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**

**Performance Work Statement:**

**Cooperation with Support Contractors** (Applicable to all purchase orders/subcontracts.)

2.11.1 The Air Force has entered into a contract with the following contractors for the services of a technical group, which support the Department of Defense (DoD) program office by performing Technical Review tasks: TASC (FA8807-16-C-0001), Booz Allen Hamilton (N66001-D-0106), Tecolote Research Incorporated (FA8802-13-D-0001).

2.11.2 Technical Review is 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 Air Force Manager as an independent technical assessment for his consideration for modifying the program or redirecting the contractor’s efforts to assure timely and economical accomplishment of program objectives.

2.11.3 In the performance of this contract, the contractor agrees to cooperate with the contractors identified in paragraph 2.11.1 and any subcontractors, by responding to invitations from authorized personnel to attend meetings; by providing access to technical information and research, development and 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; by delivering as specified in the Contract Data Requirements List (CDRL); by discussing technical matters relating to this program; by providing access to contractor facilities utilized in the performance of this contract; and by allowing observation of technical activities by appropriate technical support personnel. The support personnel engaged in technical review effort are authorized access to any technical information pertaining to the contract and are bound by their respective Non-Disclosure Agreements (NDAs) with the Government to protect the information they receive. Additionally, other than those data items delivered to the Government with “Unlimited Rights” as shown in Attachment 4 Data Rights of the Contract FA8823-17-C-0002, all contractors and subcontracts performing under the provisions of this clause shall not use, modify, reproduce, release, perform, display or disclose information they receive on any other program without written consent of both the contractor and SMC.

2.11.4 The contractor further agrees to include in each subcontract, if applicable, a clause requiring compliance by the subcontractor and succeeding levels of subcontractors with the response and access provision of paragraph 2.11.3 above, subject to coordination with the contractor. This agreement does not relieve the contractor of his responsibility to manage the subcontracts effectively and efficiently nor is it intended to establish privity of contract between the Government or with the contractor identified in paragraph 2.11.1 and such subcontractors.

2.11.5 The personnel of the contractors is identified in paragraph 2.11.1 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.

2.11.6 Notwithstanding language contained elsewhere in this contract, contractor and its subcontractors shall not be obligated to disclose proprietary financial information to any non-Government entities providing services to the Government during the proposal or contract execution and management phases of this activity.

**2.12 Systems Engineering and Integration Group** (Applicable to all purchase orders/subcontracts.)

2.12.1 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, which will support the DoD program office by performing General Systems Engineering and Integration (GSE&I), Technical Review, and/or Technical Support including informing the commander or director of the various 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.

2.12.2 GSE&I deals with overall system definition, 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 contractor's 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 DoD System Program Manager and 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.

2.12.3 Technical Review 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 Air Force Program Manager as an independent technical assessment for his consideration for modifying the program or redirecting the contractor’s efforts to assure timely and economical accomplishment of program objectives.

2.12.4 Technical Support 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 technical support tasks are: Selected Research, Development, Test, and Evaluation; Plans and System Architecture; Multi- Program Systems Enhancement; International Technology Assessment; and Acquisitions Support.

2.12.5 In the performance of this contract, the Contractor agrees to cooperate with The Aerospace Corporation by responding to invitations from authorized U.S. Government personnel to attend meetings; 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 specification; test and test equipment specification and procedures, parts and quality control procedures, records and data; and schedule and milestone data; all in their original form or reproduced form and including top-level life cycle cost data, where available\*; by delivering data as specified in the Contract Data Requirements List; where available; by discussing technical matters relating to this program; by providing access to contractor facilities utilized in the performance of this contract; and by allowing observation of technical activities by appropriate Aerospace technical personnel. The Aerospace personnel engaged in general systems engineering and integration, Technical Review, and/or Technical Support 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.

\*Cost data is defined as information associated with the programmatic elements or 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.

2.12.6 The contractor further agrees to include in each subcontract a clause requiring compliance by the subcontractor and supplier and succeeding levels of subcontractors and suppliers with the response and access and disclosure provision of paragraph 2.12.5 above, subject to coordination with the contractor, except for subcontractors for commercial item 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 supplies, except as indicated in paragraph 2.12.7 below.

2.12.7 The Aerospace Corporation shall protect the proprietary information of contractors, subcontractors, and suppliers in accordance with the Master NDA The Aerospace Corporation entered into with the Air Force, a copy which is available upon request. This Master NDA satisfies the NDA requirements set forth in 10 U.S.C 2320 (f)(2)(B) and provides that such contractors, subcontractors, and suppliers are intended third-party beneficiaries under the Master NDA and shall have the full rights to enforce the terms and conditions of the Master NDA 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 NDAs.

2.12.8 The Aerospace Corporation 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 NDA 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 NDAs directly therewith.

2.12.9 The Aerospace Corporation 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.

**DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information (Oct 2016)** (Applicable if this purchase order/subcontract involves services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting.)

(a) Definitions. As used in this clause—

“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.

“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 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.

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

"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.

"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) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party’s reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government’s activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government’s activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

**DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)** (Applicable if this purchase order/subcontract is for operationally critical support or for which purchase order/subcontract 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 this 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-Non Commercial 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 or 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, 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, the Contractor and identified in the contract 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 <http://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 http://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 <http://iase.disa.mil/pki/eca/Pages/index.aspx>.

(d) Malicious software. The Contractor or subcontractors that 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 a 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

**52.203-7, Anti-Kickback Procedures (May 2014)**

**52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2016)**

**52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)** (Applicable to all purchase orders/subcontracts, unless the Seller is furnishing commercially available off-the-shelf items, in which the Seller may have Federal contract information residing in or transiting through its information system.)

**52.215-2, Audit and Records -- Negotiation (Oct 2010) and Alternate II (Aug 2016)** (Alternate II will also apply to cost reimbursement purchase orders/subcontracts if the Seller is an educational institution, state or local government or non-profit institution.)

**52.215-21, Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data - Modifications (Oct 2010) and Alternate I (Oct 2010)** (Alternate I will also apply.)

**52.216-16 Incentive Price Revision – Firm Target (Oct 1997)** (Applicable if this purchase order/ subcontract is a fixed price incentive contract. "Contracting Officer", "contract administrative office" and "Government" mean "Lockheed Martin." Paragraph (i) is deleted. The blanks in the clause are completed with the amounts specified in the contract.)

**52.219-8, Utilization of Small Business Concerns (Nov 2016)**

**52.222-26, Equal Opportunity (Sep 2016)**

**52.222-37, Employment Reports on Veterans (Feb 2016)**

**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).)

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

**52.239-1, Privacy or Security Safeguards (Aug 1996)** (Applicable if this purchase order/subcontract is for information technology, and/or for the design development, or operation of a system of records using commercial information technology services or support services.)

**52.243-2, Changes—Cost-Reimbursement (Aug 1987) and Alternate I (Apr 1984)** (Alternate I will also apply if this purchase order/subcontract is cost reimbursement and is for services and no supplies are to be furnished.)

**52.244-6, Subcontracts for Commercial Items (Nov 2017)**

**52.245-1, Government Property (Jan 2017)**

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

# DFARS Clauses

**252.203-7004, Display of Fraud Hotline Poster(s) (Oct 2016)**

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

**252.204-7015, Notification of Authorized Disclosure of Information to Litigation Support Contractors (May 2016)**

**252.211-7003, Item Unique Identification and Valuation (Mar 2016)**

**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.)

**252.211-7008, Use of Government-Assigned Serial Numbers (Sep 2010)** (Applicable to all purchase orders/subcontracts where the seller will be in the possession of Government property for the performance of the purchase order/subcontract. If Lockheed Martin will assume responsibility for marking the property, the clause may be excluded from the purchase order/subcontract.)

**252.219-7004, Small Business Subcontracting Plan (Test Program) (Oct 2014)** (Applicable if Seller participates in the DoD test program described in DFARS 219.702.)

**252.223-7006,** **Prohibition on Storage and Disposal of Toxic and Hazardous Materials (Sep 2014) and Alternate I (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." Alternate I will also apply.)

**252.225-7001, Buy American and Balance of Payments Program--Basic (Dec 2017) and Alternate I (Dec 2017)** (Alternate I will also apply.)

**252.225-7012, Preference for Certain Domestic Commodities (Dec 2017)**

**252.225-7013, Duty-Free Entry (May 2016)**

**252.225-7021, Trade Agreements (Dec 2017)**

**252.227-7019, Validation of Asserted Restrictions--Computer Software (Sep 2016)**

**252.227-7037, Validation of Restrictive Markings on Technical Data (Sep 2016)**

**252.237-7010, Prohibition on Interrogation of Detainees by Contractor Personnel (Jun 2013)** (Applicable to all purchase orders/subcontracts that may require subcontractor personnel to interact with detainees in the course of their duties.)

**252.237-7023, Continuation of Essential Contractor Services (Oct 2010)** (Applicable to all purchase orders/subcontracts for mission essential services. "Contracting Officer" means “Lockheed Martin.” The term "Government" includes Lockheed Martin.)

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

**252.243-7002, Requests for Equitable Adjustment (Dec 2012)** (Applicable to 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 where the items furnished by you will be subject to serialized tracking.)

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

**252.246-7000, Material Inspection and Receiving Report (Mar 2008)** (Applicable if direct shipments will be made to the Government.)

**252.246-7001, Warranty of Data (Mar 2014)** (Applicable if you will be delivering data. "Government" means "Lockheed Martin or the Government." "Contracting Officer" means "Lockheed Martin." The last sentence in paragraph (b) is changed to read as follows: The warranty period shall extend for three years after completion of delivery of the data to Lockheed Martin, or if the data is delivered to the Government, either by Lockheed Martin or Seller, the warranty period shall extend for three years after delivery to the Government.")

**252.246-7001, Warranty of Data (Mar 2014) and Alternate I (Mar 2014)** (Alternate I will also apply if this is a fixed-price-incentive purchase order/subcontract.)

**252.246-7001, Warranty of Data (Mar 2014) and Alternate II (Mar 2014)** (Alternate II will also apply if this is a fixed-price purchase order/subcontract.)

**252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System (Aug 2016)**

**252.246-7008, Sources of Electronic Parts (Dec 2017)** (Applicable if this purchase order/ subcontract is for electronic parts or assemblies containing electronic parts, unless Seller is the original manufacturer. As used in the clause, "Contracting Officer" means "Lockheed Martin and the Contracting Officer. "The term "Government" means "Lockheed Martin and the Government" except in paragraph (d).)

**AFFARS Clauses**

**5352.223-9000, Elimination of Use of Class I Ozone Depleting Substances (ODS) (Nov 2012)** (Applicable for all purchase orders/subcontracts.)

**5352.242-9000, Contractor Access to Air Force Installations (Nov 2012)** (Applicable if Seller will be performing work on a government installation. "Contracting Officer" means "Lockheed Martin." In paragraph (e) "the prime contractor" means "Seller.")

**5352.242-9001, Common Access Cards (CACS) for Contractor Personnel – AF Systems (Nov 2012)** (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.)