

LOCKHEED MARTIN AERONAUTICS COMPANY
PRIME SUPPLEMENTAL FLOWDOWN DOCUMENT (PSFD)
ADDITIONAL TERMS AND CONDITIONS
FOR SUBCONTRACTS/PURCHASE ORDERS UNDER

Accounting Standards. Seller shall provide Lockheed Martin with copies of all communications concerning CAS between and the Contracting Officer if such are relevant to this contract; provided however, Seller shall not be required to disclose to Lockheed Martin such communications containing information which is privileged and confidential to Seller.")

FAR 52.227-11 ALT I PATENT RIGHTS – OWNERSHIP BY THE CONTRACTOR – ALTERNATE I, II, III, AND/OR IV (AS APPLICABLE) (DEC 2007) (Applies if this Contract, at any tier, is for experimental, developmental, or research work. Reports required by this clause shall be filed the agency identified in this

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/documentstemplates/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to --

(1) Allow DoD to request the media or decline interest; or

(2) For any United Kingdom (UK) company within scope of the UK MOD ISN Number 2021/03, allow the national/designated security authority for the UK to coordinate with the DC3 so that the DC3 may request the national/designated security authority to provide information obtained from the media related to covered defense information provided by or developed for DoD that may have been compromised or to decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis, unless the Contractor is a UK company within scope of the UK MOD ISN Number 2021/03.

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause,

(d) Procedures. Excluding any UK company within scope of the UK MOD ISN Number 2021/03, 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 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) Foreach 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 thetn heecr

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 <mailto:webptsmh@navy.mil> for posting to SPRS along with the information required by paragraph (d) of this clause

Revision 2 dated July 25, 2024. The following Special Provision clauses have been added:

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBERINCIDENT REPORTING (MAY 2024)

NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2023)