November 24, 2020

Attention: All Suppliers

Subject: Contractor Compliance with Cybersecurity Maturity Model Certification (CMMC)

Ref: DFARS 252.204-7019 Notice of NIST SP800-171 DoD Assessment Requirements; DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements; and DFARS 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Dear Austal USA Supplier,

This communication is to inform you of an interim rule (DFARS Case 2019-D041) – Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, the Department of Defense (DoD) published on September 30. The interim rule takes effect November 30, 2020 and will require immediate action by the DoD and Austal supply chain to be eligible to receive awards after the interim rule goes into effect.

Currently, pursuant to DFARS 252.204-7012, government suppliers must provide adequate security for covered contractor information systems. A "covered contractor information system" is defined as an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

More specifically, government suppliers must protect such information systems by implementing the security controls of National Institute of Standard and Technology (NIST) Special Publication (SP) 800-171.1. In order to further protect Department of Defense (DoD) Controlled Unclassified Information (CUI), the DFARS has been amended with an *interim rule* that adds three new cybersecurity clauses related to compliance assessments effective November 30, 2020. Here is a brief overview of the current and new cybersecurity DFARS clauses:

Current

- *DFARS 252.204-7012 "Safeguarding CDI & Cyber Incident Reporting"* (effective December 31, 2017)
    - Organizations that store, process, or transmit "Covered Defense Information" must implement the 110 security controls outlined in *NIST SP800-171 "Protecting CUI in Nonfederal Systems & Organizations"*

New

- *DFARS 252.204-7019 "Notice of NIST SP800-171 DoD Assessment Requirements"*
  - In order to be considered for award, offerors required to implement NIST SP800-171 must have a current (less than 3-years old) assessment score posted to "Supplier Performance Risk System" (SPRS).

- *DFARS 252.204-7020 "NIST SP800-171 DoD Assessment Requirements"*
  - Requires a contractor to provide the Government with access to its facilities, systems, and personnel (ie, on-site assessment) when it is necessary for DoD to conduct or renew a higher-level assessment. Three levels of assessment include "basic" self-assessment, "medium" documentation assessment, and "high" on-site assessment.
  - Requires the contractor to ensure that applicable subcontractors also have the results of a current assessment posted in SPRS prior to awarding a subcontract.

- *DFARS 252.204-7021 "Cybersecurity Maturity Model Certification (CMMC) Requirements"*
  - ***CMMC*** has five certification levels that build upon DFARS 252.204-7012 and NIST SP800-171. Contracts will specify CMMC level requirement and will require an accredited ***"CMMC Third-Party Assessor Organization"*** (C3PAO) to certify your organization to the contractually required CMMC level.
  - Requires a contractor to maintain requisite CMMC level for duration of contract (**CMMC certification required at time of award** rather than at time of proposal or after contract award).
  - Requires a contractor to **ensure that its subcontractors also have appropriate CMMC level** prior to awarding subcontract.
  - Requires a contractor to flow down contract clause.
  - DoD plans to phase in CMMC requirements into new contract awards over the next five years.

Please take the following actions immediately:

1. **Determine if these clauses apply** to your organization. These clauses apply to contractor information systems that process, store, or transmit Covered Defense Information, unclassified Controlled Technical Information or other information as described in the Controlled Unclassified Information (CUI) Registry at *http://www.archives.gov/cui/registry/category-list.html* that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies.

   - If you are a supplier who does not handle sensitive DoD information as described above, this isn't applicable to you; thus, you are not required to complete the cybersecurity fitness assessment. There is no further action at this time.
   - If this is applicable, continue with the following steps.

2. **Conduct a self-assessment** in accordance with the following guidance. *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html*

3. **Request user access** to DoD's "Supplier Performance Risk System" (SPRS) at *https://www.sprs.csd.disa.mil/access.htm* if your organization doesn't already have access.

4. **Upload your self-assessment to SPRS**.

5. **Email supplierinfo@austalusa.com no later than COB November 30, 2020** stating that your organization is compliant with DFARS 252.204-7019 with results of a current assessment posted in SPRS.

6. You must **insert the substance of DFARS 252.204-7020**, including paragraph (g) titled "subcontracts," in all solicitations and contracts for your purchasing, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.

Thanks again for your partnership in building and maintaining world class ships for the Navy. Please contact the SCM Compliance Manager, Carey Uhle (carey.uhle@austalusa.com), with any questions.

Very Truly Yours,

Bill Rebarick
Vice President, Supply Chain Management