AEROJET
ROCKETDYNE

2001 Aerojet Road
Rancho Cordova, CA 95742-6418

August 31, 2016

Attention: Supplier Representative, President, General Manager, Contract Manager, Program Manager

Subject: Cyber Security Awareness and Requirements

Dear Aerojet Rocketdyne Supplier:

Our customers rely on Aerojet Rocketdyne and our suppliers to protect and safeguard sensitive data to ensure it does not fall into our adversaries' possession. Our adversaries continue to seek out information in our possession by any means necessary and continue to try to compromise our systems. No one is immune to these attacks. We need our suppliers' cooperation and diligence to ensure we collectively safeguard information entrusted to us by our customers.

Information Technology (IT) security requirements are included in all Aerojet Rocketdyne subcontracts. Depending on the prime contract customer, these requirements may reflect regulations established by either NASA or the Department of Defense (DoD).

NASA IT security requirements have been in place for some time and are stipulated in NASA Federal Acquisition Regulation Supplement (NFS) Clause 1852.204-76, Security Requirements for Unclassified Information Technology Resources. The clause outlines requirements for protection of NASA Electronic Information, which is defined as any data (as defined in the Rights in Data clause of the relevant contract) or information (including information incidental to contract administration, such as financial, administrative, cost or pricing, or management information) that is processed, managed, accessed or stored on an IT system(s) in the performance of a NASA contract. By reference the NASA clause mandates compliance with security policy guidance as outlined by National Institute of Standards Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations. This document extends the protections to be provided for NASA data to all forms of data, not just the data in electronic format, and covers hardcopy, personnel, and physical security controls.

Effective December 30, 2015, the DoD revised and retitled DoD Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting." The new DFARS contract clause expands requirements for the safeguarding of Covered Defense Information (CDI) and requires compliance with the security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. CDI means unclassified information that is provided to the contractor by or on behalf of DoD in the performance of a contract or is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a contract and is either (1) controlled technical information, (2) critical operations security information, (3) export controlled information, or (4) any other information, marked or otherwise identified in a contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., private personal information, proprietary business information, For Official Use Only (FOUO) information, Controlled Unclassified Information, and foreign government information). Full compliance with the requirements of this DFARS clause is required by December 31, 2017. As with the NFS requirements, the clause includes protection of all forms of data, not just the data in electronic format, and covers hardcopy, personnel, and physical security controls.

It is imperative that our suppliers understand and comply with the Information Security requirements stated above and included in Aerojet Rocketdyne subcontracts. During the coming months Aerojet Rocketdyne will be sending out a questionnaire to members of our Supply Base that receive NASA Electronic Information or CDI to ascertain the status of compliance to the Information Security regulations. Please promptly review this questionnaire and designate a point of contact for completion by the specified date. We are also requesting that you take all necessary steps today to communicate and train your personnel in the importance of proactive steps to protecting all NASA Electronic Information and CDI. This includes using encryption, education on suspicious phishing attempts, properly marking documents, and filtering email.

For additional resources please research the following links;

NASA FARS 1852.204-76, Security Requirements for Unclassified Information Technology Resources: http://www.hq.nasa.gov/office/procurement/regs/5200-11.htm

NASA Procedural Requirement (NPR) 2810.1A, Security of Information Technology: http://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2810&s=1A

NASA Information Technology (IT) Applicable Documents List (ADL): http://www.nasa.gov/sites/default/files/atoms/files/attachment_I-information_technology_security_docs_list.pdf

NIST Special Publication (SP) 800-53, Rev 4, Recommended Security Controls for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

Federal Register Ruling: https://www.gpo.gov/fdsys/pkg/FR-2015-08-26/pdf/2015-20870.pdf

DFARS December 30, 2015 update: https://www.gpo.gov/fdsys/pkg/FR-2015-12-30/pdf/2015-32869.pdf

Additional information:

- Federal Register https://www.federalregister.gov/articles/2015/08/26/2015-20870/defense-federal-acquisition-regulation-supplement-network-penetration-reporting-and-contracting-for
- Notable among these are the United States Computer Emergency Readiness Team (US-CERT) https://www.us-cert.gov, and the DoD Defense Industrial Base Cybersecurity Information Sharing Program (DIB CS program), http://dibnet.dod.mil.
- In addition, the DoD Office of Small Business Programs (OSBP) has prepared a cybersecurity fact sheet to help guide small businesses in regulatory compliance, http://www.acq.osd.mil/osbp/docs/Cybersecurity_04272016.pdf

If you have any questions about this communication please contact your Supply Chain Management representative for more information.

Sincerely,

Hal Martin
Vice President
Supply Chain & Material Management

Mark Angelo
Vice President
Information Technology