CMMC Questions for the NDIA Luncheon

General

1. **Will small businesses doing Advisory and Assistance services on local Air Force, Space Force, and MDA contracts that have highly technical or sensitive FOUO data have to have a CMMC certification level higher than level 3?**

2. **Can subcontractors use the CMMC certification from the Prime? If so, what technical efforts are involved?**

3. **As a small business can I, with limited IT knowledge, set up and maintain my home business network to meet CMMC Level 3 standards? My research suggest NO since there are data center configurations done by Microsoft, but I may not have the whole story.**

4. **Will I be able to run one standalone computer on my network with FOUO/ CUI (e.g., Government Furnished data) for CMMC level 3 and keep all my corporate data (accounting, personnel, BD, etc.) on a separate computer using the same network/ISP?**

5. **I am getting calls and emails from companies who say they are CMMC-Certified, or saying they have CMMC-Certified tools, and can help my company get CMMC-Certified as well. Is there a list of CMMC-Certified companies? If so, where is it so we can verify?**

6. **With many references in the CMMC Guidance to practices associated with owning our own hardware, how do companies who have cloud services ensure CMMC Certification?**

7. **Who is helping small companies with this program?**

8. **What do companies need to do before they are audited?**

Cost and Auditing

1. **Will the cost of CMMC implementation and certification be reimbursed by the government and if so, will it be fully reimbursable as another direct cost or will small businesses be required to allocate the cost as overhead? Also, if reimbursable, how will startups and companies not currently on contract with the government get reimbursed?**

2. **I have heard that the companies that will do the CMMC auditing are not on contract, but the government plans to award some auditing contracts this year and start certifying a few select contractors in phases. Since I also heard that RFI's and RFP's starting in FY 20 (this October) will have CMMC requirements, how will the government make sure those businesses that have not yet been certified are not denied an opportunity to bid on contracts in FY20 and beyond that have CMMC level mandates in them but are waiting on an auditor?**

3. **I see CMMC advertisements from Google and Windows on a cloud based network. How much will outsourcing CMMC cost my company?**

4. **How do you see the Government making FEDRamp, Government Cloud Computing (GCC), and GCC-High available to companies? Will it be reimbursed or free service?**

5. **How often do I have to be recertified and what will that cost be?**

6. **As the CMMC requirements change, do we know how currently certified companies will have their certification "re-" certified? Will those companies need to pay a C3PAO again?**

7. **What is the expected cost to small businesses to implement and maintain CMMC for a company with ten or less employees and for larger small businesses under 50 employees as a point of comparison (e.g., for the email, security, cloud storage, etc.)?**

8. **How much will an independent assessment that certifies CMMC level three standards cost? Also, how much will levels 4 and 5 be if my prime flows those levels down to me?**

Input to the government

1. **What is the Government's willingness to continue to receive feedback on the financial impacts of CMMC compliance to very small businesses, for example the niche providers in the supply chain?**

2. **What can we do as companies to remain involved in the CMMC decision-making when we are busy doing our jobs?**

3. **Are our political leaders part of this process and if not how do they provide input?**

Auditor Questions

1. **Why can companies only be on the blue team or red team – i.e., auditors only?**

2. **Getting on O365 GCC and other Govt clouds for compliance seems almost impossible unless you are a prime and for indirect subcontractors its definitely impossible due to the governments unwillingness to sign the required letters. How do we get around this or get help getting the letters?**

3. **MSP and MSSP (indirect subcontractor) compliance – must they be compliant? And what are their tools?**

4. **Why have separate Level 1-3 and 4-5 tiers for assessors?**

5. **Security clearances – why are they necessary if they are working on unclassified systems?**

6. **Will CMMC Assessors be required to obtain security clearances, or will this only be a requirement for CMMC Auditors? Will this be CMMC Level-specific?**

7. **Will C3PAO's have to be CMMC certified? If so, at what level? Are they first for auditing?**

8. **Can companies or people get pre-approved to be auditors? What are the criteria?**

9. **Will there be a conflict of interest on CMMC Auditors if they also work for C3PAO's and offer Assessment Services ? In other words, can an assessment be completed by a C3PAO organization that also provides remediation and IT security services, (to help a company become CMMC Compliant) just as long as the same C3PAO does not conduct the CMMC Audit for the same company ?**

10. **We have been told a CMMC Auditor for an organization cannot be the CMMC Assessment or remediation agent for a company. I know this is under review at this point by the Accreditation Body, but because of the limited number of assessors and auditors wouldn't it be wise to be able to "double-up" the human resources available in the short term?**

11. What is the schedule for auditing?

12. Is the current CMMC Target Dates and Milestones that have been forecasted realistic ? (See below)

a. **January 2020: The official CMMC Levels and requirements will be released along with training materials for the independent CMMC Accreditation Board (CMMC AB) to use for training auditors and C3PAO's.**

b. **February-May 2020: The initial round of assessors will be trained**

c. **June-September 2020: Initial round of audits will begin for a select number of DoD Programs/RFI's with the required CMMC Levels identified and contractors wishing to bid on those Programs will need to be certified to the required Level in order to receive the RFP.**

d. **October 2020 and beyond: DoD contractors will need to get certified by an accredited Assessor/C3PAO in order to bid on new work**