**Questions**

**Q: Who pays for the 3rd party audit?**

*Each organization will be responsible for covering the cost of their CMMC certification audits. However according to Office of the Under Secretary of Defense for Acquisition & Sustainment the following has been answered so far:*

*“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.”*

**Q: If i request Certification at Level 3, but only achieve Level 2, will my company fail or will we be awarded Level 2?**

*The only information we have at this time on this subject is the following:*

*“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.”*

*Since the levels are cumulative we feel it is safe to assume if you do not meet, for example the criteria of level 3 but do in fact meet criteria for level 2 you would be awarded a certification at that level.*

**Q: Question. I am hearing that unlike DFARS 252.204-7012 , CMMC may be applicable to COTS items, is there any validity to that early assertion? We have a commercial aspect and a pure federal effort and we are trying to understand if we will see RFPs and other procurement request to our commercial side from Agencies now expecting CMMC to solicit an offering for COTS items. Any thoughts?**

*At this time the DoD has not officially announced if any of the CMMC levels will in fact apply to COTS items. While there has been some discussions around this subject all we can say is as more information becomes available we can pass that information along.*

**Q: Who will be performing the audits? The USG, approved industry, certified companies?**

*As of this time the DoD has only stated “The intent is for certified independent 3rd party organizations to conduct audits and inform risk.” That being said as of October 3, 2019 they have posted on the site* [*https://acq.osd.mil/cmmc/index.htm l*](https://acq.osd.mil/cmmc/index.html) *the following in regards for companies wishing to become certified auditors and obtaining more information:*

CMMC Accreditation Body Request For Information (RFI)

* Posted on October 3, 2019 at [**Click Here**](https://www.fbo.gov/index?s=opportunity&mode=form&id=4a4b539a0e347e540b30b3121916031c&tab=core&_cview=0)
* Solicitation Number: HQ0034SS10032019
* Responses Due: October 21, 2019, 6:00 pm Eastern

**Q: What is Chads contact number to discuss the services being offered.?**

*You can contact Steve Palamara (**stephen.palamara@e-tcc.com* *or 317-698-4242) Director of Business Development with TCC to setup a discovery call to review the program and answer any of your questions.*

**Q: Great presentation, is this webinar being recorded? If so, how can I get a copy of it to review it later on?**

*Yes, a recording of the Webinar is available on the NSTXL Website and will be distributed to all Webinar registrants. Here’s the link to the recording* [*https://www.youtube.com/watch?v=tgKEjJifEOk&t=5s*](https://www.youtube.com/watch?v=tgKEjJifEOk&t=5s)

**Q: What are the security requirements for cloud based computing?**

*As per DFARS 252.204-7012 requirements for cloud based services that protect, store, or transmit CUI/CDI, any such services utilized by contractors will need to follow the DoD Cloud Computing Security Requirements Guide (SRG). This guide states these services security controls must be equivalent to the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline. Also contractors must ensure when using such services the Cloud Service Provider (CSP) complies with requirements in DFARS 252.204-7012 for cybersecurity incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.*

*We do not at this time anticipate these requirements to change.*

**Q: Will this new Cyber Security requirement/flowdown replace RMF and FEDRamp, or will this be in addition to those requirements?**

*See above regarding any FedRAMP requirements as for replacing existing frameworks or guidelines, the Dod has released the following statement:*

*“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.”*

*Since many of these standards incorporate the key principles of the Risk Management Framework into their design, the CMMC will continue to incorporate these key principles and others to better provide security and awareness going forward. The 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.*

**Q: Do any certifications come into play for NIST or CMMC for IT department? does it affect the model, rating, or maturity level?**

*At this time we are not aware of any certification requirements for IT department personnel. However, based on the requirements provided in the Awareness and Training Domain which leverage the current NIST SP 800-171 and NIST SP 800-53 and other sources, some contractors may choose to impose certain certification requirements as part of an ongoing security awareness training program ensuring administrators and security operations staff maintain up to date relevant industry information*.

**Q: How do you deal with the challenge of having the Prime tellink you what exactly is classifed as CUI data? They normally tell you all the data is?**

*We recommend all contractors review the CUI marking program to ensure data is properly identified. Some guidance can be found at:*

[*https://fas.org/sgp/cui/marking-2016.pdf*](https://fas.org/sgp/cui/marking-2016.pdf)

*Also due to the numerous amounts of regulations, laws, and U.S. Code that govern how each of the CUI Specified information types must be controlled, the best advice is to search for those requirements on the CUI Registry at:*

[*https://www.archives.gov/cui/registry/category-list*](https://www.archives.gov/cui/registry/category-list)

*Due to the fact that CUI is such a broad umbrella that encompasses so many different categories and sub-categories, the CUI Registry will help contractors better understand what qualifies as CUI and how it should be marked especially if the contractor is the originator of the CUI as part of work being performed on a contract.*

*Resources, including online training to better understand CUI can be found on National Archives’ website at:*

[*https://www.archives.gov/cui/training.html*](https://www.archives.gov/cui/training.html)

**Q: What have you heard about companies being able to charge the government for compliance? Direct charges / Indirect charges, for example.**

*At this time the only information they have given is the following:*

*“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.”*

*Katie Arrington, the special assistant to the Assistant Secretary of Defense for Acquisition for Cyber in the Office of the Under Secretary of Acquisition and Sustainment in DoD, made this statement to a roomful of vendors,*

*““I need you all now to get out your pens and you better write this down and tell your teams: Hear it from Katie Arrington, who got permission to say it from Mr. [Kevin] Fahey [the assistant secretary of Defense for Acquisition in the Office of the Under Secretary of Acquisition and Sustainment] security is an allowable cost. Amen, right?”*

**Q: What is the cost for the evaluation and subsequent compliance plan?**

*According to the DoD:*

*The certification cost has not yet been determined. The cost, and associated assessment, will likely scale with the level requested. Additionally, the duration of a certification is still under consideration.*

**Q: Do these services comply with 3rd party audits from the government?**

*At TCC we feel our services set us apart from ordinary MSP/Security companies in that we have several years of experience in the design, implementation, and supporting of highly compliant environments. Our experience working with NIST SP 800-53, IRS Pub-1075, and FedRAMP environments, we feel provide us a solid foundational framework to help companies with the requirements of the current DFARS 252.204-7012 clause as well as the eventual evolution into the CMMC program compliance.*

**Q: Are you aware whether DoD will allow an organization to have more than 1 certification level, based on different environments/locations ?**

*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.*

**Q: If you aren't approved, you can't bid!!!**

*The CMMC stipulation requirement is expected in “all” DoD solicitations beginning October 2020.*

**Q: You must certify in your bid that your in compliance with the certification.**

*Our understanding at this time is there will be a CMMC requirement for Prime Contractors and “all” Subcontractors used on a solicitation response.*

**Q: What is the feedback you are hearing from DoD people like Crane about what they are expecting from their current contractors?**

*Crane and other DoD agencies are onboard with the new CMMC requirements and the current NIST 800-171 regulations. All are interested in seeing a heightened level of security in the supply chain.*

**Q: Do you have preferred hardware vendors for IT infrastructure and software for compliance, to close the gaps.**

*Through our remediation program/services TCC can suggest several options for vendors of hardware and software to achieve compliance. Our goals are to provide guidance and direction for securing and/or building environments to meet the necessary security requirements while remaining vendor agnostic in most cases and always taking a company’s budget into consideration.*

**Q: Are contractors required to input control validation into a specific format or is there a recommended system like eMASS, etc.?**

*At the current time we are not aware of any standard formats being required for input control validation such as system solutions like Enterprise Mission Assurance Support Service (eMASS) as part of the CMMC program.*