AEROJET ROCKETDYNE

2001 Aerojet Road
Rancho Cordova, CA 95742-6418

19 November 2020

Dear Supplier to Department of Defense Programs:

| | |
|---|---|
| **SUBJECT:** | **SUPPLY CHAIN CYBERSECURITY COMPLIANCE** |
| **Applicability:** | This letter applies to any supplier of the Aerojet Rocketdyne Companies* that performs work under Department of Defense (DoD) Programs at any tier of the supply chain.<br>Please note, the following is for informational purposes only and not for purposes of providing legal advice. Contact your attorney to obtain legal advice as needed.<br>**If you are NOT a DoD Program supplier, this letter does not apply to you.** |
| **Urgency:** | On September 30, 2020, DoD issued a new interim rule that takes effect on **November 30, 2020,** and requires your immediate action and that of your suppliers as described here. |
| **References:** | • **DFARS Interim Rule** Released 09-30-20 *(DFARS Case 2019-D041 - Defense Federal Acquisition Regulation Supplement (DFARS): Assessing Contractor Implementation of Cybersecurity Requirements).* Full text of 3 new DFARS clauses are in Appendix 1.<br>○ DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements<br>○ DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements<br>○ DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement<br>The new clauses implement a new Cybersecurity Maturity Model Certification (CMMC) framework that will eventually require an outside audit and certification, following the new requirement to complete a self-assessment now, as further described below. |
| **Exceptions:** | There are certain limited exceptions to the requirements, such as solicitations or contracts **solely for Commercial-Off-The-Shelf (COTS) items**, as those items are defined in Federal Acquisition Regulation (FAR) 2.101, Definitions (see DFARS clauses for details). |
| **Contract Flowdowns:** | • **DFARS 252.204-7012,** Safeguarding Covered Defense Information and Cyber Incident Reporting, currently requires DoD suppliers at all levels of the supply chain to provide adequate security for **"covered contractor information systems"**.<br>• A "covered contractor information system" is an *unclassified* information system owned or operated by or for, a contractor and that processes, stores or transmits **Covered Defense Information** (CDI, including "Controlled Unclassified Information" or CUI).<br>• Government suppliers must protect such information and information systems by implementing 110 cybersecurity controls of the **National Institute of Standard and Technology (NIST) Special Publication (SP) 800-171**. |
| **New DFARS Requirements:** | • **Beginning November 30, 2020**, DoD Contracting Officers will begin flowing down the new DFARS 252.204-7019 and 252.204-7020 clauses in all solicitations and contracts that use "covered contractor information systems" at all levels of the DoD supply chain that create, store, process or transmit CDI and CUI.<br>• Suppliers **QUANTIFY** compliance to NIST SP 800-171 DoD Assessment Methodology. |

*Aerojet Rocketdyne Companies include Aerojet Rocketdyne, Inc., Aerojet Ordnance Tennessee, Inc., Aerojet Rocketdyne Coleman Aerospace, Inc., ARDE' Inc., Easton Development Company, LLC, or Aerojet Rocketdyne Holdings, Inc.

| | |
|---|---|
| | • Pursuant to DFARS 252.204-7020, Contractors (such as Aerojet Rocketdyne Companies) may **not** award subcontracts to suppliers who do not implement CMMC or who will not comply with the new requirements (see Actions Required, below). |
| **Actions Required:** | All DoD suppliers (that are not exempt) must take the following actions:<br>1. Complete (at least) a Basic self-assessment of compliance to the NIST SP 800-171 controls using the DoD Assessment Methodology cited above, **AND**<br>2. Submit summary level scores of the assessment and other information required by DFARS 252.204-7020 into the Government's Supplier Performance Risk System (SPRS) or send the information via encrypted emailed to webptsmh@navy.mil; **OR**<br>3. The Government performed a Medium or High Assessment within the last 3 years on supplier's covered contractor information systems applicable to the work performed under DoD contracts (that are not part of an information technology system that the supplier operates on behalf of the Government) and the results of the Government assessment were entered into SPRS; **AND**<br>4. The supplier must flow down DFARS 252.204-7020, including paragraph (g) titled "subcontracts", in all solicitations and contracts, with certain exceptions (such as those solicitations or contracts solely for the acquisition of COTS items). |
| **Evidence of Compliance:** | Please promptly provide evidence of compliance by providing a screen print of your SPRS summary level score or government assessment score, OR send a written attestation that you have completed the *Actions Required*. If you do NOT plan to comply with DFARS cybersecurity requirements, please notify us and provide an explanation. Please send any notification via encrypted email to AerojetRocketdyneSupplyChain@Rocket.com<br>**NOTE: After December 1, 2020**, as soon as Aerojet Rocketdyne Companies receive DoD Requests for Proposals containing the new DFARS clauses, buyers will not be able to request quotes or award contracts for DoD programs without supplier SPRS compliance. |
| **Representations & Certification:** | All DoD suppliers should take action for compliance and be prepared to provide a specific representation and certification of cybersecurity compliance upon request. |
| **More Information and Resources:** | • Visit our Cybersecurity webpage on www.rocket.com in SupplierNet that provides links to government cybersecurity source documents and Company documents.<br>• It is important that you continue your actions to become CMMC certified to the appropriate level required to participate in DoD programs.<br>• It is also important that you assist your lower-tier suppliers to be aware of CMMC and become compliant to continue to participate on DoD programs. |
| **Questions:** | Aerojet Rocketdyne procurement personnel cannot answer questions about cybersecurity requirements. Please review the resources on our webpage or widely available on the internet, consult your Legal Counsel or Information Technology Cybersecurity professionals. |

Sincerely,

*Mariel Dennis*

Mariel Dennis
Director, Supply Chain Materiel Management Compliance

# APPENDIX 1 – NEW DFARS CLAUSES

## DFARS 252.204–7019, Notice of NIST SP 800–171 DoD Assessment Requirements

As prescribed in 204.7304(d), use the following provision: **NOTICE OF NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)**

(a) *Definitions.*
*Basic Assessment, Medium* Assessment, and *High Assessment* have the meaning given in the clause 252.204–7020, NIST SP 800– 171 DoD Assessments.
*Covered contractor information system* has the meaning given in the clause 252.204– 7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.
(b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204–7020) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800–171 DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology located at
*https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html* .
(c) *Procedures.*
(1) The Offeror shall verify that summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/* ) for all covered contractor information systems relevant to the offer.
(2) If the Offeror does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to *webptsmh@navy.mil* for posting to SPRS in the format identified in paragraph (d) of this provision.
(d) *Summary level scores.* Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to provide DoD Components visibility into the summary level scores of strategic assessments.
(1) *Basic Assessments.* An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.
(i) The email shall include the following information:
(A) Cybersecurity standard assessed (*e.g.,* NIST SP 800–171 Rev 1).
(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).
(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—
(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and
(*2*) A brief description of the system security plan architecture, if more than one plan exists.

(D) Date the assessment was completed.
(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).
(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.
(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

- System security plan
- CAGE codes supported by this plan
- Brief description of the plan architecture
- Date of assessment
- Total score
- Date score of 110 will be achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:
(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).
(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).
(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.
(iv) A brief description of the system security plan architecture, if more than one system security plan exists.
(v) Date and level of the assessment, *i.e.,* medium or high.
(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).
(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.
(3) *Accessibility.* (i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).
(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*.
(iii) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as ''Controlled Unclassified Information (CUI)'' and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

## DFARS 252.204–7020, NIST SP 800–171 DoD Assessment Requirements

As prescribed in 204.7304(e), use the following clause: **NIST SP 800–171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)**

(a) *Definitions.*

*Basic Assessment* means a contractor's self assessment of the contractor's implementation of NIST SP 800–171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology; and

(3) Results in a confidence level of ''Low'' in the resulting score, because it is a self generated score.

*Covered contractor information system* has the meaning given in the clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

*High Assessment* means an assessment that is conducted by Government personnel using NIST SP 800–171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of ''High'' in the resulting score.

*Medium Assessment* means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review; and

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of ''Medium'' in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment, as described in NIST SP 800–171 DoD Assessment Methodology at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html*, if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (*https://www.sprs.csd.disa.mil/*) to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800–171 DoD Assessment Methodology to *webptsmh@navy.mil* for posting to SPRS.

(i) The email shall include the following information:
(A) Version of NIST SP 800–171 against which the assessment was conducted.
(B) Organization conducting the assessment (*e.g.,* Contractor self-assessment).
(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—
(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan; and
(*2*) A brief description of the system security plan architecture, if more than one plan exists.
(D) Date the assessment was completed.
(E) Summary level score (*e.g.,* 95 out of 110, NOT the individual value for each requirement).
(F) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.
(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

- System security plan CAGE codes supported by this plan
- Brief description of the plan architecture
- Date of assessment
- Total score
- Date score of 110 will be achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:
(i) The standard assessed (*e.g.,* NIST SP 800–171 Rev 1).
(ii) Organization conducting the assessment, *e.g.,* DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).
(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.
(iv) A brief description of the system security plan architecture, if more than one system security plan exists.
(v) Date and level of the assessment, *i.e.,* medium or high.
(vi) Summary level score (*e.g.,* 105 out of 110, not the individual value assigned for each requirement).
(vii) Date that all requirements are expected to be implemented (*i.e.,* a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800–171.
(e) *Rebuttals.* (1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*).
(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.
(f) *Accessibility.*

(1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).
(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at *https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf*.
(3) A High NIST SP 800–171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as ''Controlled Unclassified Information (CUI)'' and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (*e.g.,* Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).
(g) *Subcontracts.*
(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).
(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800–171 security requirements, in accordance with DFARS clause 252.204–7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800–171 DoD Assessment, as described in *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html*, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.
(3) If a subcontractor does not have summary level scores of a current NIST SP 800–171 DoD Assessment (*i.e.,* not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800–171 DoD Assessment Methodology, to *webptsmh@navy.mil* for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

## DFARS 252.204–7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

As prescribed in 204.7503(a) and (b), insert the following clause: **CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (NOV 2020)**
(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see *https://www.acq.osd.mil/cmmc/index.html*).
(b) *Requirements.* The Contractor shall have a current (*i.e.* not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.
(c) *Subcontracts.* The Contractor shall—
(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (*i.e.,* not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

(End of clause)