pm

THE LINK

Connecting Suppliers with DLA

Issue 18
October 2020

2020 TKO Mark Your Calendars!

TKO Seminars are FREE!

Learn how to do business with the Government

Virtual: November 3

Register at: https://tko.dla.mil/

All seminars are held in Columbus, OH
8:00 AM - 4:30 PM E.S.T

www.dla.mil

www.facebook.com/dla.mil

www.twitter.com/dlamil

www.youtube.com/user/dodlogisticsagency

TRACEABILITY COMPLIANCE REVIEW PROGRAM

DLA Land and Maritime recently launched a Traceability Compliance Review Program to assess contractor compliance with FAR 52.246-2, Inspection of Supplies, and DLAD Procurement Note C03, Contractor Retention of Supply Chain Traceability.

FAR 52.246-2 and DLAD Procurement Note C03 are included in all solicitations and awards issued by DLA and are critical to ensuring the integrity of the material supplied to DLA's military customers. FAR 52.246-2 requires a contractor to provide and maintain a documented inspection system. Records evidencing all inspections made under the system are to be "kept complete and made available to the Government during contract performance and for as long afterwards as the contract requires." Similarly, DLAD Procurement Note C03 requires a contractor to obtain and retain, for a period of five years after final payment under the contract, documented evidence that the item of supply is from an approved manufacturing source and conforms to the technical requirements of the contract, otherwise known as "supply chain traceability documentation." The contractor is required to immediately make such documentation available upon request of the contracting officer.

Contractors selected for compliance review will be asked to provide supply chain traceability for a specified number of recently completed purchase orders requiring the supply of the designated part number of an approved manufacturing source. If a contractor fails to respond to the request or if the documentation is determined to be inadequate, the contractor may be subject to contractual or administrative remedies, including, but not limited to, demand for payment under FAR 32.604 or administrative debarment under FAR 9.406-2.

ATTENTION SUPPLIERS WHO USE SUBCONTRACTORS

As the prime contractor, you are responsible for ensuring the delivery of material that conforms to DLA contract requirements and that you inspect material for contract compliance. Accordingly, DLA encourages you to exercise due diligence in your selection of subcontractors under all government contracts. We recommend that you not allow a supplier to direct ship until you have vetted that supplier and the supplier's quality systems, and that your quality system is able to ensure delivery of conforming material. Vetting of your suppliers would include reviews of the subcontractor's business history, public corporate records, location based data, and other information that could verify its manufacturing capabilities. Additional steps such as undertaking a manufacturing and testing capability assessment would provide further assurance that your subcontractors are legitimate sources.

WAWF URL CHANGE

As part of the planned PIEE migration from DISA hosting to the Amazon Web Services (AWS) cloud-hosting environment, the PIEE/WAWF URL updated from https://wawf.eb.mil to https://piee.eb.mil effective July 1, 2020. The old URL is supposed to automatically redirect users. In the event this does not occur, users should access the new URL directly.

CHANGE IN MATERIAL REQUIREMENTS FIELD ON QUOTE

A recent release changed how the DIBBS web quote form and batch quote treat "Material Requirements." The quote form for this field previously defaulted the radio button to "No" when the question "Used, Reconditioned, Remanufactured, or New/Unused Government Surplus?" was asked, under the "Material Requirements" header. This question no longer has a default and now requires a conscious affirmative action by selecting "Yes" or "No." If selecting "Yes," then the drop down still applies for what type of other than new/unused material is being supplied. For those who utilize batch quoting, the BQ download file no longer defaults field 67 to "0" and now requires the field to be populated when uploading a quote. If not populated, an error will be received. Questions can be directed to the DIBBS Helpdesk at DibbsBSM@dla.mil

SMALL BUSINESS WEBINAR SCHEDULE

Need more information on how to do business with the Government? The Small Business Office holds webinars on various topics at no charge to you!

Register here: https://tko.dla.mil/Public/Main.aspx

Doing Business with the Government (TKO) Virtual:	November 3rd, 8—4:30 pm EST
Sources Sought:	November 10th, 3—4 pm EST
Technical Data Packages (Bid sets and cFolders):	November 17th, 2—3 pm EST
Doing Business with DLA (overview):	December 15th, 2—3 pm EST

PROHIBITION ON CONTRACTING WITH ENTITIES USING CERTAIN TELECOM AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

Implementation of the Section 889(a)(1)(B) Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment

FAR rule 2019-009, published on July 14, 2020, was effective on August 13, 2020 and implements prohibitions contained in section 889(a)(1)(B) of the National Defense Authorization Act (NDAA) for Fiscal Year 2019.

Section 889 of the NDAA for FY 2019 contains two prohibitions related to Federal contracting:

The first prohibition, set forth in section 889(a)(1)(A), took effect August 13, 2019, and prohibits the Government from buying and using covered telecommunications equipment or services from five named Chinese companies and their subsidiaries or affiliates.

The second prohibition, set forth in section 889(a)(1)(B), was effective August 13, 2020, and prohibits the Government from contracting with any entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, on or after August 13, 2020, unless an exception applies or a waiver has been granted.

The interim rule requires offerors, after conducting a reasonable inquiry, to provide a representation regarding use of covered telecommunications equipment or services when submitting an offer. Further, contracts, task orders, and delivery orders must contain a clause that requires reporting if use of covered telecommunications equipment or services is discovered during performance of the contract. The interim rule applies to acquisitions of commercial items, including COTS items, and to purchases at or below the simplified acquisition threshold.

These implementation procedures apply to contracts, task orders, and delivery orders, including orders against basic ordering agreements (BOAs), and calls against blanket purchase agreements (BPAs). These implementation procedures also apply to BPAs and BOAs to facilitate the inclusion of these terms in BPA calls and BOA orders, which is required.

For DLA's Automated Simplified Acquisitions, the DLA Master Solicitation will be updated on Page 1 to include amended language in Section 2 (b). In addition, effective dates will be revised for clauses 52.204-24 (AUG 2020) and 52.204-25 (AUG 2020).

For other contract ordering vehicles such Indefinite Delivery Indefinite Quantity contracts (IDIQs), Basic Order Agreements (BOAs), and Blanket Purchase Agreements (BPAs), DLA contracting activities are in the process of issuing modifications to insert section 889 requirements.

New contract actions issued after August 13, 2020 will contain the appropriate clauses to implement section 889 requirements. In the event contractor compliance is not possible, follow the reporting requirements in Section (d) of Clause 52.204-25 and discuss with your contract administrator/contracting officer.

Additional information is available at https://www.acquisition.gov/FAR-Case-2019-009/889_Part_B .

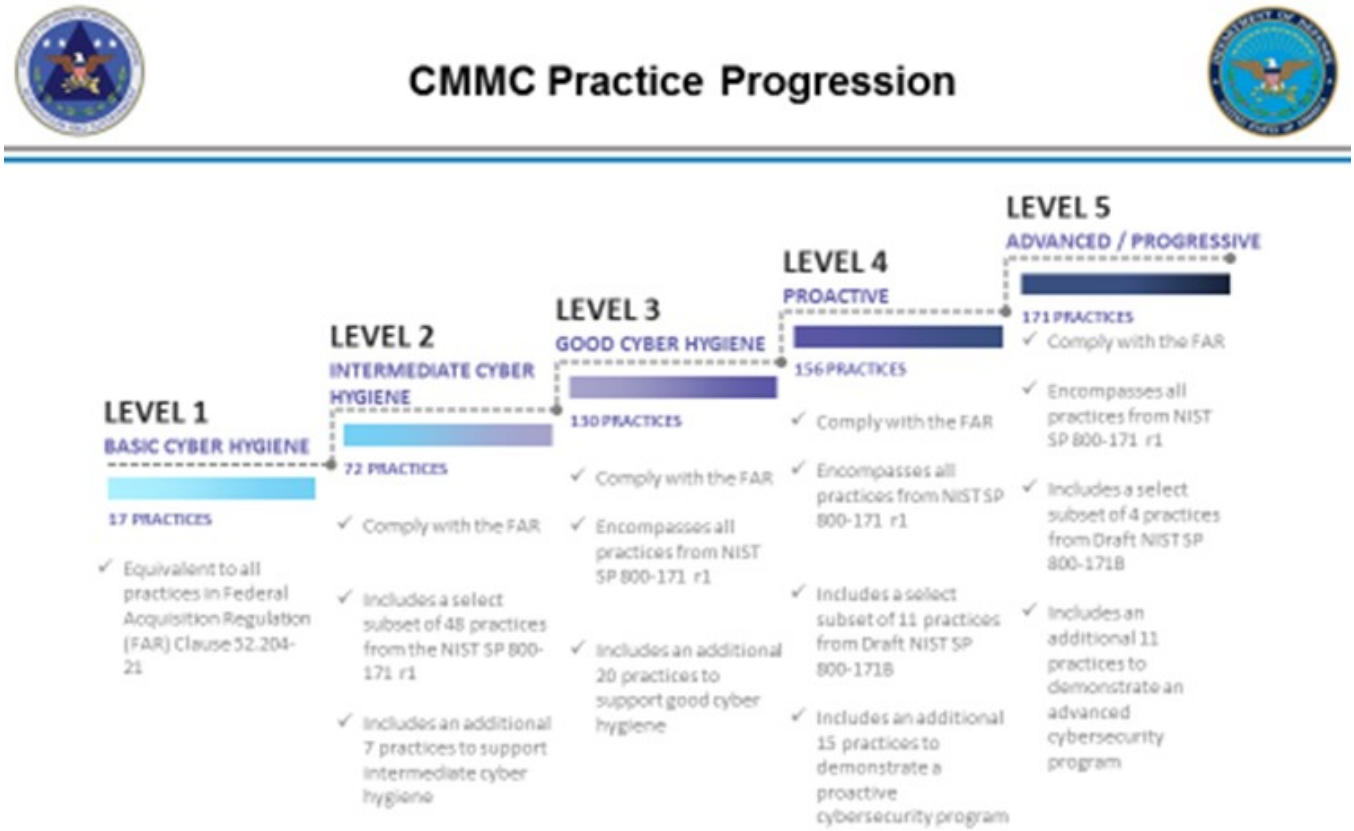
DOD'S NEW CYBERSECURITY REQUIREMENT (CMMC)

What is CMMC?

The DoD is currently working to enhance the protection of controlled unclassified information (CUI) within the supply chain. OUSD (A&S) has been working with DoD stakeholders and industry to develop the **Cybersecurity Maturity Model Certification** (CMMC). The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements. The CMMC will review and combine various cybersecurity standards and best practices. CMMC charts these controls and processes across several maturity levels that range from basic to advanced cyber hygiene. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats. The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels. Certified independent third party organizations will conduct audits and inform business of uncovered risk.

When will CMMC be required?

DoD originally planned to release requirements for CMMC in October of 2020, however, the current pandemic has caused delays in the official release. No estimated date has been set for release of official DFARS requirement. The initial CMMC pilot program is scheduled to occur from October 2020 to March of 2021. DoD is currently working two test phase CMMC programs (Pathfinder and Pilot), which will help evaluate how DoD will assess CMMC levels to align with requirements. The plan is to conduct CMMC pilot programs with new solicitations/contracts issued this year and previously awarded contracts via the Pathfinder program.



DISTRIBUTION A. Approved for public release

DOD'S NEW CYBERSECURITY REQUIREMENT (CMMC) CONT.

How should a DoD contractor prepare for the CMMC requirement?
While CMMC is not yet officially operative, its outline and objectives are well known. Contractors may consider the following appropriate actions to prepare for CMMC:

- Determine if your company receives federal funds from the DoD either directly as a prime contractor or indirectly via subcontracts, purchase orders, or other contractual agreements. If so, you should be prepared to obtain at least a Level 1 certification.
- Determine whether your company currently or in the future expects to electronically process, store, or transmit controlled unclassified information (CUI) in the performance of its defense contracts. If so, you should be prepared to obtain at least a Level 3 certification.
- Review your company's current compliance with NIST SP 800-171 Rev 1 in relationship to your expected CMMC level requirements.
- If you haven't already, begin drafting a system security plan (SSP) in accordance with NIST SP 800-18 Rev 1.
- If you currently have a plan of action and milestones (POAM) in place or identify additional concerns, dedicate appropriate resources to ensure progress is being made to close any gaps as quickly as possible. Examine Draft NIST SP 800-171B for enhanced security requirements to improve cybersecurity maturity capabilities as applicable given the CMMC level you intend to attain.
- Investigate your subcontractor base as CMMC requirements will likely flow down to subcontractors, including commercial item subcontractors. It is expected that consent to subcontract at the order level may also consider subcontractor CMMC level.
- When the opportunity arises, participate in CMMC workshops/webinars recommended or hosted by DoD.

Contractor Resources

"The Cybersecurity Maturity Model Certification - Overview and Latest Developments"
https://www.dau.edu/SiteAssets/DAU-Webcasts/index.html
Cyber Collaboration Center
https://www.cybercollaborationcenter.org
CMMC Accreditation Body
https://www.cmmcab.org/cmmc-standard
CMMC program office FAQs
https://www.acq.osd.mil/cmmc/faq.html
NIST (National Institute of Standards and Technology) publications
https://csrc.nist.gov/publications/detail/sp/800-171a/final