AEROJET ROCKETDYNE

2001 Aerojet Road
Rancho Cordova, CA 95742-6418

16 September 2020

SUBJECT: CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Dear Valued Supplier:

Aerojet Rocketdyne (AR) is a proud contractor to the United States Department of Defense (DoD), and we have been closely watching the DoD's development of the new CMMC process. It is our intent with this letter to ensure that all AR suppliers on DoD programs are aware of and getting ready for CMMC. You have probably heard through industry associations, news sources or training providers about CMMC and that it takes cybersecurity compliance to the next level.

While the CMMC development has been dynamic and had some delays, here are key points as we currently understand them:

- Suppliers no longer self-attest to cybersecurity compliance; CMMC requires an accredited third party audit.

  NOTE: Unlike the current environment where suppliers must have detailed System Security Plans to address the various controls and can have Plans of Action and Milestones to remediate any open items, the CMMC will not provide certification unless all relevant controls for the level are met. If the audit results in findings and requires corrective action, a recertification audit will likely be necessary before a firm is eligible to be certified. With over 300,000 firms in the DoD supply chain, scheduling audits and subsequent re-checks could take a considerable time.

- An accreditation body has been formed and many firms are being trained to audit the DoD supply chain.
- There are five levels of certification (from 1 to 5). For instance:
  - Level 1 is the minimum "cybersecurity hygiene" which even those that possess Federal Contract Information (FCI) subject to FAR 52.204-21 will be required to have.
  - Level 3 certification is the minimum level for processing Controlled Unclassified Information (CUI). A significant portion of the existing framework relies on NIST 800-171 controls already required by DFARS 252.204-7012 (assessed via NIST 800-171A Assessment Guide) and the, yet to be finalized, NIST 800-171 B "enhanced controls."
- Beginning in late 2020, DoD is expected to issue 10 Requests for Proposals (RFPs) with CMMC requirements for prime contractors. (There is still some debate on the requirement for subcontractors in the 2020 RFPs.)
- At some point, *EVERY supplier on a DoD program at all tiers* must be certified (if certification is a requirement of the DoD prime contract). Certification may be required to submit a proposal or, at the latest, prior to award of the prime contract.
- Suppliers who do not qualify to be certified at a level 1 (or higher as is required to participate on a contract) will be precluded from being on the program.
- It is expected to impact ALL DoD suppliers at all tiers of the supply chain, except those that solely produce commercial-off-the-shelf (COTS) items. The requirement will apply to foreign companies and small businesses.

Information is available on the internet and knowledgeable cybersecurity consultants can help you get ready. Understand and keep current with the status of the CMMC by frequently visiting the DoD OUSD CMMC website. Additionally, AR has created a Cybersecurity page on SupplierNet at www.rocket.com that provides links to many helpful resources.

AR expects that you and your suppliers are informed about the CMMC and are getting ready now. Our customers depend on us to support DoD programs and the nation's defense.

Sincerely,

Chris Stone

Christopher A. Stone
Vice President
Supply Chain/Materiel Management