DLA
DEFENSE LOGISTICS AGENCY

The Nation's Combat Support Logistics Agency

DLA Troop Support Overview of Cybersecurity Requirements

November 17, 2021

Agenda

- Key Terms
- Background
- Current NIST CDI Requirements
- How to Identify a CDI Procurement
- New Vendors - Steps for Procurements with CDI
- Vendor Resources
- Future CMMC Requirements

Key Terms

- **Covered Defense Information (CDI)**: Means unclassified controlled technical information or other information such as Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) that require safeguarding or dissemination controls. For purposes of determining if the CDI/NIST cybersecurity requirements apply, the CDI should be:
  - Marked or otherwise identified in the procurement and provided to the contractor by or on behalf of DoD in support of the performance of the contract (i.e. export control drawings provided to vendors by DLA)
  - Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. (i.e. tech data of a contract item developed by the vendor as part of performance)

- **National Institute of Standards and Technology (NIST) Special Publication 800-171**: Document that contains the actual cybersecurity requirements for protection of CDI.
- **Commercially available off-the-shelf (COTS) item:** A commercial item that is sold in substantial quantities in the commercial marketplace and offered to the Government without any modification to what is sold commercially.

Background

- DoD is taking a phased approach to implementing cybersecurity requirements.

- DFARS clause 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting” implemented requirements to protect CDI and has been a required clause since 2015 for contracts with CDI

- In December of 2020, new requirements were implemented that require vendors to complete a NIST self-assessment and post their score in Supplier Performance Risk System (SPRS) to eligible for awards that have CDI.

- In the future, Cybersecurity Maturity Model Certification (CMMC) is expected to be implemented on most procurements, including those that do not have CDI
  - On November 4, 2021, DoD announced CMMC 2.0
  - Only limited information is currently available about CMMC 2.0

Current NIST CDI Requirements

- Vendors are required do a NIST self-assessment of applicable systems if CDI applies
- Self-assessments are done only for the applicable vendor system(s) that handle CDI and not all vendor IT systems
- Vendors must evaluate the 110 NIST elements to determine if they meet each requirement.
  - Vendors start with a 110 score and deduct points for each element they do not meet, with different weights
- Having a low or negative score is acceptable and the vendor would still become eligible for award
  - Vendors should continue working on improving their score

Current NIST CDI Requirements (continued)

- Vendors must post their NIST self-assessment score on SPRS prior to any award. **If no assessment is posted on SPRS then the vendor is not eligible for award.**

- The NIST self-assessment and SPRS posting requirements only apply to procurements with CDI

- Only exceptions for procurements with CDI are:
  - COTS items
  - Actions below micro-purchase threshold

How to Identify a CDI Procurement

- If any of the following indicators are contained in the DLA solicitation, CDI applies to the procurement:
  - Tech Note RD002 - Covered Defense Information Applies
  - Tech Note RD003 - Covered Defense Information Potentially Applies
  - Tech Note RQ032 - Export Control of Technical Data
  - Other solicitation CDI applicability statement or narrative is included stating that CDI applies to the procurement

- If CDI does not apply prior to award but CDI is identified or created after award, the NIST self-assessment and posting requirements would apply on a Postaward basis.
  - In such a situation, failure to post a NIST self-assessment score to SPRS on a post-award basis could result in termination of the contract.

Sample of RFQ CDI Indicator

SECTION B

PR: 0090079099
NSN/MATERIAL:8110002545719

ITEM DESCRIPTION
DRUM,SHIPPING AND STORAGE

RA001: THIS DOCUMENT INCORPORATES TECHNICAL AND/OR QUALITY REQUIREMENTS (IDENTIFIED BY AN 'R' OR AN 'I' NUMBER) SET FORTH IN FULL TEXT IN THE DLA MASTER LIST OF TECHNICAL AND QUALITY REQUIREMENTS FOUND ON THE WEB AT: http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx
FOR SIMPLIFIED ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE SOLICITATION ISSUE DATE OR THE AWARD DATE CONTROLS. FOR LARGE ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE RFP ISSUE DATE APPLIES UNLESS A SOLICITATION AMENDMENT INCORPORATES A FOLLOW-ON REVISION, IN WHICH CASE THE AMENDMENT DATE CONTROLS.

RP001: DLA PACKAGING REQUIREMENTS FOR PROCUREMENT

RQ011: REMOVAL OF GOVERNMENT IDENTIFICATION FROM NON-ACCEPTED SUPPLIES

MILITARY STANDARD
P/N MS24347-2
MATERIAL STEEL, 26 GAGE/GAUGE, 167 CU. IN. CAPACITY
CLASS S AND TYPE 1
TECHNICAL DATA AVAILABILITY:
I/L/O ASTM A366, USE ASTM A1008/A1008M

RD002, COVERED DEFENSE INFORMATION APPLIES

IAW BASIC SPEC NR MS24347F NOT 3
REVISION NR DTD 04/12/2001
PART PIECE NUMBER:

New Vendor Steps for Procurements with CDI

If a vendor expects to compete for procurements with CDI and the vendor does not have a NIST self-assessment score posted in SPRS, the following actions should be taken proactively:

(1.) Review DFARS clauses, NIST SP 800-171 publication, NIST SP 800-171 DoD Assessment Methodology and other resources to learn what actions need to be taken.

(2.) Conduct the self-assessment by using the NIST SP 800-171 DoD Assessment Methodology document which has the actual methodology and self-assessment scoring criteria.

(3.) Concurrently, while doing the self-assessment, the vendor should begin drafting their system security plan, NIST Plan of action and Milestones (POAM), and Subcontractor flow down plan.

(4.) The vendors shall post their score on the SPRS website.

(5.) Vendors who post a score below 110 should work on improving areas that they do not meet or are unsure of, updating SPRS when they make improvements.

Vendor Resources

- **DFARS 204.73 and DFARS Clauses**: DFARS and DFARS clauses provide guidance and links related to the requirements

- **Project Spectrum**: Website designed to help vendors understand CMMC as part of an initiative supported by the DoD Office of Small Business Programs (https://projectspectrum.io). Project Spectrum provides information, training, and risk assessments to help vendors improve cyber readiness and comply with DoD requirements.

- **PTAC**: PTACs help businesses understand Government contracting requirements, provide tips to make application processes easier and more successful. PTACs have developed additional guides relating to NIST self-assessments.

- **NIST SP 800-171 publication**: The actual standard for ensuring cybersecurity that needs to be met to safeguard CDI and which provides more detail on the requirements that must be met.

- **NIST SP 800-171 DoD Assessment Methodology**: This document provides actual information on how vendors should score each of the 110 elements of the NIST requirements.

- **SPRS website**: SPRS has a job aid and Q&A on posting assessments

Future CMMC Requirements

- CMMC strategy has been revised as part of CMMC 2.0 but few details have been released

- Preliminary overview of CMMC 2.0
  - Information is subject to change as DoD finalizes and releases more guidance
  - Appears that implementation will not be until 2025.
  - CMMC now has only 3 levels
  - Level 1 for non-CDI procurements will now be based on vendor self-assessment
  - Level 2 will likely cover all current CDI procurements
    - A subset will be based on an annual self-assessment vs third-party assessment
  - Level 2 is only based on NIST and CMMC unique requirements were removed
  - Level 3 is unlikely to apply to any DLA procurements
  - A minimum score and a Plan of Actions and Milestones (POA&M) may be acceptable for award eligibility vs having to meet all requirements prior to award
  - CMMC 2.0 intends to reduce vendor costs

- DoD will engage in rulemaking and could change requirements as part of this process
  - Part of rulemaking process will seek and consider public comments

- **DLA will provide further guidance prior to implementing CMMC**