

## Webinar 4 Q&As

### Q&As for Paul Shaw, DAU

As an experienced Acquisition Professional - my suggestion if in doubt - communicate with the Contracting Officer. DoD Contracting Officers are a very professional group with a wide variety of experience in handling issues - when the channels of communication are open.

Q. If a company has a contract for mowing grass or cleaning porta-pots on DoD site, do they need to be CMMC Level 1 certified?

Under the current DFARS Clause 252.204-7012, such contractors were not included. The standard under the existing DFARS Clause 252.204-7012 is the possession of Controlled Unclassified Information (CUI). Under the current DFARS Clause 252.204-7012, there was an extremely high probability that a contractor mowing grass or cleaning porta-pots was exempt from DFARS Clause 252.204-7012 due to the services they provided, but because they most likely do not have Controlled Unclassified Information (CUI). Note under the current DFARS Clause 252.204-7012 - the test for compliance was not the service provided, but the presence of Controlled Unclassified Information (CUI).

CMMC has created a second category of information that requires a level of protection -- Federal Contract Information (FCI). There have been earlier public comments that all DoD Contractors would require some level of CMMC certification. But there are refinements to those statements. On the CMMC website, under the frequently asked question (FAQ) of "My organization does not handle Controlled Unclassified Information (CUI). Do I need to be certified anyway?" The answer was refined to say "Companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification." The point being there are contractors that could meet an existing exception to CMMC certification. Another response under the same FAQ was "If a DIB company does not possess CUI but possesses Federal Contract Information (FCI), it is required to meet FAR Clause 52.204-21 and must be certified at a minimum of CMMC Level 1."

So the question for a contractor providing either a grass mowing or porta-potty cleaning service - do they have Federal Contract Information (FCI)? If they have Federal Contract Information (FCI), there is a possibility they will need to be at least CMMC Level 1 Certified. Remember FY20 NDAA Section 1648 calls for "Tailoring cybersecurity requirements for small- and medium-sized contractors based on a risk-based approach."

I expect there will be an ongoing development of the framework for managing risk for loss of data confidentiality - as CMMC matures. As an example, I could see even a grass mowing or a porta-potty cleaning service at a DoD ballistic missile site - having potentially sensitive Federal Contract Information (FCI) and being at least CMMC Level 1 Certified. Remember the intent is less about the service provided and more about the risk to the DoD for the loss of data confidentiality for either Controlled Unclassified Information (CUI) or Federal Contract Information (FCI).

Q. CMMC will be required for OEA grantees?

A. OEA is under the same requirements as all DoD organizations. The current standard as discussed in the above response for DFARS Clause 252.204-7012 is the presence of Controlled Unclassified Information (CUI). The standard under CMMC still has the presence of Controlled Unclassified

Information (CUI) and further includes the presence of Federal Contract Information (FCI). If the OEA grantee does not have either Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI) or meets another CMMC exemption (such as solely produce Commercial-Off-The-Shelf (COTS)) - then they might not require CMMC certification. I expect DoD contracting requests to develop explicit language as the CMMC framework matures -- for when it applies and when it does not. The key will be for effective communication between the government and contractors to achieve a tailorable, risk-based approach as called for in FY20 NDAA Section 1648 -- "Tailoring cybersecurity requirements for small- and medium-sized contractors based on a risk-based approach." The objective for acquisition is to create a fair and open competitive process that does not create unnecessary barriers for new entrants as DoD suppliers and ensures new DoD suppliers understand expected qualifications.

Q. Could Paul talk about the requirement that potential contractors will not even be able to submit bids on RFPs that contain CUI without the appropriate DFARS (and eventually) CMMC compliance?

A. There are organizations in the DoD today that specify compliance with DFARS Clause 252.204-7012 - as a condition of being a qualified applicant. As an example, Defense Advanced Research Projects Agency (DARPA) puts out information on various FAR and DFAR clauses that could apply to a potential bid. See: <https://www.darpa.mil/work-with-us/procurementcontracts>

"Potential FAR-Based Procurement Contract Clauses and Provisions"

This opportunity has the potential to result in one or more of several different award instruments, including FAR-based procurement contracts, grants, cooperative agreements, or Other Transactions.

Below is a list of clauses and provisions that may apply if this opportunity results in one or more FAR-based procurement contracts, depending on the circumstances and rules for applicability. This list is not exhaustive, and the clauses and provisions that may apply will depend on the nature of the award, the award type, the award recipient, security or publication restrictions, and other factors. This list serves to put potential proposers and awardees on notice of potential requirements (including clauses and provisions) which may apply should they be selected for negotiation for potential award."

Under the current DFARS Clause 252.204-7012, the requesting DoD agency usually allows a contractor a period of time to become compliant. If doubt exists, the potential contractor should submit a question to the DoD contracting agency for clarification.

As the CMMC framework matures and the DoD Acquisition Workforce experience with the CMMC in contract language matures, there is a possibility that CMMC certification compliance could be a condition for bidding. On the CMMC website, under the frequently asked question (FAQ) of "How will I know what CMMC certification is required on a Contract?" The answer to the questions says, "The DoD will specify the required CMMC level in Requests for Information (RFIs) and Requests for Proposals (RFPs)." If a CMMC certification level is specified in a Request for Information (RFI) or a Request for Proposal (RFP), the logic is that a potential contractor is not qualified candidate without the specified appropriate CMMC certification. The issue is to balance the need for the contractor to provide a level of security to sensitive DoD data, either Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI), at the beginning of contract performance, without creating an unnecessary barrier to potential new DoD suppliers of services and goods.

## Q&A for Ashlee Breitner

Q. You mentioned linking companies up with state-level resources. Which ones specifically do you flag? What state resources (from Michigan) are available for UM's program?

A. In looking at the questions posed there are different resources at a state level that we utilize depending on the area of our grant focus. For cybersecurity initiatives, we collaborate with the Michigan Economic Development Corporation (MEDC) and Michigan Manufacturing Technology Center (MMTC is the MEP for Michigan) as well as the PTAC's. In relation to our workforce focus groups, we also collaborate with MEDC as well as the Department of Labor to connect companies with the correct resources.

## Q&A for Eileen Sanchez, California Governor's Office of Policy and Research

Q. How many companies have you helped?

A. Quantified impacts across 15 projects in CASCADE I included providing substantive assistance for nearly 4000 defense workers and over 1000 defense firms, touching over 80% of the 30,000 defense suppliers in the state via outreach and educational activities, and impacting over 250 communities.