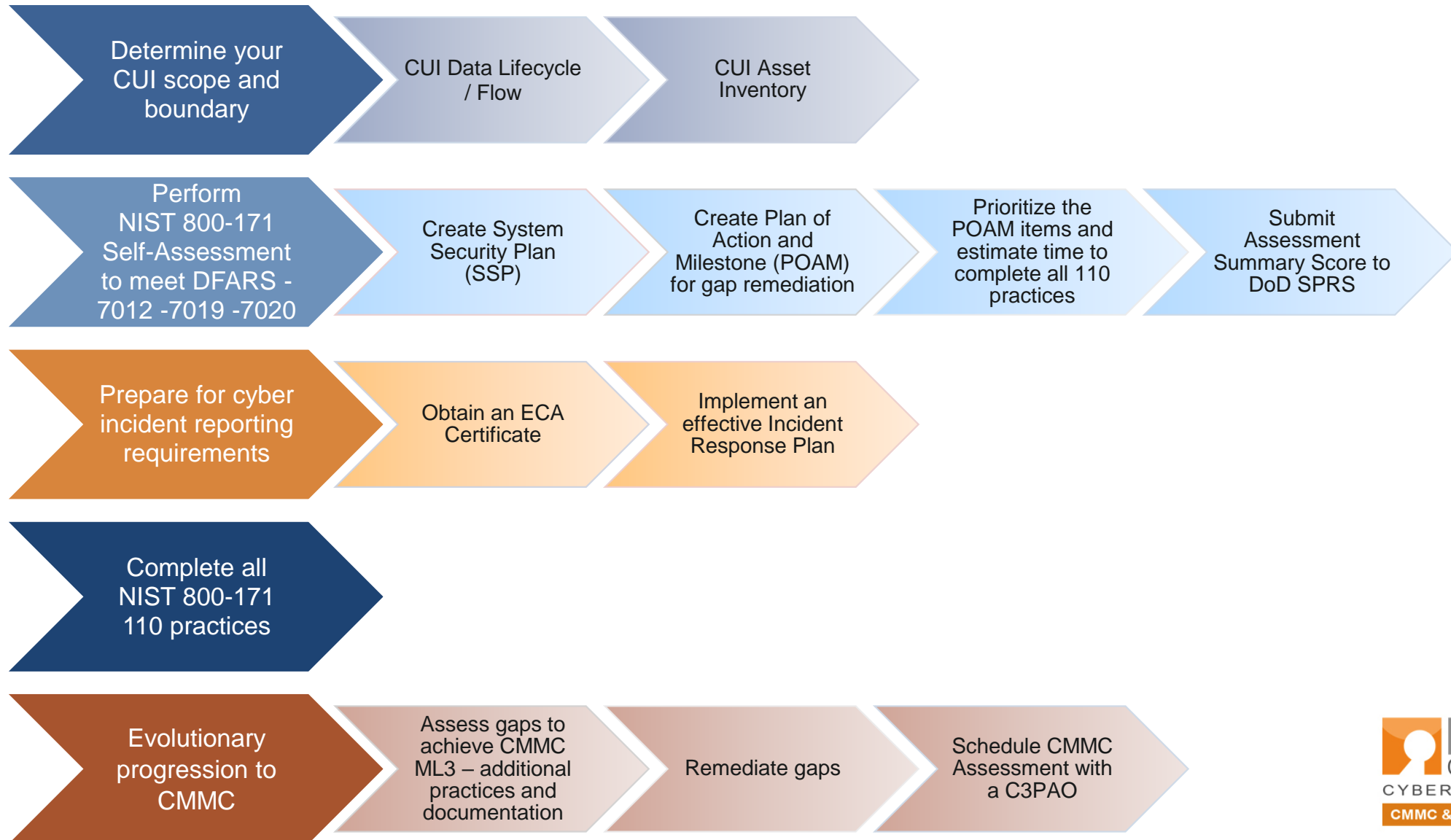
DISTRIBUTION A. Approved for public release

## Safeguarding Covered Defense Information and Cyber Incident Reporting

### DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1. Provide **adequate security** to safeguard **covered defense information** that resides on or transits through a **contractor's internal information system or network (NIST 800-171)**
2. Report cyber incidents that affect a **covered contractor information system** or the **covered defense information** residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support **within 72 hours of discovery**
3. **Submit malicious software** discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
4. If requested, submit media and additional information to support damage assessment
5. Flow down the requirements to subcontractors who perform operationally critical support, or for which subcontract performance will involve covered defense information

# Ready For Your Journey to CMMC Maturity Level 3



# How Do I Know I Am Ready for CMMC Level 3?

## Scoping

- Have you done an explicit scoping of your environment for the assessment?

## SSP, Policies, Procedures, Processes, Plans

- Are your procedures and processes finalized, aligned, and supporting the SSP and policies?
- Have evidence to show effectiveness for each practice assessment objective?
- Have you identified roles and responsibilities for each policy, procedure, and plan?
- The staff with identified roles will be interviewed during the assessment
- Cloud/MSP Customer Responsibility Matrix referenced or inherited in the SSP, policy, and procedures?

## Have you

- Conducted a self-assessment with [CMMC Assessment Guide](#) (AG) and gotten your compliance status?
- Closed all Plan of Action (POA) Items?
- Added Cloud / MSP's Customer Responsibilities Matrix actions to your procedures?
- Confirmed you had met all Practice Assessment Objectives specified in CMMC AG

## Access Control (AC)

### Level 1 AC Practices

#### **AC.1.001**

---

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

#### **ASSESSMENT OBJECTIVES [NIST SP 800-171A]**

---

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).

- **Confirm required documentation is in place (CMMC ML3 Assessment Guide)**
  - CMMC SSP for all 130 practices
  - Policies, procedures, processes and plans requirements (Know your policies & procedures)
  - Evidence of effectiveness for all practice assessment objectives (internal and outsourced)
  - Evidence of flow down to subs
  - CUI scope & boundary diagram
  - **NOTE: All 130 practices must be implemented - no POAM for CMMC gaps!**
  - **NOTE: If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a NOT MET for the practice or process. (per CMMC ML3 Assessment Guide)**
- **Engage services of a C3PAO to perform the CMMC ML3 assessment**
  - Schedule and perform CMMC ML3 assessment
- **CMMC-AB must evaluate and validate the C3PAO assessment package**
  - If no issues CMMC-AB will grant the CMMC ML3 Certification

**NOTE: The certification process may take about 3 months. Plan Accordingly!**



## **Kyle Lai**

*President & CISO*

KLC Consulting, Inc.



[Klai@klcconsulting.net](mailto:Klai@klcconsulting.net)



[@KyleOnCyber](https://twitter.com/KyleOnCyber)



<https://www.Linkedin.com/in/kylelai>



[KLC Consulting Youtube Channel on CMMC](#)

[www.klcconsulting.net](http://www.klcconsulting.net)

[cmmc@klcconsulting.net](mailto:cmmc@klcconsulting.net)

# Thank you!























## About KLC Consulting

- KLC is a CMMC-AB approved C3PAO (pending CMMC ML3 Assessment) company incorporated in 2002. We specialize in providing NIST 800-171, DFARS 7012 and CMMC consulting solutions to medium-sized Defense Industrial Based (DIB) companies who seek CMMC Maturity Level 3 certification.
- Accurate and complete CUI scoping is critical to your ML3 certification. We utilize our proprietary “CUI Data Lifecycle” approach to scoping and managing CUI in the 17 CMMC Capability Domain Processes and Practices.

- As part of our flexible consulting service model, KLC **only** staffs exceptionally talented and highly specialized cybersecurity personnel resources who support all areas of NIST 800-171, DFARS and CMMC compliance requirements. We possess the highest level of expertise and professional certification including:

 CMMC AB - Provisional Assessor	 CISM - Certified Information Security Manage	 CDPSE - Certified Data Privacy Solutions Engineer
 CISSP - Certified Information Systems Security Professional	 CIPP/US - Certified Information Privacy Professionals/Private	 CCNA - Cisco Certified Network Associate
 CISA - Certified Information Systems Auditor	 Cisco Certified Network Associate Routing and Switching	 Redhat Engineer
 CIPP/G - Certified Information Privacy Professionals/Government	 CMMC AB - Registered Practitioner	 CCSK - Certificate of Cloud Security Knowledge
 CCSP - Certified Cloud Security Professional	 CSSLP - Certified Secure Software Lifecycle Professional	 ACE - Palo Alto Networks
 MCSE - Microsoft Certified Systems Engineer	 CRISC - Certified in Risk and Information System Control	 DISA - System Administrator

- And we are without equal in quality and quantity of informational and educational CMMC cybersecurity videos, and written content we create and publish through our [YouTube Channel](#), our [vBlog page](#), and our [LinkedIn page](#). We inspire greater awareness and understanding of CMMC compliance because we continuously strive to improve and innovate. And we align ourselves with like-minded people who also strive to be the best within their specialized area of practice.
- [Please check out our website](#). And [Our CMMC services page](#) with 11m CMMC Overview Video.

# Useful sources of information

- Learn more about CUI at <https://www.dodcui.mil/>
- CMMC Accreditation Body website <https://cmmcab.org/>
- DoD Procurement reference website <https://dodprocurementtoolbox.com/>
- DoD CMMC Acquisition website <https://www.acq.osd.mil/cmmc/index.html>

Summary of the SPRS process with links to authoritative PIEE and SPRS materials hosted by DoD  
<https://www.exostar.com/blog/nist-800-171-basic-assessment-reporting-easy-as-1-2-3/>

- Exostar Partner Listing <https://www.exostar.com/partners/> (note – select CMMC)

## Free Trial Information:

- Exostar Certification Assistant <https://www.exostar.com/product/certification-assistant/>
- Exostar PolicyPro <https://www.exostar.com/product/policypro/>

---

# Q&A

---

# Exit Poll

See link in YouTube description

---

# Thank you for joining us.

[cmmc-team@exostar.com](mailto:cmmc-team@exostar.com)

**EXOSTAR<sup>®</sup>**

We build trust.

