Office of the Under Secretary of Defense for Acquisition & Sustainment

Cybersecurity Maturity Model Certification

Frequently Asked Questions

1 - What is Controlled Unclassified Information (CUI)?

CUI is information the 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.

A CUI Registry provides information on the specific categories and subcategories of information that the Executive branch protects. The CUI Registry can be found at: https://www.archives.gov/cui and includes the following organizational index groupings:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal

- Natural and Cultural Resources
- NATO
- Nuclear
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax

Resources, including online training to better understand CUI can be found on National Archives' website at https://www.archives.gov/cui/training.html

2 - What is the difference between CUI and FOUO?

CUI, established by Executive Order 13556, is an umbrella term for all unclassified information that requires safeguarding. FOUO, which stands for 'For Official Use Only', is a document designation used by the DoD.

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845

3 - What are the concerns regarding cybersecurity in the Defense Industrial Base (DIB)?

The aggregate loss of controlled unclassified information (CUI) from the DIB sector increases risk to national economic security and in turn, national security. In order to reduce this risk, the DIB sector must enhance its protection of CUI in its networks.

The Council of Economic Advisers, an agency within the Executive Office of the President, estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 Billion in 2016 [Ref: "The Cost of Malicious Cyber Activity to the U.S. Economy, CEA" in February 2018].

The Center for Strategic and International Studies (CSIS), in partnership with McAfee, reports that as much as $600 Billion, nearly 1% of global GDP, may be lost to cybercrime each year. The estimate is up from a 2014 study that put global losses at about $445 Billion. [Ref: "Economic Impact of Cybercrime - No Slowing Down" in February 2018].

4 - What is CMMC?

CMMC stands for "Cybersecurity Maturity Model Certification". The CMMC will encompass multiple maturity levels that ranges from "Basic Cybersecurity Hygiene" to "Advanced". The intent is to identify the required CMMC level in RFP sections L and M and use as a "go / no go decision."

5 - Why is the CMMC being created?

DOD is planning to migrate to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

6 - When will the final CMMC framework be released to the public?

Version 1.0 of the CMMC framework will be available in January 2020 to support training requirements. In June 2020, industry should begin to see the CMMC requirements as part of Requests for Information.

7 - Will other Federal (non DoD) contracts use CMMC?

8 - What is the relationship between NIST SP 800-171 rev.1 and CMMC?

The intent of the CMMC is to combine various cybersecurity control standards such as NIST SP 800-171, NIST SP 800-53, ISO 27001, ISO 27032, AIA NAS9933 and others into one unified standard for cybersecurity. In addition to cybersecurity control standards, the CMMC will also measure the maturity of a company's institutionalization of cybersecurity practices and processes.

9 - How will CMMC be different from NIST SP 800-171?

Unlike NIST SP 800-171, CMMC will implement multiple levels of cybersecurity. In addition to assessing the maturity of a company's implementation of cybersecurity controls, the CMMC will also assess the company's maturity/institutionalization of cybersecurity practices and processes.

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845

10 - How will my organization become certified?

Your organization will coordinate directly with an accredited and independent third party commercial certification organization to request and schedule your CMMC assessment. Your company will specify the level of the certification requested based on your company's specific business requirements. Your company will be awarded certification at the appropriate CMMC level upon demonstrating the appropriate maturity in capabilities and organizational maturity to the satisfaction of the assessor and certifier.

11 - How much will CMMC certification cost? Will the cost be based on the level we requested or the size of the organization?

The certification cost has not yet been determined. The cost, and associated assessment, will likely scale with the level requested.

12 - Will there be a self-certification?

No.

13 - How do I request a certification assessment?

We expect that there will be a number of companies providing 3rd party CMMC assessment and certification.

14 - Who will perform the assessments?

An independent 3rd party assessment organization will normally perform the assessment. Some of the higher level assessments may be performed by organic DoD assessors within the Services, the Defense Contract Management Agency (DCMA) or the Defense Counterintelligence and Security Agency (DCSA).

15 - Are the results of my assessment public? Does the DoD see my results?

Your certification level will be made public, however details regarding specific findings will not be publically accessible. The DoD will see your certification level.

16 - How often does my organization need to be reassessed?

The duration of a certification is still under consideration.

17 - If my organization is certified CMMC and I am compromised, do I lose my certification?

You will not lose your certification. However, depending on the circumstances of the compromise and the direction of the government program manager, you may be required to be recertified.

18 - If my organization is certified CMMC and I am compromised will my organization require re-certification?

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845

A compromise will not automatically require a recertification. However, depending on the circumstances of the compromise and the direction of your government program manager, you may be required to be recertified.

19 - What if my organization cannot afford to be certified? Does that mean my organization can no longer work on DOD contracts?

The cost of certification will be considered an allowable, reimbursable cost and will not be prohibitive. For contracts that require CMMC you may be disqualified from participating if your organization is not certified.

20 - My organization does not handle Controlled Unclassified Information (CUI). Do I have to be certified anyway?

Yes. All companies conducting business with the DoD must be certified. The level of certification required will depend upon the amount of CUI a company handles or processes.

21 - I am a subcontractor on a DoD contract. Does my organization need to be certified?

Yes, all companies doing business with the Department of Defense will need to obtain CMMC.

22 - How will I know what CMMC level is required for a contract?

The government will determine the appropriate tier (i.e. not everything requires the highest level) for the contracts they administer. The required CMMC level will be contained in sections L & M of the Request for Proposals (RFP) making cybersecurity an "allowable cost" in DoD contracts.

23 - Will CMMC certifications and the associated third party assessments apply to a classified systems and / or classified environments within the Defense Industrial Base?

The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to protect controlled unclassified information (CUI) that resides on the Department's industry partners' unclassified networks. CMMC audits by third party assessment organizations will not be applied to classified systems or environments. The Defense Counterintelligence and Security Agency (DCSA) will include CMMC assessments as part of their holistic security rating score.

Edward J Kinberg
EJK@StewartLawCS.com
321-541-6845