Where necessary, to identify the applicable parties under the following clauses, “Contractor” shall mean “Seller,” “Contracting Officer” shall mean “Lockheed Martin Procurement Representative,” “Contract” means this subcontract and “Government” means “Lockheed Martin.” However, the words “Government” and “Contracting Officer” do not change: (1) when a right, act, authorization or obligation can be granted or performed only by the Government or the Prime Contract Contracting Officer or duly authorized representative, including but not limited to (i) audit rights to Seller’s proprietary business records or (ii) any indemnification or limitation of liability obligation, which obligation shall remain with the Government; (2) when title to property is to be transferred directly to the Government, and (3) when the Government is granted ownership or other rights to Seller’s intellectual property or technical data.

**Full Text Clauses**

**Section H – Special Contract Requirements**

**SMC—H001 ENABLING CLAUSE FOR GOVERNMENT PROGRAM CONTRACTS REQUIRING INTERFACE WITH AEROSPACE FFRDC CONTRACT SUPPORT (JUL 2020)** (Applicable for all purchase orders/subcontracts.)

a. This contract covers part of the Evolved Strategic SATCOM (ESS) program which is under the general program management of the Air Force Space and Missile Systems Center (SMC). The Air Force has entered into a contract with The Aerospace Corporation, a California nonprofit corporation operating a Federally Funded Research and Development Center (FFRDC), for the services of a technical group that will support the DoD/U.S. Government program office by performing General Systems Engineering and Integration, Technical Review, and/or Technical Support including informing the commander or director of the various Department of Defense (“DoD”) organizations it supports and any U.S. Government program office of product or process defects and other relevant information, which, if not disclosed to the U.S. Government, could have adverse effects on the reliability and mission success of a U.S. Government program.

1. General Systems Engineering and Integration (GSE&I) deals with overall system definition; system safety, integration both within the system and with associated systems; analysis of system segment and subsystem design; design compromises and tradeoffs; definition of interfaces; review of hardware and software, including manufacturing and quality control; observation, review and evaluation of tests and test data; support of launch, flight test, and orbital operations; appraisal of the contractors' technical performance through meetings with contractors and subcontractors, exchange and analysis of information on progress and problems; review of plans for future work; developing solutions to problems; technical alternatives for reduced program risk; providing comments and recommendations in writing to the applicable DoD System Program Manager and/or Project Officer as an independent technical assessment for consideration for modifying the program or redirecting the contractor's efforts; all to the extent necessary to assure timely and economical accomplishment of program objectives consistent with mission requirements.

2. Technical Review (TR) includes the process of appraising the technical performance of the contractor through meetings, exchanging information on progress and problems, reviewing reports, evaluating presentations, reviewing hardware and software, witnessing and evaluating tests, analyzing plans for future work, evaluating efforts relative to contract technical objectives, and providing comments and recommendations in writing to the applicable Air Force Program Manager as an independent technical assessment for consideration for modifying the program or redirecting the contractor's efforts to assure timely and economical accomplishment of program objectives.

3. Technical Support (TS) deals with broad areas of specialized needs of customers for planning, system architecting, research and development, horizontal engineering, or analytical activities for which The Aerospace Corporation is uniquely qualified by virtue of its specially qualified personnel, facilities, or corporate memory. The categories of TS tasks are: Selected Research, Development, Test and Evaluation; Plans and System Architecture; Multi-Program Systems Enhancement; International Technology Assessment; and Acquisition Support.

In the performance of this contract, the Contractor agrees to cooperate with The Aerospace Corporation by

1) responding to invitations from authorized U.S. Government personnel to attend meetings;

2) by providing access to technical information and research, development planning data such as, but not limited to, design and development analyses, test data and results, equipment and process specifications, test and test equipment specifications and procedures, parts and quality control procedures, records and data, manufacturing and assembly procedures, and schedule and milestone data, all in their original form or reproduced form and including top-level life cycle cost data, where available;

3) by discussing technical matters relating to this program;

4) by providing access to Contractor facilities utilized in the performance of this contract;

5) and by allowing observation of technical activities by appropriate technical personnel of The Aerospace Corporation. The Aerospace Corporation personnel engaged in GSE&I, TR, and/or TS efforts:

(i) are authorized access to all such technical information (including proprietary information) pertaining to this contract and may discuss and disclose it to the applicable DoD personnel in a program office;

(ii) are authorized to discuss and disclose such technical information (including proprietary information) to the commander or director of the various DoD organizations it supports and any U.S. Government personnel in a program office which, if not disclosed to the U.S. Government, could have adverse effects on the reliability and mission success of a U.S. Government program; and

(iii) Aerospace shall make the technical information (including proprietary information) available only to its Trustees, officers, employees, contract labor, consultants, and attorneys who have a need to know.

b. The Contractor further agrees to include in all subcontracts a requirement requiring compliance by subcontractor and supplier and succeeding levels of subcontractors and suppliers with the response and access and disclosure provisions of this Enabling Requirement, subject to coordination with the Contractor, except for subcontracts for commercial items or commercial services. This agreement does not relieve the Contractor of its responsibility to manage the subcontracts effectively and efficiently nor is it intended to establish privity of contract between the Government or the Aerospace Corporation and such subcontractors or suppliers, except as indicated in paragraph (d.) below.

c. The Aerospace Corporation shall protect the proprietary information of contractors, subcontractors, and suppliers in accordance with the Master Non-disclosure Agreement The Aerospace Corporation entered into with the Air Force, a copy of which is available upon request. This Master Non-disclosure Agreement satisfies the Nondisclosure Agreement requirements set forth in 10 U.S.C. §2320 (f)(2)(B), and provides that such contractors, subcontractors, and supplier are intended third-party beneficiaries under the Master Non-disclosure Agreement and shall have the full rights to enforce the terms and conditions of the Master Non-disclosure Agreement directly against the Aerospace Corporation, as if they had been signatory party hereto. Each such contractor, subcontractor, or supplier hereby waives any requirement for the Aerospace Corporation to enter into any separate company-to-company confidentiality or other non-disclosure agreements.

d. Aerospace shall make the technical information (including proprietary information) available only to its Trustees, officers, employees, contract labor, consultants, and attorneys who have a need to know, and Aerospace shall maintain between itself and the foregoing binding agreements of general application as may be necessary to fulfill their obligations under the Master Non-disclosure Agreement referred to herein, and Aerospace agrees that it will inform contractors, subcontractors, and suppliers if it plans to use consultants, or contract labor personnel and, upon the request of such contractor, subcontractor, or supplier, to have its consultants and contract labor personnel execute non-disclosure agreements directly therewith.

e. The Aerospace Corporation personnel are not authorized to direct the Contractor in any manner. The Contractor agrees to accept technical direction as follows:

1. Technical direction under this contract will be given to the Contractor solely by SMC.

2. Whenever it becomes necessary to modify the contract and redirect the effort, a change order signed by the Contracting Officer or a Supplemental Agreement signed by both the Contracting Officer and the Contractor will be issued.

\* Cost data is defined as information associated with the programmatic elements of life cycle (concept, development, production, operations, and retirement) of the system/program. As defined, cost data differs from "financial" data, which is defined as information associated with the internal workings of a company or contractor that is not specific to a project or program.

**Section I – Contract Clauses**

**252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)** (Applicable if this purchase order/subcontract, including purchase orders/subcontracts for commercial items, is for operationally critical support or for which performance will involve covered defense information. Seller shall furnish Lockheed Martin copies of notices provided to the Contracting Officer at the time such notices are sent.)

(a) *Definitions*. As used in this clause—

“Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

“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.

“Contractor information system” means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“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 statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means 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 Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

“Operationally critical support” means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

“Rapidly report” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) *Adequate security*. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service of system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” (available via the Internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) (A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at [osd.dibcsia@mail.mil](mailto:osd.dibcsia@mail.mil), within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor’s requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(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/resources/documents/>) 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 and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) *Cyber incident reporting requirement*.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <https://dibnet.dod.mil>.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <https://dibnet.dod.mil>.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <https://public.cyber.mil/eca/>.

(d) *Malicious software*. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(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 allow DoD to request the media or 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.

(g) *Cyber incident damage assessment activities*. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) *DoD safeguarding and use of contractor attributional/proprietary information*. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) *Use and release of contractor attributional/proprietary information not 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 not created by or for DoD is authorized to be released outside of DoD—

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(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, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government’s use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) *Other safeguarding or reporting requirements*. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor’s responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) *Subcontracts*. The Contractor shall—

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to—

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

# FAR Clauses

**52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020)**

**52.203-7, Anti-Kickback Procedures (Jun 2020)**

**52.203-12, Limitation on Payments to Influence Certain Federal Transactions (Jun 2020)**

**52.203-13, Contractor Code of Business Ethics and Conduct (Jun 2020)**

**52.203-16, Preventing Personal Conflicts of Interest (Jun 2020)** (Applicable if this purchase orders/ subcontracts exceeds the simplified acquisition threshold; and in which Seller employees will perform acquisition functions closely associated with inherently governmental functions (i.e., instead of performance only by a self-employed individual).)

**52.203-17, Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Jun 2020)**

**52.204-10, Reporting Executive Compensation and First Tier Subcontract Awards (Jun 2020)**

**52.204-18, Commercial and Government Entity Code Maintenance (Aug 2020)** (Seller shall maintain their CAGE code(s) throughout the life of the purchase order/subcontract.)

**52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items "Government" in paragraph (b)means "Government or Lockheed Martin." Reports required by this clause will be made to Lockheed Martin. Paragraph (b)(2) is deleted.)

**52.209-6, Protecting the Government's Interest when Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Jun 2020)**

**52.215-2 Audit and Records -- Negotiation (Jun 2020)**

**52.215-12, Subcontractor Certified Cost or Pricing Data (DEVIATION) (May 2018)** (The version of the clause in DoD Class Deviation [2018-O0015](https://www.acq.osd.mil/dpap/policy/policyvault/USA001197-18-DPAP.pdf) applies in lieu of the standard FAR version of the clause.)

**52.215-13, Subcontractor Certified Cost or Pricing Data–Modifications (DEVIATION) (May 2018)** (The version of the clause in DoD Class Deviation [2018-O0015](https://www.acq.osd.mil/dpap/policy/policyvault/USA001197-18-DPAP.pdf) applies in lieu of the standard FAR version of the clause.)

**52.215-14, Integrity of Unit Prices (Jun 2020)**

**52.215-21, Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data – Modifications (Jun 2020)**

**52.215-23, Limitations on Pass-Through Charges (Jun 2020)**

**52.222-35, Equal Opportunity for Veterans (Jun 2020)**

**52.222-36 Equal Opportunity for Workers with Disabilities (Jun 2020)**

**52.222-37, Employment Reports on Veterans (Jun 2020)**

**52.222-50, Combating Trafficking in Persons (Jan 2019)**

**52.222-99, Establishing a Minimum Wage for Contractors (DEVIATION** [**2014-O0017**](https://www.acq.osd.mil/dpap/policy/policyvault/USA03832-14-DPAP.pdf)**) (Jun 2014)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items.)

**52.223-18, Encouraging Contractor Policies to Ban Text Messaging While Driving (Jun 2020)**

**52.227-1, Authorization and Consent (Jun 2020) and Alternate I (Apr 1984)** (Alternate I also applies.)

**52.227-2, Notice and Assistance Regarding Patent and Copyright Infringement (Jun 2020)**

**52.227-21, Technical Data Declaration, Revision, and Withholding of Payment—Major Systems (May 2014)** (Applicable if Seller will be delivering technical data. "Contracting Officer" means "Lockheed Martin." "Government" means "Lockheed Martin" in paragraph (b)(2) and "Lockheed Martin or Government" in paragraph (d).)

**52.230–2, Cost Accounting Standards (Jun 2020)**

**52.230-2, Cost Accounting Standards (DEVIATION) (May 2018)** (The version of the clause in DoD Class Deviation [2018-O0015](https://www.acq.osd.mil/dpap/policy/policyvault/USA001197-18-DPAP.pdf) applies in lieu of the standard FAR version of the clause.)

**52.232-16, Progress Payments (DEVIATION) (Mar 2020)** (The version of the clause in DoD Class Deviation [2020-O0010](https://www.acq.osd.mil/dpap/policy/policyvault/USA000801-20-DPC.pdf) applies in lieu of the standard FAR version of the clause. "Contracting Officer" means "Lockheed Martin" except in paragraph (g) where it means "Lockheed Martin or Contracting Officer." "Government" means "Lockheed Martin" except: (1) in paragraphs (d), (e) and (j)(5) where the term is unchanged and (2) in paragraphs (g) and (i) where it means "Lockheed Martin and the Government.")

**52.232-17, Interest (May 2014)** (Applicable if this purchase order/subcontract contains any clauses which refers to an Interest clause. “Government” means “Lockheed Martin.”)

**52.232-39, Unenforceability of Unauthorized Obligations (Jun 2013)** (Applicable for all purchase orders/ subcontracts where software or services will be retransferred to the Government.)

**52.243-1, Changes – Fixed Price (Aug 1987) and Alternate V (Apr 1984)** (Alternate V will also apply if this purchase order/subcontract is for research and development.)

**52.243-2, Changes – Cost Reimbursement (Aug 1987) and Alternate V (Apr 1984)** (Alternate V will also apply if this purchase order/subcontract is for research and development.)

**52.244-6, Subcontracts for Commercial Items (Aug 2020)**

**52.245-9, Use and Charges (Apr 2012)** (Applicable for all purchase orders/subcontracts where FAR 52.245-1 is inserted. Communications with the Government under this clause will be made through Lockheed Martin.)

**52.246-7, Inspection of Research and Development – Fixed Price (Aug 1996)** (Applicable if Seller has a fixed price purchase order/subcontract and will be performing research and development work. "Government" means "Lockheed Martin and the Government " in paragraphs (a), (b) and (c). "Government" means "Lockheed Martin" in paragraphs (d), (e), and (f). "Contracting Officer" means "Lockheed Martin.")

**52.246-8, Inspection of Research and Development – Cost Reimbursement (May 2001)** (Applicable if Seller has a cost reimbursable purchase order/subcontract and will be performing research and development work. "Government" means "Lockheed Martin" except (1) in paragraphs (b), (c) and (d) where it means "Lockheed Martin and the Government" and in paragraph (k) where the term is unchanged.)

**52.249-9, Default (Fixed-Price Research and Development) (Apr 1984)** (Applicable if Seller has a fixed-price purchase order/subcontract for research and development. "Government" and "Contracting Officer" mean "Lockheed Martin" except in paragraph (c) where the term "Government" is unchanged.)

# DFARS Clauses

**252.203-7003, Agency Office of the Inspector General (Aug 2019)**

**252.203-7004, Display of Fraud Hotline Poster(s) (Aug 2019)**

**252.204-7000, Disclosure of Information (Oct 2016)** (Applicable for all purchase orders/subcontracts. In paragraph (b) "Contracting Officer" means "Lockheed Martin" and "10 days" means "20 days.")

**252.204-7004, Antiterrorism Awareness Training for Contractors (Feb 2019)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items, where performance requires routine physical access to a Federally-controlled facility or military installation.)

**252.211-7007, Reporting of Government-Furnished Property (Aug 2012)** (Applicable if Seller will be in possession of Government property for the performance of this purchase order/subcontract.)

**252.219-7004, Small Business Subcontracting Plan (Test Program) (Jan 2011)** (Applicable for purchase orders/subcontracts that offer subcontracting possibilities, are expected to exceed $650,000 ($1.5 million for construction of any public facility), and are required to include the clause at 52.219-8, Utilization of Small Business Concerns.)

**252.223-7006, Prohibition on Storage, Treatment, and Disposal of Toxic or Hazardous Materials (Sep 2014)** (Applicable if this purchase order/subcontract requires or may require, or permits Seller to treat or dispose of non-DoD-owned toxic or hazardous materials as defined in the clause. "Government" means "Lockheed Martin and Government.")

**252.225-7013, Duty-Free Entry (DEVIATION) (Jul 2020)** (The version of the clause in DoD Class Deviation [2020-O0019](https://www.acq.osd.mil/dpap/policy/policyvault/USA001510-20-DPC.pdf) applies in lieu of the standard DFARS version of the clause.)

**252.225-7021, Trade Agreements (DEVIATION) (Jul 2020)** (The version of the clause in DoD Class Deviation [2020-O0019](https://www.acq.osd.mil/dpap/policy/policyvault/USA001510-20-DPC.pdf) applies in lieu of the standard DFARS version of the clause.)

**252.227-7014, Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb 2014) and Alternate I (Jun 1995)** (Alternate I also applies.)

**252.227-7038, Patent Rights--Ownership by the Contractor (Large Business) (Jun 2012) and Alternate II (Dec 2007)** (Alternate II will also apply.)

**252.235-7003, Frequency Authorization - Basic (Mar 2014) and Alternate I (Mar 2014)** (Alternate I also applies.)

**252.235-7011, Final Scientific or Technical Report (Dec 2019)** (Applicable for all purchase orders/subcontracts for research and development.)

**252.239-7000, Protection Against Compromising Emanations (Dec 2019)** (Applicable if classified work is required. "Contracting Officer" means "Lockheed Martin." "Government" means "Lockheed Martin and the Government" in paragraphs (c) and (d).)

**252.239-7001, Information Assurance Contractor Training and Certification (Jan 2008)** (Applicable if Seller will be accessing DoD Information Systems.)

**252.239-7010, Cloud Computing Services (Oct 2016)** (Applicable if this purchase order/subcontract involves use of cloud services.)

**252.243-7002, Requests for Equitable Adjustment (Dec 2012)** (Applicable for all purchase orders/subcontracts over $150,000. “Government” means “Lockheed Martin.”)

**252.245-7001, Tagging, Labeling, and Marking of Government-Furnished Property (Apr 2012)** (Applicable for purchase orders/subcontracts, including purchase orders/subcontracts for commercial items, where the items furnished by Seller will be subject to serialized tracking.)

**252.245-7004, Reporting, Reutilization, and Disposal (Dec 2017)** (Applicable for all purchase orders/ subcontracts, including purchase orders/subcontracts for commercial items, that include the clause at FAR 52.245-1, Government Property. "Contracting Officer" means “Lockheed Martin.”)

**252.246-7008, Sources of Electronic Parts (May 2018)**

**252.247-7023, Transportation of Supplies by Sea (Feb 2019)**

**252.249-7002, Notification of Anticipated Contract Termination or Reduction (Jun 2020)**

**AFFARS Clauses**

**5352.223-9000, Elimination of Use of Class I Ozone Depleting Substances (ODS) (Oct 2019)** (Applicable for all purchase orders/subcontracts. The blank in paragraph (d) is completed with "None."  In paragraph (d) "Contracting Officer" means "Lockheed Martin.")

**5352.242-9000, Contractor Access to Air Force Installations (Oct 2019)** (Applicable if Seller will be performing work on a government installation. "Contracting Officer" means "Lockheed Martin." In paragraph (e) "the prime contractor" means "Seller." The blank in paragraphs (b) and (d) is completed with "TBD.”)

**5352.242-9001, Common Access Cards (CACS) for Contractor Personnel – AF Systems (Oct 2019)** (Applicable if Seller will be performing work on a government installation. All communication with the government required by this clause shall be conducted through Lockheed Martin.)