COMPLIANCE WITH DFARS 252.204-7020 NIST SP 800-171 DoD ASSESSMENT REQUIREMENTS

Thank you for your efforts to date to secure controlled unclassified information (CUI) by ensuring that if you receive, transmit, create, or store CUI, your information technology environment is compliant with DFARS 252.204-7012. General Dynamics Mission Systems depends on our suppliers to help us protect the information that supports our customer missions.

On November 30, 2020, an interim rule will be effective to amend the Defense Federal Acquisition Regulation Supplement (DFARS). This interim rule will implement the following requirements for **verifying** a contractor's compliance with cybersecurity requirements in accordance with DFARS 252.204-7012 and to enhance the protection of CUI within the Department of Defense (DoD) supply chain:

1. DoD Assessment Methodology; and
2. Cybersecurity Maturity Model Certification (CMMC) framework.

What DFARS clauses have been added?

Three new regulations will further define contractor obligations to protect Department of Defense (DoD) Controlled Unclassified Information (CUI) in addition to DFARS 252.204-7012. The interim rule adds the following new DFARS clauses:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements

DFARS 252.204-7021 clause formally begins DoD's adoption of the Cybersecurity Maturity Model Certification (CMMC). CMMC requirements will be implemented on a contract by contract basis incrementally over the new five years. DFARS 252.204-7019 and DFARS 252.204-7020 require that all contractors maintain a current DoD assessment score (less than three years old, using the DCMA assessment methodology) in the DoD Supplier Performance Risk System (SPRS), and that prior to awarding contracts/subcontracts involving CUI, the contracting organization must confirm that a current DoD assessment score is in SPRS. To the extent these clauses are included in **new** GDMS prime contracts, these obligations will flow to all organizations in the supply chain who manage CUI with their subcontractors.

DFARS 252.204-7020 and DFARS 252.204-7021 are required flow-downs in all subcontracts, purchase orders, or other contractual instruments, including for commercial items. They exclude procurements of solely COTS items and procurements at or below the micro-purchase threshold (currently $10,000).

Requested Actions:

To avoid disruptions to future business, suppliers should begin taking the following actions immediately:

Ensure that you have a current DoD Assessment score in SPRS (for all CAGE codes covered by your System Security Plan (SSP)). Information regarding SPRS is available at the following link: https://www.sprs.csd.disa.mil/. If you do not have an account in SPSR, register at https://piee.eb.mil/piee-landing/ and include the role of SPRS.

- **At a minimum**, determine your score through the basic assessment (self-assessment), and submit it to DoD in accordance with DFARS 252.204-7020. (Reference: Annex B within NIST SP 800-171 DoD Assessment Methodology, V1.2.1)
- If your organization's NIST SP 800-171 implementation was already assessed by the DCMA (DIBCAC medium or high assessment) and you have received your score, you should have satisfied this requirement. However, suppliers should confirm that their medium or high assessment scores are posted in SPRS.
- Consider requesting DCMA perform a DIBCAC Medium or High confidence assessment. The external assessment will not only document your score in SPRS, but it will also help your organization prepare for CMMC (third-party) assessment required in DFARS 252.204-7021.

DoD has indicated that it will take approximately 30 days to post a basic self-assessment in SPRS, if you choose to send your basic assessment to DoD for posting in SPRS in accordance with the procedures in DFARS 252.204-7020. Alternatively, suppliers may post their own basic assessment scores in SPRS using the link above. After November 30, 2020, we will not be able to issue you an award under a DoD contract containing these requirements, unless you have a DoD assessment posted in SPRS. It is imperative that you take action immediately to avoid disruptions to future business.

- **Address the Additional CMMC Practices and Processes Now**

  - We anticipate future guidance from DoD regarding the CMMC process with the CMMC accreditation body.
  - To the extent a new solicitation or contract includes CMMC requirements per DFARS 252.204-7021, **you must have an assessment score of level 3 or greater to receive, store, create, or transmit CUI.**
  - To achieve CMMC Level 3 certification by a CMMC Third-Party Assessor Organization (C3PAO), organizations need to demonstrate

implementation of all 130 Level 3 practices (NIST 800-171's 110+20), as well as the three processes associated with Maturity Level (ML) 3 (inclusive of ML2). Plans of Action and Milestones (POAMs) will not satisfy the certification requirement.
    - Additional information regarding CMMC is available at the following:
        - https://www.acq.osd.mil/cmmc/index.html
        - https://www.cmmcab.org/

- **Provide Status to General Dynamics Mission Systems.**

    - In order for General Dynamics Mission Systems to assess risk and preparedness for the November 30 effective date of the new rules, we must receive the status of our applicable suppliers. We request that you complete the attached representation and certification and return it to us at RepsCerts@gd-ms.com.

As we anticipate seeing the DoD CMMC requirements in RFIs/RFPs/Contracts in late-2020/early-2021, addressing outstanding actions now to become fully compliant with all security requirements is the best strategy for staying ahead of the curve and minimizing potential supply chain disruptions.

Thank you in advance for your cooperation and we will continue to update you as implementation of these regulations evolves.

Additional Resources

- The DIB SCC CyberAssist site provides resources to assist Defense Industrial Base (DIB) companies and suppliers of varying sizes with their implementation of cyber protections, accountability for their supply chain, and awareness of cyber risk and regulations, including recently added CMMC resources.
- DoD Procurement Toolbox
- DoD CUI
- NIST SP 800-171 Rev 2