

THE LINK

Connecting Suppliers with DLA



Issue 32
April 2024

2024 TKO Mark Your Calendars!

TKO SEMINARS ARE FREE!

Learn how to do
business with the
Government!



HELD VIRTUALLY

9:00 AM - 2:30 PM (EST)

May 7-8, 2024

June 11-12, 2024

July 9-10, 2024

September 10-11, 2024

November 5-6, 2024

Register at:

[Outreach Calendar \(dla.mil\)](https://www.dla.mil/outreach/calendar)

Find other Training
Opportunities here:

[DLA SMALL BUSINESS TRAINING](https://www.dla.mil/small-business-training)

[WWW.DLA.MIL](https://www.dla.mil)

[WWW.FACEBOOK.COM/DLA.MIL](https://www.facebook.com/dla.mil)

[WWW.TWITTER.COM/DLAMIL](https://www.twitter.com/dlamil)

[WWW.YOUTUBE.COM/USER/](https://www.youtube.com/user/dodlogisticsagency)

[DODLOGISTICSAGENCY](https://www.dla.mil/dodlogisticsagency)

REMINDER TO DLA OFFERORS

UPDATE NIST SP 800-171

ASSESSMENT IN SPRS TO REMAIN ELIGIBLE FOR CONTRACTS

In accordance with DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements and DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, DLA offerors must have a valid National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 assessment and score on file in SPRS to be considered eligible for contract award. Assessments are valid for a period of three years. It is the offeror's responsibility to update their assessment prior to expiration to remain eligible for awards subject to controlled unclassified information (CUI) and/or covered defense information (CDI) safeguarding requirements.

For more information regarding posting or updating an assessment on SPRS, please go to: <https://www.sprs.csd.disa.mil/>

Protecting Controlled Unclassified
Information in Nonfederal Systems
and Organizations

NIST 800-171

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



The Cybersecurity Maturity Model Certification (CMMC) program is aligned to the Department of Defense (DoD) information security requirements for its Defense Industrial Base (DIB) partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program provides the DoD increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI).

The changes reflected in CMMC 2.0 will be implemented through the rulemaking process. Companies will be required to comply once the forthcoming rules go into effect. DoD intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Both rules will have a public comment period.

On December 26, 2023, DoD published for comment the proposed Part 32 rule for the Cybersecurity Maturity Model Certification (CMMC) 2.0 program at <https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>. Stakeholder input is critical to meeting the objectives of the CMMC program. The public comment period for the Part 32 rule in the CFR closes on February 26, 2024. The Part 48 CMMC DFARS rule is currently undergoing the rule making process.

DoD encourages contractors to continue to enhance their cybersecurity posture during the interim period while the rulemaking is underway. DoD has developed Project Spectrum (<https://www.projectspectrum.io/>) to help DIB companies assess their cyber readiness and begin adopting sound cybersecurity practices.

Additional information on the CMMC program can be found on the DoD Chief Information Officer (CIO) website: <https://dodcio.defense.gov/CMMC/About/>

HAVING SECURITY CERTIFICATE ISSUES ON DLA APPLICATIONS?

While most computers automatically recognize public Certification Authorities (CAs) that are trusted to validate the identity of the secure (HTTPS) websites, many .MIL sites are verified through private DoD CAs whose certificates require manual installation by a local system administrator. IT departments within the DoD typically install and update these certificates for their employees automatically, but there are occasions that updates do not reach all user workstations and a manual installation becomes necessary. Non-DoD agencies, private sector organizations, and home users do not typically have DoD CA certificates installed on their computers and will more than likely be required to complete the steps on the [Defense Acquisition University \(DAU\) guide](#) in order to access many DLA resources.

CHANGES TO DIBBS BATCH QUOTING FEB 2024 - MOVED TO APRIL 2024

The following changes of the quote form and batch quote/EDI will be incorporated with the next release of DIBBS changes. It is anticipated this will now occur on or about 5 Apr 2024.

Major changes include:

Fields 014 thru 017 have been eliminated and are now RESERVED.

Fields 039 thru 043 have been eliminated and are now RESERVED.

Field 058 validations have changed.

Field 067 definitions have changed.

Field 071 has removed North Macedonia from the Non-Designated Country list.

Field 072 has added North Macedonia to the Designated Country list.

See link for the new batch quote instructions.

<https://www.dla.mil/Portals/104/Documents/InformationOperations/EBS%20Supplier%20Information/DIBBS%20Batch%20File%2023%20Feb%202024.docx?ver=QaUeLbpRZP3poyZLji4D-w%3d%3d>



LAND SUPPLY CHAIN - "HOT" ITEMS LIST

Do you have parts on hand? Government surplus? Manufacturers' overruns?

DLA Land Supply Chain has posted a list of items that are urgently needed at: [Selling to DLA Land and Maritime](#)

We are looking for readily available and usable material. We are asking our industry partners to review this list and let us know if you have surplus, manufacturers' overruns, or residual inventory. The intent is to update this list monthly so please check back regularly.

Please submit inquiries to FL.AvailMat@dlamail.

