

DATE: October 27, 2020

TO: Booz Allen Suppliers

SUBJECT: Ramp Up Oversight and Compliance Enforcement of the Protection of Controlled Unclassified Information (CUI) of Defense Contractors by the Department of Defense (DoD)

As malicious cyber actors continue to target U.S. Defense Industrial Base (DIB) companies throughout the supply chain, the DoD is responding to cyber incidents and driving significant changes to DoD acquisition policies.

On September 29, 2020, DoD issued an interim final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) in order to better assess contractor implementation of cybersecurity requirements. The interim rule amends the DFARS and establishes three new DFARS clauses:

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements;
- DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements; and
- DFARS clause 252.204-7021, Cybersecurity Maturity Model Certification (CMMC) Requirements.

DFARS 252.204-7012 is currently included in all DoD solicitations and contracts except for acquisitions solely for commercially available off-the-shelf (COTS) items. This clause requires contractors to apply the security requirements of NIST SP 800-171 to “covered contractor information systems” that are not part of an IT service or system operated on behalf of the Government. Many of our suppliers have indicated that they are currently in compliance with NIST SP 800-171 security requirements pursuant to DFARS 252.204-7012.

Compliance with NIST SP 800-171 has always been based on self-attestations. The new DFARS 252.204-7019 and DFARS 252.204-7020 clauses revise this process by mandating the use of the NIST SP 800-171 DOD Assessment Methodology, which provides for the standardized assessment of a contractor’s implementation of NIST SP 800-171 security requirements. The Assessment uses a standard scoring methodology and three assessment levels (Basic, Medium, and High). A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The results of Assessments will be documented in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility into the scores of Assessments already completed.

Separately, the interim final rule clarifies that DoD is implementing a phased rollout of CMMC. Starting October 1, 2025, the interim final rule’s new CMMC clause will be included in all DoD solicitations and contracts, including those for the acquisition of commercial items (except those for exclusively COTS items) valued at greater than the micro-purchase threshold. In the interim, DoD has indicated the CMMC clause will be included in only a limited number of contracts as specifically approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment. Contracting Officers will not

make award, or exercise an option, on a contract including the new CMMC clause, if the offeror or contractor does not have a current (i.e. not older than three years) certification for the required CMMC level.

Booz Allen Suppliers Should Carefully Review the New Interim Final Rule and DoD Guidance to Ensure Timely Compliance

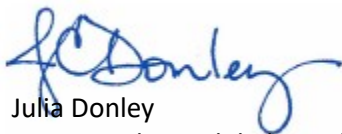
Booz Allen shares the DoD's concerns with, and commitment to, cybersecurity and safeguarding information from our adversaries. Take the time to understand and comply with the new DFARS clauses and how you play a critical role in demonstrating our commitment to making the client's mission our own. You should understand and complete any outstanding implementation of policy and/or technical controls under the new clauses by visiting the [Federal Register DFARS Case 2019-D041](#). You must also ensure your suppliers are informed of these new clauses and have completed their Basic Assurance assessment and uploaded their score to the SPRS database.

For contracts including the new DFARS clause at 252.204-7020, contractors will be prohibited from awarding a subcontract or other contractual instrument, for which subcontract performance will involve covered defense information, unless the subcontractor has completed and posted to SPRS, within the last 3 years, a Basic NIST SP 800-171 DoD Assessment at a minimum. The clause also provides additional information on how a subcontractor can conduct and submit an Assessment to SPRS and requires the contractor to include the requirements of the clause in all lower-tiered subcontracts or other contractual instruments.

Therefore, in the near future, in order to perform certain work for Booz Allen under a DoD contract or subcontract, it will be necessary for Booz Allen suppliers to have completed at least a Basic NIST SP 800-171 DoD Assessment and posted the results of the Assessment to SPRS. More information on the NIST SP 800-171 DoD Assessment Methodology is available [here](#). More information on SPRS is available [here](#).

For contracts including the new CMMC Clause, contractors will be required to flow down the appropriate CMMC certification requirement to subcontractors through the entire supply chain. More information on CMMC and a copy of the CMMC model can be found [here](#).

Sincerely,



Julia Donley
Vice President, Global Supply Chain