CMMC Update & Tools to Assist Your Clients

by KLC Consulting, Inc.

A DoD/Cyber AB Authorized C3PAO

March 2024

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Kyle Lai

President and CISO
KLC Consulting

CMMC-CCA, CCP, CISSP, CSSLP, CISA, CDPSE, CIPP/US/G

Email: Klai@klcconsulting.net

LinkedIn: https://www.linkedin.com/in/kylelai

YouTube

- Nationally recognized as a CMMC cybersecurity expert with over 20 years of experience, Kyle architects NIST 800-171 and CMMC compliance solutions for the Defense Industrial Base (DIB).
- His distinguished career includes cybersecurity advisor roles at ExxonMobil, Zoom, DISA, Boeing, and Microsoft. Kyle specializes in efficient CMMC compliance and serves manufacturers, aerospace, software, engineering, and IT/MSP companies.

About KLC Consulting

- Founded in 2002, we bring decades of experience and the powerful advocacy of an authorized C3PAO to the table.
- Our collaborative approach alleviates stress and inspires confidence.
- We’ll get you CMMC certified so you can win more DoD contracts and grow your business.

Agenda

- CMMC Update – The CMMC Proposed Rule
- 5 Tools to Assist Your Clients with CMMC
- Q&A

CMMC Acronyms

C3PAO	CMMC Third-Party Assessment Organization
CAICO	CMMC Assessors and Instructors Certification Organization
CAGE	Commercial and Government Entity
CCA	CMMC Certified Assessor
CCP	CMMC Certified Professional
CFR	Code of Federal Regulations
CMMC	Cybersecurity Maturity Model Certification
CMMC PMO	CMMC Program Management Office
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
ESP	External Service Provider
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FedRAMP	Federal Risk and Authorization Management Program
IoT	Internet of Things
IR	Incident Response
MSP	Managed Service Provider

MSSP	Managed Security Service Provider
NARA	National Archives and Records Administration
NAICS	North American Industry Classification System
NIST	National Institute of Standards and Technology
N/A	Not Applicable
ODP	Organization-Defined Parameter
OSA	Organization Seeking Assessment
OSC	Organization Seeking Certification
OT	Operational Technology
PIEE	Procurement Integrated Enterprise Environment
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
RM	Risk Management
SAM	System for Award Management
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SP	Special Publication
SPRS	Supplier Performance Risk System
SSP	System Security Plan

FCI & CUI

FCI = Federal Contract Information

Information not intended for public release, that is provided by or generated for the 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.

CUI = Controlled Unclassified Information

Government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

CMMC Proposed Rule – Overview

- Title 32 CFR Part 170 - Released 12/26/2023
- Incorporates NIST 800-171 Rev 2. (No reference to Rev 3)
- The 60-day public comment period ended 2/26/2024
- We’re now in the DoD response period (up to 280 days)
- The CMMC Ecosystem estimates the updated DFARS 252.204-7021 (CMMC) will be issued in Q2-Q3 of 2025

Optional Early Recognition

- Joint Surveillance Voluntary Assessment (JSVA) – DoD will convert it to CMMC L2 Certification <u>IF all controls are MET with NO POA&M items</u>

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

CMMC Proposed Rule – Overview

4 Types of Assessments

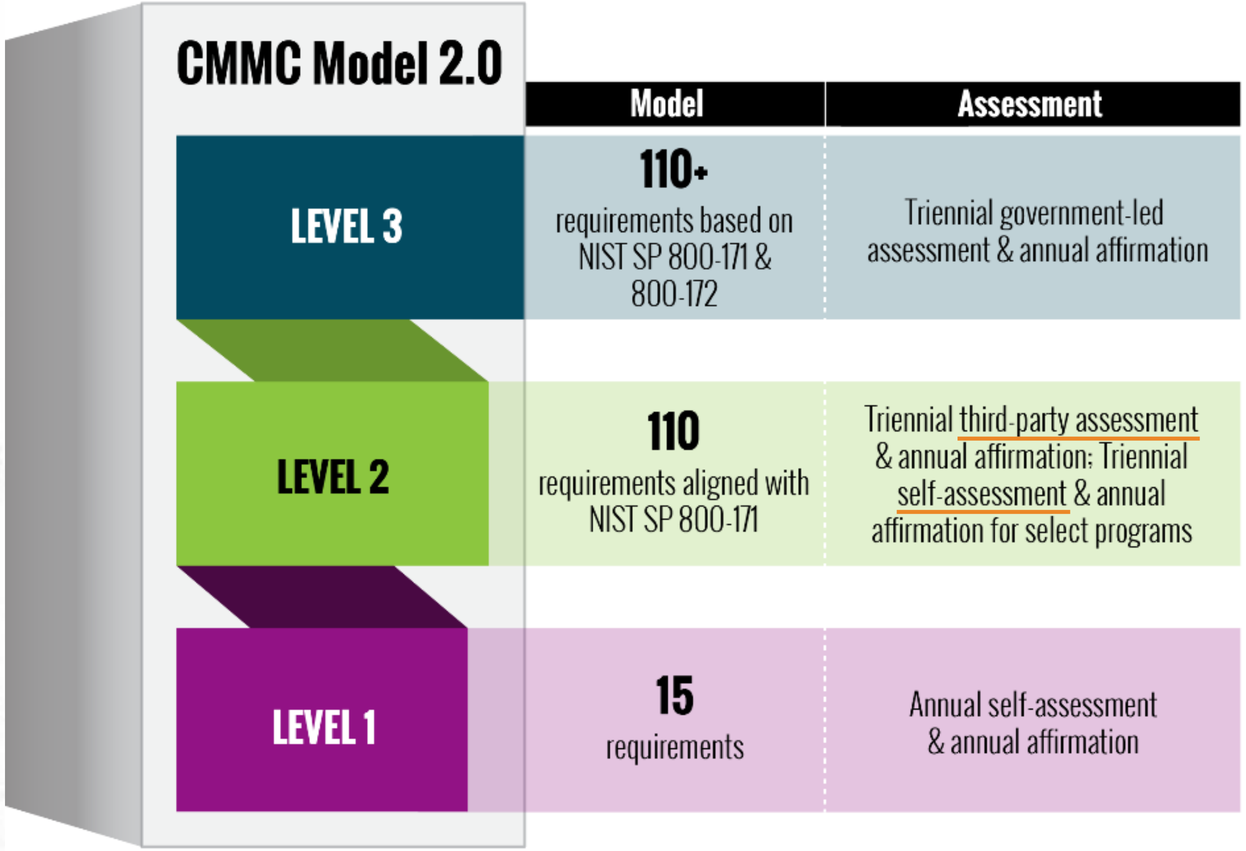
- **Level 1:** Self-Assessment
- **Level 2:** Self-Assessment
  Certification Assessment (C3PAO)
- **Level 3:** Certification Assessment (DoD)

External Service Provider

(ESP) processes, stores, or transmits CUI or Security Protection Data (i.e., security logs) via the ESP’s assets must get CMMC Level 2 or higher Certification

Cloud Service Provider

(CSP) must have FedRAMP Moderate or Equivalency



CMMC Model 2.0

	Model	Assessment
LEVEL 3	**110+** requirements based on NIST SP 800-171 & 800-172	Triennial government-led assessment & annual affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171	Triennial third-party assessment & annual affirmation; Triennial self-assessment & annual affirmation for select programs
LEVEL 1	**15** requirements	Annual self-assessment & annual affirmation

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

DoD’s Estimated Number of OSAs / OSCs

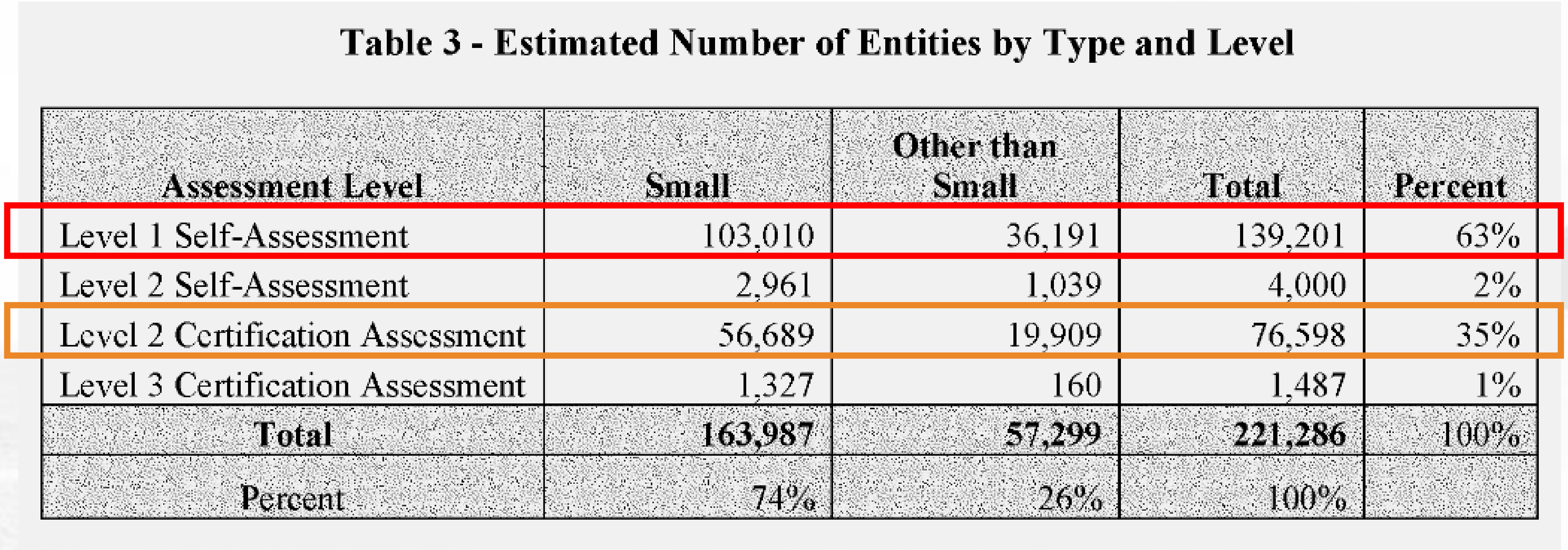


Table 3 - Estimated Number of Entities by Type and Level

Assessment Level	Small	Other than Small	Total	Percent
Level 1 Self-Assessment	103,010	36,191	139,201	63%
Level 2 Self-Assessment	2,961	1,039	4,000	2%
Level 2 Certification Assessment	56,689	19,909	76,598	35%
Level 3 Certification Assessment	1,327	160	1,487	1%
Total	**163,987**	**57,299**	**221,286**	100%
Percent	74%	26%	100%	

Source: CMMC Proposed Rule (32 CFR Part 170)

Level 1 – Self-Assessment

Level 1 Self-Assessment Requirements

- Performed annually
- Results entered in the Supplier Performance Risk System (SPRS)
- POA&M: **No POA&M is allowed**
- **Annual Affirmation**:
  - A company senior official annually affirms continuing compliance with the specified security requirements
  - **Affirmations are entered in SPRS**
- New numbering based on FAR 52.204-21 numbering scheme
- Requirements flow down to subcontractors

Level 2 – Certification Assessment

Level 2 Certification Assessment Requirements

- Assessed (audited) by a C3PAO triennially (once every three years)
- Specialized Assets (e.g., IoT, OT) aren’t assessed (if not used for CMMC L3 Certification) but must be documented in the SSP
- C3PAO enters results into the eMASS reporting system (managed by DoD)
    - Results transfer to the SPRS system
- POA&M Allowed: Non-critical NIST 800-171 security practices are allowed but must be closed within 180 days of the assessment (Only applies if 80%+ (88+) of the 110 requirements are MET)
- **Annual Affirmation**:
    - A company senior official affirms continuing compliance after every assessment
    - **Affirmations are entered in SPRS**
- **Retain artifacts for a minimum of 6 years**
- New numbering scheme – aligns with Level 2 Assessment Guide.
    - Level 2 assessments/certifications will only assess CUI, not FCI.
- Requirements flow down to subcontractors

DoD’s Estimate of Company Assessments

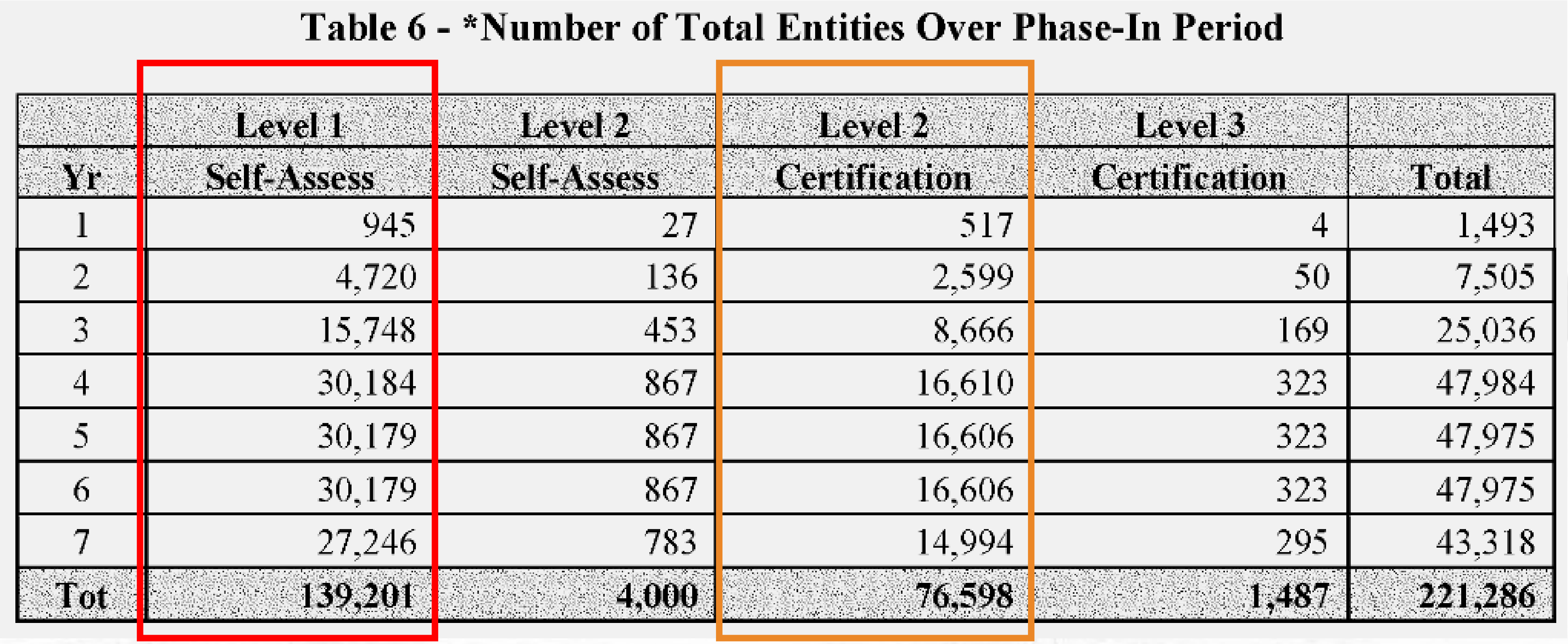
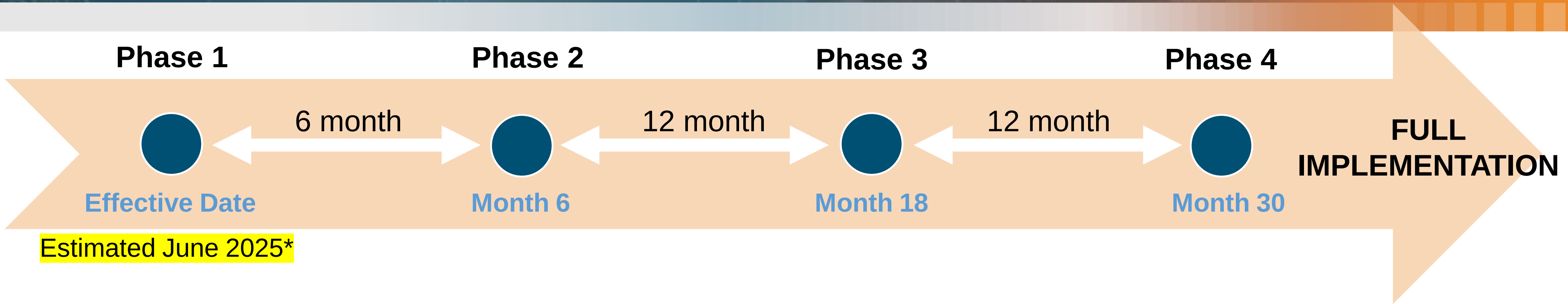


Table 6 - *Number of Total Entities Over Phase-In Period

	Level 1	Level 2	Level 2	Level 3	
Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	945	27	517	4	1,493
2	4,720	136	2,599	50	7,505
3	15,748	453	8,666	169	25,036
4	30,184	867	16,610	323	47,984
5	30,179	867	16,606	323	47,975
6	30,179	867	16,606	323	47,975
7	27,246	783	14,994	295	43,318
Tot	139,201	4,000	76,598	1,487	221,286

Source: CMMC Proposed Rule (32 CFR Part 170)
Note: This estimate does not include organizations requiring re-certifications after 3 years.

CMMC Program Implementation – 4 Phases



Estimated June 2025*

- **PHASE 1:** Begins on the date of CMMC implementation – requires Level 1 and Level 2 **Self-Assessment**
- **PHASE 2 (Month 6):** Begins six months after Phase 1 – requires **CMMC Level 2 Certification Assessment on new contracts**.
- **PHASE 3 (Month 18):** Begins one year after Phase 2 –
  - requires CMMC Level 3 Assessment-Certification
  - requires **Level 2 Assessment-Certification** for all applicable contracts and option periods started **before the effective date**.
- **PHASE 4 (Month 30):** **Full implementation** one year after Phase 3 begins, **mandatory for all applicable DoD contracts**.

5 Useful Tools To Assist Your Clients

TOOL 1: Typical Journey to CMMC

TOOL 2: Objective Evidence List

TOOL 3: Free Cybersecurity & CUI Training

TOOL 4: Decision for FCI, CUI, Public Info

TOOL 5: CUI Data Flow - Discovery Questions

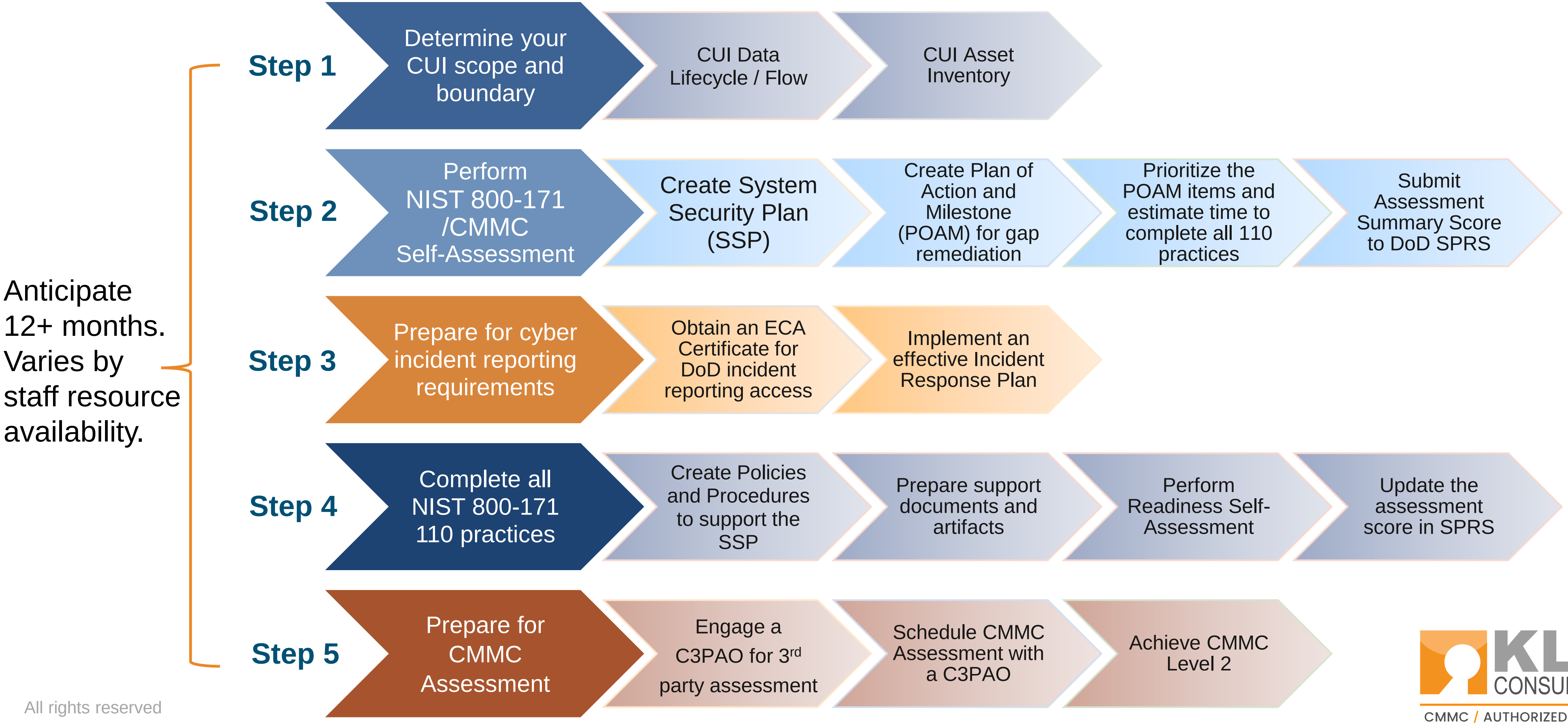
Available for download:

https://klcconsulting.net/napex

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 1: Typical Journey to CMMC Level 2 Certification

(created by KLC Consulting)



Anticipate 12+ months. Varies by staff resource availability.

Step 1
- Determine your CUI scope and boundary
- CUI Data Lifecycle / Flow
- CUI Asset Inventory

Step 2
- Perform NIST 800-171 /CMMC Self-Assessment
- Create System Security Plan (SSP)
- Create Plan of Action and Milestone (POAM) for gap remediation
- Prioritize the POAM items and estimate time to complete all 110 practices
- Submit Assessment Summary Score to DoD SPRS

Step 3
- Prepare for cyber incident reporting requirements
- Obtain an ECA Certificate for DoD incident reporting access
- Implement an effective Incident Response Plan

Step 4
- Complete all NIST 800-171 110 practices
- Create Policies and Procedures to support the SSP
- Prepare support documents and artifacts
- Perform Readiness Self-Assessment
- Update the assessment score in SPRS

Step 5
- Prepare for CMMC Assessment
- Engage a C3PAO for 3rd party assessment
- Schedule CMMC Assessment with a C3PAO
- Achieve CMMC Level 2

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 2: CUI Data Flow Discovery (created by KLC Consulting)

To Document CUI Flow, Scope, and Roles & Responsibilities

Document each stage of CUI flow through your business:

Stage 1: CUI Receipt/Input/Creation:

- Who receives/creates CUI?
- What type of CUI do people receive/create?
- What methods do people use to acquire CUI?
- What system(s) do people use to process CUI?
- What system(s) do people use to store CUI?
- Who do people notify after receiving CUI (manually or automatically)?

Stage 2: CUI Flow (through Each Successive Process or Department):

- What do the responsible people do with the CUI they receive?
- What system(s) are used to process CUI?
- What system(s) are used to store CUI?
- Who does the person notify in the next Process or Department?
- Continue Stage 2 through successive Processes/Departments leading to Product or Service delivery)

Stage 3: Product or Service Delivery:

- What do people do with CUI before customer delivery?
- Is there any CUI attached to the products/services delivered? (I.e., technical report, test results)
- What steps do people take to archive CUI (if required to store for an extended period)?
- For paper CUI, how do people store (I.e., file cabinet) or destroy (I.e., shredding) CUI?

CUI Scoping Considerations

People

- Employees
- Contractors
- Vendors
- External Service Provider Personnel

Technologies

- Computers (servers, laptops,.)
- Firewall / VPN
- Applications, Database
- Devices (USB, external hard drives)

Facilities

- Physical Office Locations
- Satellite Offices
- Secure rooms, Data Centers
- Manufacturing Plants

External Service Providers

- Cloud Service Providers (CSP)
- Data Center Providers
- Hosting Providers (i.e., website)
- Managed Service Providers (MSP)

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 3: Objective Evidence List (Created by DCMA DIBCAC)

OBJECTIVE	SECURITY REQUIREMENT	TEAM INPUT	EVIDENCE EXAMPLES (ASSESSORS ARE NOT LIMITED OR RESTRICTED TO EXAMPLES)	CMMC ASSESSMENT CONSIDERATIONS (CMMC Assessment Guide - Level 2)
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			
3.1.1[a]	Authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	Is a list of authorized users maintained that defines their identities and roles?
3.1.1[b]	Processes acting on behalf of authorized users are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[c]	Devices (and other systems) authorized to connect to the system are identified.	Screen Share	Document defining account request, approval, provisioning.	
3.1.1[d]	System access is limited to authorized users.	Screen Share	Screen share showing login requirements are enforced. Example of an unauthorized user denied (Unauthorized username entered at login)	Are account requests authorized before system access is granted?
3.1.1[e]	System access is limited to processes acting on behalf of authorized users.	Screen Share	Screen shot showing that service accounts are assigned to authorized users only. No rogue accounts without an authorized user are active.	Are account requests authorized before system access is granted?
3.1.1[f]	System access is limited to authorized devices (including other systems).	Screen Share	Screen share showing that all devices running are authorized. No rogue devices on the network.	Are account requests authorized before system access is granted?
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.			
3.1.2[a]	The types of transactions and functions that authorized users are permitted to execute are defined.	Document	SSP, AUP, or IAM document that defines what authorized users can execute.	Are access control lists used to limit access to applications and data based on role and/or identity?
3.1.2[b]	System access is limited to the defined types of transactions and functions for authorized users.	Screen Share	Screen shot of security roles in AD or IAM tool that shows transactions are as defined in the SSP or IAM document. Priveleged and Non-priveleged accounts need to be defined and identified in the artifact. Screenshot of a non-priveleged user trying to execute a priveleged function.	Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools)?

Tool 4: Free CMMC Training Resources (created by KLC Consulting)

To Meet Cybersecurity Training Requirements for CMMC 3.2.x

FREE DoD-developed cybersecurity training for Regular and Privileged Users:

We’ve aggregated this list of free DoD-required training for the protection of CUI and FCI data.

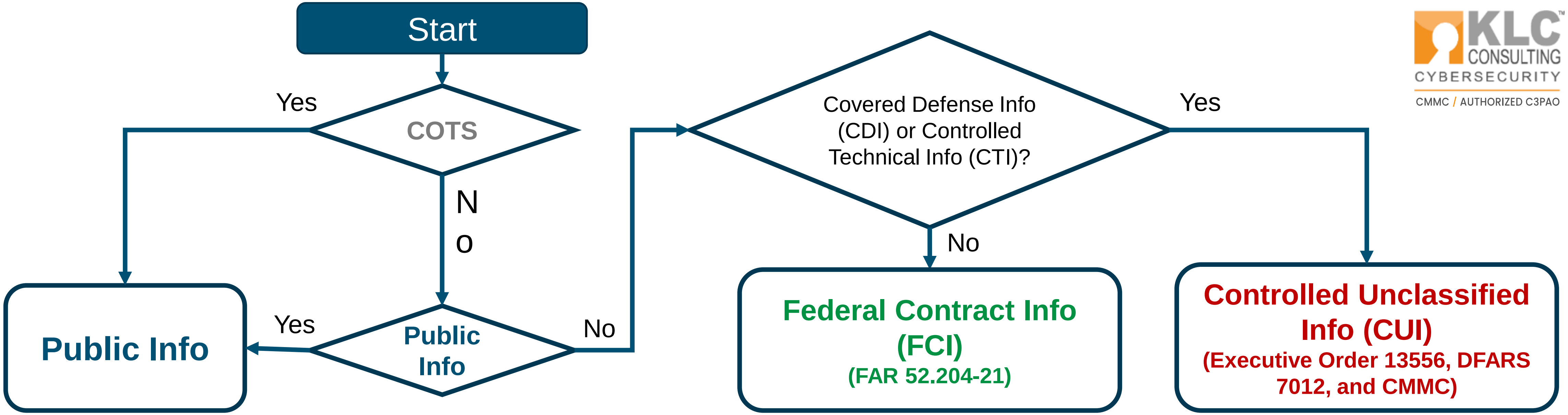
- **(All users) DoD Cyber Awareness training –** https://public.cyber.mil/training/cyber-awareness-challenge/
  - This training covers cybersecurity awareness, phishing, insider threats, social media security
- (All users) DoD **Insider Threat** Awareness Training - https://securityawareness.usalearning.gov/itawareness/index.htm
  - This training covers the Insider Threat training
- (CUI users) DoD Mandatory **CUI** Training - https://securityhub.usalearning.gov/index.html
  - This training covers the definition and nature of CUI and the proper handling of CUI

Privileged Users Training:

- DoD **Privileged Users** Training https://www.cdse.edu/Training/eLearning/DS-IA112/
  - This training covers the additional cybersecurity responsibilities for privileged users

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Tool 5: Decision Tree to Distinguish FCI, CUI, & Public Info (created by KLC Consulting)



Start

COTS

Yes

No

Public Info

Public Info

Yes

No

Covered Defense Info (CDI) or Controlled Technical Info (CTI)?

No

Yes

Federal Contract Info (FCI)
(FAR 52.204-21)

Controlled Unclassified Info (CUI)
(Executive Order 13556, DFARS 7012, and CMMC)

COTS (Commercially Off-The-Shelf) = software and hardware that already exists and is available from commercial sources. It is also referred to as off-the-shelf.

Controlled Technical Information (CTI) = technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

FCI = Information not intended for public release, that is provided by or generated for the 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.

Covered Defense Information (CDI) = unclassified controlled technical information (CTI), DoD critical infrastructure security information, naval nuclear propulsion info, and DoD unclassified controlled nuclear info.

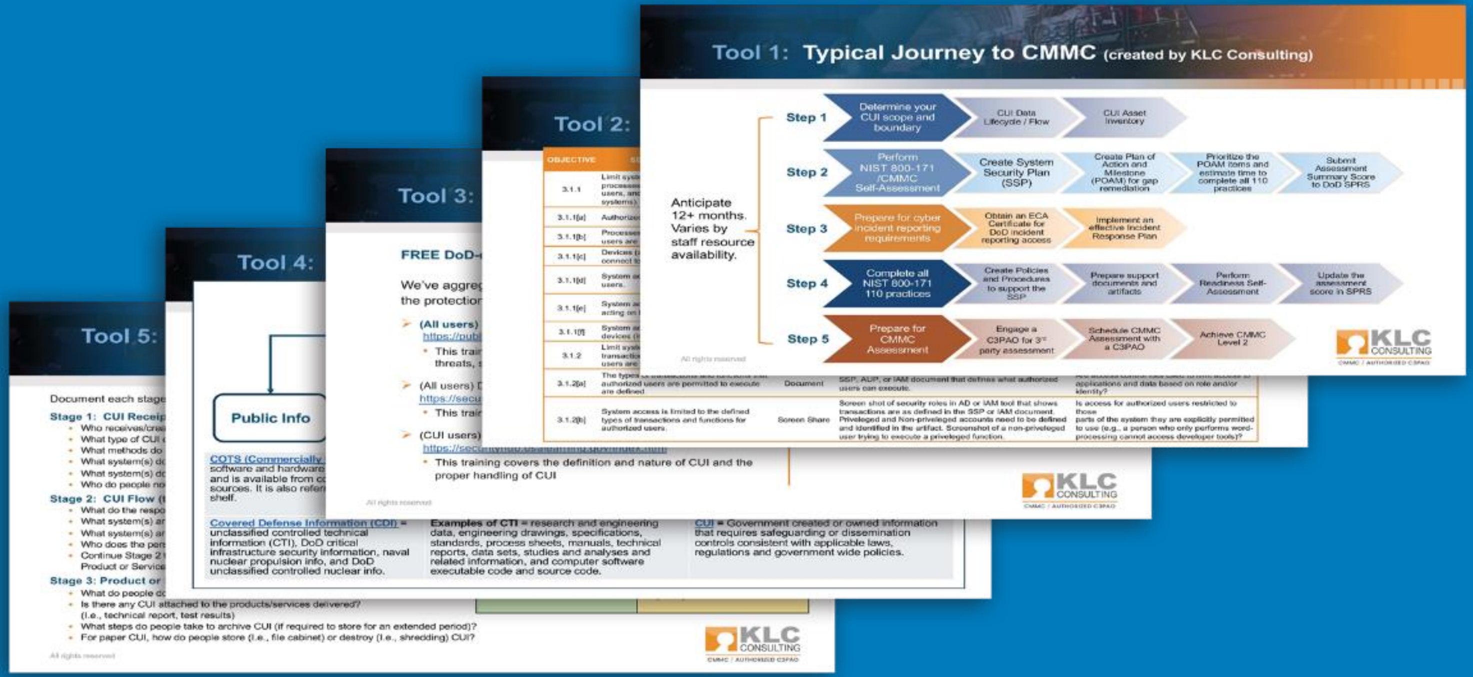
Examples of CTI = research and engineering data, engineering drawings, specifications, standards, process sheets, manuals, technical reports, data sets, studies and analyses and related information, and computer software executable code and source code.

CUI **=** Government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

Download Our Tools at: https://kcconsulting.net/napex

5 Useful Tools To Assist Your Clients

Scan QR Code to Download



Tool 1: Typical Journey to CMMC (created by KLC Consulting)

Anticipate 12+ months. Varies by staff resource availability.

- Step 1: Determine your CUI scope and boundary → CUI Data Lifecycle / Flow → CUI Asset Inventory
- Step 2: Perform NIST 800-171 /CMMC Self-Assessment → Create System Security Plan (SSP) → Create Plan of Action and Milestone (POAM) for gap remediation → Prioritize the POAM items and estimate time to complete all 110 practices → Submit Assessment Summary Score to DoD SPRS
- Step 3: Prepare for cyber incident reporting requirements → Obtain an ECA Certificate for DoD incident reporting access → Implement an effective Incident Response Plan
- Step 4: Complete all NIST 800-171 110 practices → Create Policies and Procedures to support the SSP → Prepare support documents and artifacts → Perform Readiness Self-Assessment → Update the assessment score in SPRS
- Step 5: Prepare for CMMC Assessment → Engage a C3PAO for 3rd party assessment → Schedule CMMC Assessment with a C3PAO → Achieve CMMC Level 2

All rights reserved

KLC CONSULTING CMMC / AUTHORIZED C3PAO

Tool 2:

OBJECTIVE				
3.1.1	Limit sys processes users, and systems)			
3.1.1[a]	Authorize			
3.1.1[b]	Processes users are			
3.1.1[c]	Devices (connect t			
3.1.1[d]	System a users.			
3.1.1[e]	System a acting on			
3.1.1[f]	System a devices (			
3.1.2	Limit syst transactio users are			
3.1.2[a]	The types of transactions and functions that authorized users are permitted to execute are defined	Document	SSP, AUP, or IAM document that defines what authorized users can execute.	Are access control lists used to limit access to applications and data based on role and/or identity?
3.1.2[b]	System access is limited to the defined types of transactions and functions for authorized users.	Screen Share	Screen shot of security roles in AD or IAM tool that shows transactions are as defined in the SSP or IAM document. Priveleged and Non-priveleged accounts need to be defined and identified in the artifact. Screenshot of a non-priveleged user trying to execute a priveleged function.	Is access for authorized users restricted to those parts of the system they are explicitly permitted to use (e.g., a person who only performs word-processing cannot access developer tools)?

Tool 3:

FREE DoD-

We've aggreg the protection

- (All users) https://publ
  - This trai threats,
- (All users) https://secu
  - This trai
- (CUI users) https://securityhub.usalearning.gov/index.html
  - This training covers the definition and nature of CUI and the proper handling of CUI

All rights reserved

Tool 4:

Public Info

COTS (Commercially software and hardware and is available from c sources. It is also refer shelf.

Covered Defense Information (CDI) = unclassified controlled technical information (CTI), DoD critical infrastructure security information, naval nuclear propulsion info, and DoD unclassified controlled nuclear info.

Examples of CTI = research and engineering data, engineering drawings, specifications, standards, process sheets, manuals, technical reports, data sets, studies and analyses and related information, and computer software executable code and source code.

CUI = Government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies.

Tool 5:

Document each stage

Stage 1: CUI Receip

- Who receives/crea
- What type of CUI
- What methods do
- What system(s) do
- What system(s) do
- Who do people no

Stage 2: CUI Flow (

- What do the respo
- What system(s) ar
- What system(s) ar
- Who does the pers
- Continue Stage 2 Product or Service

Stage 3: Product or

- What do people do
- Is there any CUI attached to the products/services delivered? (I.e., technical report, test results)
- What steps do people take to archive CUI (if required to store for an extended period)?
- For paper CUI, how do people store (I.e., file cabinet) or destroy (I.e., shredding) CUI?

All rights reserved

KLC CONSULTING CMMC / AUTHORIZED C3PAO

KLC CONSULTING

CMMC / AUTHORIZED C3PAO

FREE 2-Hour CMMC Workshop for Any APEX Accelerator

KLC Consulting empowers small businesses to pursue certification in CMMC with ***confidence***

FREE CMMC WORKSHOP

For any local APEX Accelerator, KLC Consulting offers a **no-cost, 2-hour CMMC workshop** to demystify **CMMC** for you and your clients.

KLC CONSULTING
CMMC / AUTHORIZED C3PAO

Contact Information

KLC™ CONSULTING
CYBERSECURITY
CMMC / AUTHORIZED C3PAO

Kyle Lai, CMMC-CCA, CISSP, CSSLP
klai@KLCConsulting.net

✉ cmmc@klcconsulting.net

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

▶ KLC Consulting Youtube Channel on CMMC

www.klcconsulting.net

Thank you!