Advanced Technology International (ATI)/Summit 7 Systems (S7S)

Cyber Security Maturity Model Certification (CMMC) Webinar – 20 Feb 20

Question and Answer Session

ATI is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this site is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information. The development of CMMC is ongoing and as such ATI recommends that prior to initiating activities related to CMMC compliance users seek advice directly from OSD POC or C3POA representative or other legal or professional advice on the subject matter.

1. **Is there a Request for Information (RFI) / Request for Proposal (RFP) for auditors?**

   Please refer to CMMC Accreditation Body website www.cmmcab.org.

2. **Is there guidance on the primes' supplier on compliance to NIST 800-171? Are they still required that they be 100% compliance?**

   Current DFARS regulations require compliance or POAM on steps and timeline to be completed.

3. **Why won't anything be dropping at L2?**

   Ms. Arrington spoke on this at a recent conference. She opined, “Level 2 is seen by the CMMC team as a transitional level or ‘maturing phase’.” She described it as a company “who is actively working towards Level 3, where most companies need to be.”

4. **In other maturity frameworks, the higher levels require process improvement processes and activities. I did not see any of this in Level 4 or 5. Will this be added later?**

   It is anticipated that the model will evolve so that could be added at a later date.

5. **I still do not understand how the June 2020 RFIs can have CMMC and later RFPs will have CMMC but the audits cannot start until late 4th quarter 2020?**

   RFIs will be select and simply mention expected level requirements. An actual certification will not be necessary to submit an RFI response. Similarly RFPs will be select and be for the Pathfinder program. Ms. Arrington spoke of a handholding scenario between those specific vendors selected for award on those contracts.

6. **When you say this year, do you mean a calendar year, or the government’s fiscal year which ends in September?**
   The presumption is OSD is referencing calendar year.

7. **Will this [CMMC] affect SBIR contracts?**

   To our knowledge, DOD has not identified contract types excluded from CMMC. There are specific SBIR contracts that have already called out CMMC as a requirement and offered funding in assistance to gain a CMMC certification.

8. **Is there a list of the 10 procurements that will contain the CMMC requirement?**

To our knowledge, this list has not been shared publically.

9. **Will the 10 test contract winner have to pass down to small sub-contractors?**

   Yes, the Pathfinder contracts will require flow down of the CMMC Requirements. It is not yet clear if all sub-contractors will need to be at the same CMMC level as the prime or if they will be able to be at a lower CMMC level based on the information they have access to.

10. **How will the pathfinder requirements flow down to suppliers? If so, is that included in the approximately 1,500 companies expected to meet CMMC.**

    Not completely known at this time, but assume that those prime contracts will have language placed in them to make this a requirement. Could be an upcoming DFARS 252.204.7012 change.

11. **What if you are a small company with no server at all and everyone works off of individual laptops?**

    If you are awarded a DOD contract, the “information system” handling CUI content will need to be secured to NIST 800-171, will need to meet DFARS 252.204-7012 and will be required to meet the applicable CMMC level if the contract has one specified.

12. **How is this going to play out in university/college type environments? We're relatively new to this space, and typically only participate in R&D contracts with DOD/DOE. Are we able to simply identify a “secure building” or a “secure room” within a given building, and all these CMMC requirements would only apply to the contract work that would have to be done “inside that room, and on these specific computers”?**

    Academia working with DOD CUI information will be expected to complete CMMC certification. You are able to specify a boundary around the enclave which needs to be certified, but there are broader University systems that may need to be compliant as well. I would suggest working with the University IT Security or Compliance Department to help make those determinations. Please refer to CMMC Accreditation Body website www.cmmcab.org.

13. **Where is a list of C3PAO audit companies?**

    There will be a CMMC Marketplace that identifies C3PAO organizations, among other vendors. That system is expected to be available in Q2CY20.

14. **From the previous slide, what does it mean; No medium assurance certificate/token?**

    As part of your requirements for DFARS 252.204-7012, you have the requirement to maintain a medium assurance certificate that will allow you to login to DibNet and make the appropriate notifications in case of a breach. There are companies that do not yet have that certificated and cannot effectively report to the government.

15. **How can I get the CUI data catalog that I can map for my upcoming contracts for data marking policy?**

    The CUI registry https://www.archives.gov/cui/registry/category-list

16. **Philosophical difference between strategies of zero trust and trusted domains. Is government addressing this?**

    This has not been addressed in CMMC.

17. **I did not understand the bullet stating 10 contracts and 1,500 companies. Does that mean they have identified 10 solicitations that are planned for release that they anticipate having up to 1,500 companies participate at subcontractors?**

    Yes, 10 initial prime contracts will be selected and those contracts are anticipated to have at least 150 subs each, which could impact up to approximately 1500 members of the Defense Industrial Base (DIB).

18. **How will DOD define CUI, particularly when it comes to technical data?**

    It is currently defined by the National Archives CUI registry.
    https://www.archives.gov/cui/registry/category-list

19. **How is it anticipated CMMC will apply to cloud service providers which DOD contractors use for SaaS services where covered data may be stored and processed?**

    CMMC does not specifically address Cloud Services. It treats On Premises environments the same as Cloud environments; however, DFARS 252.204-7012 requires that any cloud based service that is used to process CUI must be built to FedRAMP Moderate standards.

20. **CMMC is only for DFARS, not FAR, correct? How about HSAR (Homeland Security Acquisition Regulation)?**

    Per OSD FAQ, CMMC is currently only for DOD contracts.

21. **Who is being identified to be auditors? If our company wants to be a trained auditor, who do we contact?**

    Please refer to www.cmmcab.org.

22. **Will you be able to partition certifications if you have both commercial and gov't contracts? Meaning - if some locations in the US support defense but your international locations do not - will you be able to sub-certify operations?**

    It is expected that you will be able to define accreditation boundaries within your organization based on how those systems handle CUI data.

23. **For companies that pursue work geographically via a branch/division structure, will auditors be required to verify compliance at both the corporate headquarters and the specific division supporting the contract? Will there be a separate score for corporate vs. branches of a company?**

    If the organization as a whole uses a single Information System then the entire system will be audited as a single environment. It is not expected that different locations using the same information system will have different CMMC audits / certifications.

24. **We are currently licensed for Microsoft 365 through 3/21. Moving to GCC High to meet CMMC requirements would be extremely costly to implement at this time. Has Microsoft addressed this and provided any options for current customers?**

    Office 365 GCC High and Azure Government are the only Microsoft option for meeting both CMMC and DFARS 252.204-7012 requirements. Office 365 Commercial and Office 365 GCC will not meet the standards set forth by the government.

25. **Has it been defined how far down the supply chain a vendor needs to be certified? For example, we provide components two or three tiers down from the original Government contract.**

    The intent is to certify the entire supply chain.

26. **If there's a clearinghouse for auditors, will there be standardized rates?**

    The auditors will have standards to abide by as proposed by the CMMC Accreditation Body but auditors are independent and will set their own rates.

27. **Did I hear correctly that certification is required for DOD grants to universities? Are there any exemptions?**

    Yes, any contract with the DOD will require a certification. We don't anticipate any exemptions.

28. **If you outsource your IT, do you recommend an IT SME on company staff to implement CMMC?**

    It's good to have a dedicated (part or half time) POC or PM even for third party involvement.

29. **Are there specific differences in NIST requirements based on type of contracts your company will be bidding on? 800-171 versus 800-53 requirements, etc.**

    Each contract will specify the Cybersecurity requirements and we expect all DOD contracts will be moving to CMMC during solicitation.

30. **So it would be reasonable to shoot for CMMC 3 compliance by the end of the year?**

    If you are currently working on DOD projects involving CUI, then it is advisable to have an external entity perform a gap analysis and subsequent certification as soon as feasible for your organization.

31. **Any suggestions for the mobile platforms like cell phone emails, texting etc.?**

    We typically implement Office 365 GCC High which includes Intune for Mobile Device Management and Mobile Application Management. It will meet all of the CMMC requirements for mobile devices. However, texting CUI is not a compliant solution and should not be used.

32. **Does a Level 3 Prime have to have Level 3 on all of their supply chain?**

    It is expected that a prime certified at level 3 may have subcontractors at different levels depending on the contract and the level of information processed by the contractors. This has not been 100% verified by OSD yet, but we are expecting that this will be the case.

33. **Are there guidelines instructing contracting officers how to assign CMMC levels to their solicitations? Is there a specific DLA guideline?**

DOD acquisition officers are undergoing training from DAU so the intent is that they will have the necessary skills to make those determinations.

34. **With Microsoft - Office 365 Multi-Tenant & Supporting Services being on the approved list in FedRAMP, do we need to start to move from there to the GCC?**

    Office 365 GCC High and Azure Government are the only Microsoft cloud options for meeting both CMMC and DFARS 252.204-7012 requirements. Office 365 Commercial and Office 365 GCC will not meet the standards set forth by the government.

35. **Is there any standards for Internet of Things (IOT), smartwatch, refrigerator, etc.?**

    No specific standard for IOT devices. If an IOT device is used in performance of a contract with the DFARS clause, then devices will have to adhere to the same controls.

36. **If company (single business entity) has both commercial and DoD contracts, performed by different divisions. Can pure commercial divisions be excluded from CMMC?**

    Yes, you can define the boundary around the systems to be certified, just do not co-mingle systems and data from the both sides of the operation.

37. **For the blacklisting/white listing applications control mean you have to use a product like bit9 or, if people don't have local admin rights to install, will that fly?**

    We believe you will have to have an application that performs the function such as Bit9, AppLocker, etc.

38. **Are there anymore upcoming CMMC in-person events or webinars?**

    We anticipate offering additional training webinars and in-person training at consortia events.

39. **Do you expect other agencies such as DHS, DOE, and Treasury to incorporate this?**

    ATI can't confirm if other agencies will follow DoD CMMC requirements but DOD has mentioned they are speaking with other agencies and foreign countries about the possibility for the scope of CMMC to expand.

40. **Will CMMC certification be required if there is no CDI (Covered Defense Information)/CUI involved (which exempts many universities from the 7012 burden)?**

    That will be determined by the new contract language, but we would expect at a minimum that CMMC level 1 certification will be required.

41. **Will "DoD grants" be subject to the same CMMC requirements as "DoD contracts"?**

    While not fully defined, it is expected that DOD grants will be subjected to the same CMMC requirements as other contracts.

42. **Separation of duties for a small company is always a challenge. How do you recommend complying with this?**

Yes, this is somewhat difficult. You can have multiple accounts with different rights and switch between them so that you don’t have any single account that can do everything within the environment. Pay attention to logical control as well as technical control here. Another option is to work with a 3rd Party outsourced provider to assist you with management of the environment.