GDIT

December 2023

Dear GDIT Supplier,

General Dynamics Information Technology, Inc. (GDIT) depends on our Suppliers to help us protect information that supports our customer missions. We appreciate your efforts to secure controlled unclassified information (CUI) to ensure that if you receive, transmit, create, or store CUI, your information technology environment is compliant with Defense Federal Acquisition Regulations Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

On November 30, 2020, an interim rule amended DFARS to implement requirements for verifying a Prime Contractor's compliance with cybersecurity requirements of DFARS 252.204-7012: DoD Assessment Methodology and Cybersecurity Maturity Model Certification (CMMC) Framework. Suppliers and Subcontractors under Prime Contractors will also be required to verify compliance to enhance the protection of CUI within the Department of Defense (DoD) supply chain.

Three new DFARs clauses will be added under this interim rule to further define Prime Contractor and Supplier/Subcontractor obligations to protect DoD CUI.

- 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 252.204-7019 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, or purchase orders involving CUI, the Government or Prime Contractor must confirm that a current DoD assessment score is in SPRS. To the extent these clauses are included in GDIT prime contracts, these obligations will flow to all Suppliers and Subcontractors who manage CUI under a Purchase Order, Subcontractor, or other contractual instruments from GDIT.

Additionally, DFARS 252.204-7020 is a required flow-down 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/
- 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)

  DoD has indicated that it will take approximately 30 days to post a basic self-assessment in SPRS. As of December 1, 2020, we will not 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.

- If your organization's NIST SP 800-171 implementation was already assessed by 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.

Address Additional CMMC Practices and Processes Now

- We anticipate future guidance from DoD regarding the CMMC process with the CMMC accreditation body.
- Additional information regarding CMMC is available at the following:
    - https://www.acq.osd.mil/cmmc/index.html
    - https://www.cmmcab.org/

Certify Status to GDIT Upon Request

- GDIT requires certification from Suppliers that you have a DoD assessment posted in SPRS for any new awards or change orders/modifications to existing awards containing these requirements. It is imperative that you complete the certification and return the GDIT requestor in a timely manner.

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:
- CMMC resources.
- DoD Procurement Toolbox
- DoD CUI
- NIST SP 800-171 Rev 2

Sincerely,

Alexis McGuire

SCM Staff Vice President
& Chief Supply Chain Officer

Lisa Lax

Vice President
Contracts & Acquisition Management Office