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.

**Section H –  Special Contract Requirements**

**SMC H001 CONTRACTOR CYBERSECURITY REQUIREMENTS (MAY 2019)** (Applicable if for all purchase orders/subcontracts for which the Seller has Covered Contractor Locations, without alteration except to identify the parties and to properly flow the requirements in the CDRLs A021- A025 to Sellers, except as provided in subsection (k), Waiver.)

(a) ***Purpose***. The purpose of this clause is to:

(1) Require the Contractor and all of its subcontractors to implement cybersecurity hygiene practices throughout their respective supply chains; and

(2) Provide the Government visibility into the effectiveness of those implemented practices in protecting the unauthorized exfiltration and use of Controlled Technical Information (CTI) residing within a covered contractor or subcontractor’s information system.

(b) ***Definitions***. As used in this clause-

“Adversary Emulation Testing” means testing of a network or information system using threat- representative cyber exploitation techniques to identify security vulnerabilities and the effectiveness of defensive capabilities. Adversary emulation testing evaluates the ability of the system, tiered defenses, and defenders to protect critical functions; to detect and respond to cyber attack; and to survive and recover from cyber attack. Testing also examines relevant insider and outsider threat postures.

“Controlled Technical Information” (CTI) as defined in DFARS 252.2047012.

“Covered Contractor Information System” as defined in DFARS 252.2047012.

“Covered Contractor Location” means a Contractor facility that is owned or operated by or for the Contractor where Controlled Technical Information relevant to this Contract on a Covered Contractor Information System is processed, stored, or transmitted.

“Data Loss Detection” (DLD) are techniques that provide an ability to the Contractor to forensically locate and positively identify program information if it is stolen.

“Illicit Activity Alerts” (IAA) are ways to configure computer systems to provide indication and warning to the Contactor’s network owners in advance of attempted data theft to assist in stopping the threat prior to losing key information.

“Routine” means no more often than one annual occurrence of the activity described, not including follow-on occurrences to assess any required remediations. Follow-on occurrence may occur more than once annually.

“Trusted Agent” means a Contractor employee with system, technical, managerial, or other knowledge relevant to the security and design of a network or information system who assists an assessor to perform testing on the network or information system.

(c) ***CTI Identification***. Within 60 calendar days after Contract award, the Contractor shall identify the technologies being developed or used on this Contract that would result in the creation or use of CTI. Additionally, the Contractor shall identify the types of documents (e.g., PowerPoint, CAD drawings, excel) within which the technologies are memorialized physically, electronically, graphically, photographically, or in writing. (CDRL A021 Information Management Control Plan (IMCP), Part A & CDRL A022 Information Management Control Plan (IMCP) Part B). In accordance with DFARS 252.204-7012(a), the Government will mark or otherwise identify any covered defense information (as that term is defined in that clause) it will provide to the Contractor in support of the performance of this Contract.

(d) ***Information Management Control Plan (IMCP)***.

(1) IMCP Part A. The Contractor shall develop and provide an IMCP Part A. The Contractor shall deliver the IMCP Part A to the Government POC identified in subsection (l), Contact Information, and each of its subcontractors shall deliver the IMCP Part A only to the next higher tier subcontractor (or if the subcontractor is a first-tier subcontractor, only to the Contractor). (CDRL A021 Information Management Control Plan (IMCP), Part A).

(2) IMCP Part B, Supplier Compliance Supplement. If the Contractor has subcontractors that receive or generate CTI in performance of this Contract, the Contractor shall ensure those subcontractors submit an IMCP Part B, Supplier Compliance Supplement, directly to the Government POC identified in subsection (l), Contact Information, within 60 calendar days after award of the subcontract (CDRL A022).

(3) The Government reserves the right to review and inspect the IMCPs to verify implementation of the IMCP and DFARS 252.204-7012. Further, the Government reserves the right to use the IMCPs to iteratively navigate through the tiered supply chain to accomplish the activities as enumerated in this clause. The Contractor will only have visibility to their next lower- tier subcontractor IMCP(s) Part A.

(e) ***Compliance Auditing***. The Contractor shall assist the Government during routine onsite compliance audits conducted by Defense Contracting Management Agency (DCMA) or by a third-party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) at Government-selected Covered Contractor Locations to ensure compliance with DFARS 252.204-7012 and the Contractor’s System Security Plan (including all relevant Plan of Actions and Milestones (POAMs)). Prior to any such audit, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5. The Government will provide written notification at least 30 calendar days prior to performing a routine audit.

(f) ***Adversary Emulation Testing***.

(1) The Contractor, at its sole discretion and option, shall choose one of the three options below:

(i) Conduct at a regular interval, based on the Contractor’s risk-based determination, adversary emulation testing on Covered Contractor Information Systems, or a subset thereof, as mutually agreed to between the Contracting Officer and Contractor. The Contractor shall provide the Contracting Officer or Government Point of Contact (POC) identified in subsection (l) 30 calendar day notice of planned adversary emulation testing. The Contractor shall provide the opportunity for the Government or a third party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) to observe the testing, review the results, and verify the level of testing meets the criteria outlined in CDRL A023, Adversary Emulation Testing, derived from the National Institute of Standards and Technology Special Publication (NIST SP) 800-115, Section 5.2 Penetration Testing. The Contractor shall use the MITRE ATT&CK Framework and the current Open Web Application Security Project (OWASP) Top Ten vulnerabilities as published at the time of Contract award when planning its Adversary Emulation Testing, which will be verified in CDRL A023. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5.

Or,

(A) The Contractor shall deliver the Adversary Emulation Testing process documentation outlined in CDRL A023, Adversary Emulation Testing, to the Government, and each of its subcontractors shall, deliver CDRL A023 to the Government POC identified in subsection (l), Contact Information.

(ii) Permit the Government to, and assist the Government in, performing routine Adversary Emulation Testing conducted by a third-party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) on Government- selected Covered Contractor Information Systems. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5. Prior to conducting the Adversary Emulation Testing, the Government-selected assessor shall initiate a Collaborative Onsite Security Assessment (COSA). The Contractor shall mutually agree to a COSA with the Government. The COSA agreement shall address:

(A) Any Adversary Emulation Testing in-process or those already conducted on the selected Covered Contractor Information Systems;

(B) Rules of engagement;

(C) Roles and responsibilities of the parties;

(D) Pre-assessment activities;

(E) Scope of the assessment;

(F) Assessment methodology;

(G) Assessment tools used;

(H) Frequency of assessment;

(I) Confidentiality and handling of data;

(J) Schedule;

(K) Cost Implications; and

(L) Post assessment obligations of the parties.

For the routine Adversary Emulation Testing, the Contractor shall provide at least one trusted agent. The Government assessor will coordinate activities and results relating to routine Adversary Emulation Testing with the trusted agent(s).

Or,

(iii) Subcontract with a third party, approved by the Government (approval shall not be unreasonably withheld), that is capable of Adversary Emulation Testing and verify this third party is capable of Adversary Emulation Testing by delivering directly to the Government POC identified in subsection (l), Contact Information, the Adversary Emulation Testing Process (CDRL A023). If the Contractor elects to subcontract with a third party to perform Adversary Emulation Testing, they shall provide the Contracting Officer or Government Point of Contact (POC) identified in subsection (l) 30 calendar day notice of planned adversary emulation testing. The Contractor shall provide the opportunity for the Government or a third party firm that satisfies the definition of a Covered Government Support Contractor in DFARS 252.227-7013(a)(5) and DFARS 252.227-7014(a)(6)) to observe the testing, review the results, and verify the level of testing meets the criteria outlined in CDRL A023, Adversary Emulation Testing, derived from the National Institute of Standards and Technology Special Publication (NIST SP) 800-115, Section 5.2 Penetration Testing. Prior to any such testing, the Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest as set forth in FAR Part 9.5.

(2) The Contractor shall, at its sole discretion with the exception of high level criticality findings, disposition security-related findings from adversary emulation testing on a risk-based determination. If the Contractor determines disposition is required, the Contractor shall determine the manner of disposition. The Contractor shall mitigate high level criticality findings or work with the Government Point of Contact (POC) identified in subsection (l) to come to an agreement for a mitigation approach.

(g) ***Perimeter Threat Detection Augmentation***.

(1) The Contractor, at its sole discretion and option, shall choose one of the three options below:

(i) Verify they are capable of Perimeter Threat Detection by delivering directly to the Government the Perimeter Threat Detection Process Part A (CDRL A024). If the Contractor elects to do the above, they shall assist the Government in auditing against the above documentation in conjunction with the activities described in subsection (e). The Contractor shall deliver CDRL A024 to the Government POC identified in subsection (l), Contact Information, and each of its subcontractors shall deliver the CDRL A024 to the Government POC identified in subsection (l) Contact Information.

Or,

(ii) Provide the information requested in Perimeter Threat Detection Process Part B (CDRL A025) for the Government to provide threat detection augmentation on the forward facing IP space and domains of networks. CDRL A025 shall be delivered to the Government, and each of Contractor’s subcontractors shall deliver CDRL A025 to the Government.

Or,

(iii) Subcontract with a third party, approved by the Government (approval shall not be unreasonably withheld), that is capable of Perimeter Threat Detection and verify this third party is capable of Perimeter Threat Detection by delivering directly to the Government POC identified in subsection (l), Contact Information, the Perimeter Threat Detection Process Part A(CDRL A024). CDRL A024 shall be delivered to the Government, and each of Contractor’s subcontractors shall deliver CDRL A024 to the Government. If the Contractor elects to subcontract with a third party to perform Perimeter Threat Detection, they shall assist the Government in auditing against the documentation in conjunction with the activities described in subsection (e).

(h) ***Illicit Data Loss Exploitation (IDLE)***.

(1) Upon written direction from the Contracting Officer, the Contractor shall follow the process identified in the IDLE Procedures.

(2) Upon receipt of the above written direction, and at any time thereafter during the period of performance of this contract, the Contracting Officer may direct the Contractor to perform IDLE efforts via CLIN 0003, IDLE Efforts.

(3) IDLE

(i) The Government shall issue a task statement to the Contractor for each IDLE effort. Upon receipt, the Contractor shall submit to the Government an estimate which shall include, at a minimum, a description of the effort, the number of hours required for completion broken out by skill mix, the total estimated cost, Government Fiscal Year (GFY) and Contractor Accounting Year (CY), and a period of performance.

(ii) Each effort performed in accordance with this clause shall be directed by the Contracting Officer via unilateral modification to the contract. IDLE efforts shall be incorporated into Attachment 14, “Illicit Data Loss Exploitation Efforts." Such modification shall:

(A) Provide specific direction as to effort to be accomplished;

(B) Establish a period of performance for the effort;

(C) Establish the maximum number of hours; and

(D) Establish the estimated cost.

(iii) In no event shall the Contractor exceed the established hours, total estimated cost, or period of performance authorized in each individual modification without written approval from the Contracting Officer.

(iv) The Contractor shall segregate all costs associated with CLIN 0003, IDLE Efforts, from the costs associated with all other CLINs. The Contractor shall segregate the costs for each IDLE effort from the costs of every other IDLE effort.

(v) The table below states the total hours available, the total hours used, and the composite hourly rate for each GFY.

(i) In accordance with FAR 16.306, the IDLE scope will be performed on a level of effort basis within the time periods specified and is a CPFF term form. The below stated hours designate the available hours Contractor may expend on a level of effort basis as unilaterally required by the Government for the time period specified.

|  |  |  |  |
| --- | --- | --- | --- |
| **IDLE Effort** | **FY21** | **FY22** | **TOTAL** |
| **Total Hours Available** | 750 | 750 | 1,500 |
| Total Systems Administrator Hours Available | 630 | 630 | 1,260 |
| Total Systems Engineer Hours Available | 120 | 120 | 240 |
| **Total Hours Used** | 0 | 0 | 0 |
| Total Systems Administrator Hours Used | 0 | 0 | 0 |
| Total Systems Engineer Hours Used | 0 | 0 | 0 |
| **Systems Administrator Composite Hourly Rate** |  | N/A |  |
| **Systems Engineer Composite Hourly Rate** |  |  | N/A |

(j) ***Subcontractors***. The Contractor shall include this H001 clause, including this subsection (j), in all subcontracts, or similar contractual instruments, for which the subcontractor has Covered Contractor Locations, without alteration except to identify the parties and to properly flow the requirements in the CDRLs A021- A025 to subcontractors, except as provided in subsection (k), Waiver.

(k) ***Waiver***. The Contractor may submit in writing to the Contracting Officer a request to waive, in part, the requirements of subsections (e) through (h) of this clause accompanied by a detailed rationale for the request.

(1) The Contractor, and if necessary any lower tier subs in the requisite chain, shall flow this H001 clause in its entirety to the following subcontractors:

1. Northrop Grumman / Ball Aerospace

2. Raytheon

3. SEAKR

For all other subcontractors, the Government hereby waives the requirement to flow down subsections (e) through (h) of this H001 clause. This waiver list will be reviewed annually by the Contractor and Government PCO. The Contractor shall submit a list of new 1st tier subcontractors 30 calendar days prior to the annual review. At its discretion, the Government may unilaterally direct the flow of the entirety of this clause to any specific subcontractor subject to equitable relief within the requisite chain.

(l) ***Contact Information***. For questions on this clause or to notify the Government as directed by the subsections above, contact directly the following organization inbox: [SMC.RS.OPIR@us.af.mil<mailto:SMC.RS.OPIR@us.af.mil](mailto:SMC.RS.OPIR@us.af.mil%3cmailto:SMC.RS.OPIR@us.af.mil)>.

(m) ***Nondisclosure agreements (NDA)***. If the Government-selected third-party firm is a Covered Government Support contractor, that firm will sign a nondisclosure agreement with the Contractor prior to starting work under this H001 clause. Any such Government-selected third-party firm shall not be a competitor of the Contractor and shall not create a conflict of interest as set forth in FAR Part 9.5. The Government and the Contractor will work jointly to avoid or mitigate any conflicts of interest or potential conflicts of interest that arise. The nondisclosure agreement will describe the conditions under which the Contractor will agree to furnish the Covered Government Support Contractor access and proprietary data prior to, during, or subsequent to the Covered Government Support Contractor conducting routine onsite compliance audits (per (e)) or routine Adversary Emulation Testing (per (f)(1)(i) or (f)(1)(ii)). No NDA shall prohibit the Government-selected third-party firm from disclosing relevant information to the Government.

(n) RESERVED.

(o) ***Other compliances***. The Contractor shall not be required to perform any requirement of this clause that violates applicable U.S. federal, state, or non- U.S. laws or regulations unless an exception to those laws or regulations applies due to the use of log-on consent banners.

(p) ***Duration***. The rights and obligations of the parties under this clause shall end upon the period of performance defined in the prime contract.

(q) ***CDRLs***. All CDRLs delivered under this H001 clause do not contain technical data, computer software, or computer software documentation and are data incidental to contract administration, such as management information. All CDRLs will be marked as Contractor’s proprietary or confidential information.

**H003 CROSS-UTILIZATION OF GOVERNMENT PROPERTY (GP) AMONG CONTRACTS (Oct. 2020)** (Applicable if the purchase order/subcontract includes the use of Government-owned property.)

(a) *Definitions*. Definitions applicable to this contract are provided in the clause at FAR 52.245-1, Government Property and FAR 52.245-9, Use and Charges. Additional Definitions as used in this clause include:

“Cross Utilization” means sharing GP on a rent-free non-interference basis between authorized contracts.

“Transfer” means the reassignment of overall management and accountability responsibilities from one contract to another.

(b) *Cross Utilization of Government Property*. This clause does not take precedence over FAR 52.245-9, Use and Charges, except to the extent this clause provides the authorizations required in FAR 52.245-9(b). In accordance with FAR 52.245-9 (b), the Contracting Officer authorizes the Contractor to provide, on a rent-free non-interference basis, GP accountable to this contract to the following contracts:

* SBIRS GEO 5-6 Production FA8810-13-C-0001
* SBIRS EMD F04701-95-C-0017
* SBIRS SFP FA8810-08-C-0002
* SBIRS CLS/S2E2 FA8810-13-C-0002
* AEHF SV1-4 and SV5/6 LL F04701-02-C-0002
* AEHF SV5/6 Production FA8808-12-C-0010
* COOLS FA8823-15-C-0001
* GPS III FA8807-08-C-0010
* GPS III Follow-On FA8807-18-C-0009

(c) *Reciprocal Provisions*. Cross utilization of GP accountable to the listed contracts in support of this contract requires a similar clause in the listed contracts before any RFNI use of GP accountable to the listed contracts is permitted under this clause.

(d) *Additional Rules*. The Contractor will comply with the following rules when cross utilizing GP amongst the contracts listed above:

(1) The Contractor shall comply with the management and accountability requirements set forth in FAR 52.245-1, Government Property.

(2) In the event of a usage conflict, the accountable contract maintains the right to use the GP.

(3) Since scheduling the cross utilization of GP accountable to the above listed contracts is controlled by the Contractor, no claim for late delivery or unavailability will be recognized by the Government as described under

FAR 52.245-1(d).

(e) Exceptions. The Contractor shall not cross utilize Controlled Cryptographic Items (CCI) (COMSEC or TRANSEC) or restricted rights software to support other contracts.

(f) *General*.

(1) This clause only gives the Contractor the authority to cross utilize GP amongst the listed contracts. This clause does not give the Contractor the authority to transfer GP to any contract (including those listed) without Government approval.

(2) The Government may revoke authorization provided under this clause upon 30 days written notice and require the Contractor to follow the formal process outlined in FAR 52.245-9, Use and Charges, when requesting to cross utilize Government property.

**Section I – Contract Clauses**

**252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)** (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, 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 con tractor’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 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*. 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.

**252.234-7002, Earned Value Management System (DEVIATION) (Sep 2015)** (The version of the clause in DoD Class Deviation [2015-O0017](https://cyberguide.global.lmco.com/source-dod-cd-2015-o0017.pdf) applies in lieu of the standard DFARS version of the clause. Applicable if Seller is listed in paragraph (k) of this clause in the prime contract. "Government" means "Lockheed Martin and Government." Paragraphs (i) and (j) are deleted.)

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

“Acceptable earned value management system” means an earned value management system that generally complies with system criteria in paragraph (b) of this clause.

“Earned value management system” means an earned value management system that complies with the earned value management system guidelines in the ANSI/EIA-748.

“Significant deficiency” means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b) *System criteria*. In the performance of this contract, the Contractor shall use-

(1) An Earned Value Management System (EVMS) that complies with the EVMS guidelines in the American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748); and

(2) Management procedures that provide for generation of timely, reliable, and verifiable information for the Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) required by the CPR and IMS data items of this contract.

(c) If this contract has a value of $100 million or more, the Contractor shall use an EVMS that has been determined to be acceptable by the Cognizant Federal Agency (CFA). If, at the time of award, the Contractor’s EVMS has not been determined by the CFA to be in compliance with the EVMS guidelines as stated in paragraph (b)(1) of this clause, the Contractor shall apply its current system to the contract and shall take necessary actions to meet the milestones in the Contractor’s EVMS plan.

(d) If this contract has a value of less than $100 million, the Government will not make a formal determination that the Contractor’s EVMS complies with the EVMS guidelines in ANSI/EIA-748 with respect to the contract. The use of the Contractor’s EVMS for this contract does not imply a Government determination of the Contractor’s compliance with the EVMS guidelines in ANSI/EIA-748 for application to future contracts. The Government will allow the use of a Contractor’s EVMS that has been formally reviewed and determined by the CFA to be in compliance with the EVMS guidelines in ANSI/EIA-748.

The Contractor shall submit notification of any proposed substantive changes to the EVMS procedures and the impact of those changes to the CFA. If this contract has a value of $100 million or more, unless a waiver is granted by the CFA, any EVMS changes proposed by the Contractor require approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes as soon as practicable (generally within 30 calendar days) after receipt of the Contractor’s notice of proposed changes. If the CFA waives the advance approval requirements, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(e) The Government will schedule integrated baseline reviews as early as practicable, and the review process will be conducted not later than 180 calendar days after-

(1) Contract award;

(2) The exercise of significant contract options; and

(3) The incorporation of major modifications.

(4) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer’s final determination concerning-

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action;

(iii) System noncompliance, when the Contractor’s existing EVMS fails to comply with the earned value management system guidelines in the ANSI/EIA-748; and

(iv) System disapproval, if initial EVMS validation is not successfully completed within the timeframe approved by the Contracting Officer, or if the Contracting Officer determines that the Contractor's earned value management system contains one or more significant deficiencies in high-risk guidelines in ANSI/EIA-748 standards (guidelines 1, 3, 6, 7, 8, 9, 10, 12, 16, 21, 23, 26, 27, 28, 30, or 32). When the Contracting Officer determines that the existing earned value management system contains one or more significant deficiencies in one or more of the remaining 16 guidelines in ANSI/EIA-748 standards, the Contracting Officer will use discretion to disapprove the system based on input received from functional specialists and the auditor.

(5) If the Contractor receives the Contracting Officer’s final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the significant deficiencies.

(f) *Withholding payments*. If the Contracting Officer makes a final determination to disapprove the Contractor’s EVMS, and the contract includes the clause at 252.242-7005 <http://www.acq.osd.mil/dpap/dars/dfars/html/current/252242.html>, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(g) With the exception of paragraphs (i) and (j) of this clause, the Contractor shall require its subcontractors to comply with EVMS requirements as follows:

(1) For subcontracts valued at $100 million or more, the following subcontractors shall comply with the requirements of this clause: Selected two (2) separate Mission Payload vendors.

(2) For subcontracts valued at less than $100 million, the following subcontractors shall comply with the requirements of this clause, excluding the requirements of paragraph (c) of this clause: Selected two (2) separate Mission Payload vendors.

**Enabling Requirements for Government Program Contracts Requiring Interface with Aerospace FFRDC Contract Support** (Applicable for all purchase orders/subcontracts.)

1. This contract covers part of a 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.

a. General Systems Engineering and Integration (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 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.

b. 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.

c. 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.

2. 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 delivering data as specified in the Contract Data Requirements List; 4) by discussing technical matters relating to this program; 5) by providing access to Contractor facilities utilized in the performance of this contract; 6) 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.

3. The Contractor further agrees to include in all subcontracts a contract 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 Clause, 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.

4. The Aerospace Corporation shall protect the proprietary information of Contractors, subcontractors, and suppliers IAW 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 suppliers 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.

5. 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 Nondisclosure 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.

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

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

b. 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.

**Enabling Requirements for Prime Contractors and Service Contractors** (Applicable for all purchase orders/ subcontracts over $1 million or 10 percent of prime contract value, whichever is less.)

1. The Air Force has entered into contracts for services to provide technical, evaluation, financial, and acquisition management support. Service tasks involve the application of a broad range of education, skills, knowledge, and experience in many disciplines in support of weapon system acquisition tasks. Tasks involve specialty engineering, engineering support, configuration control management, systems engineering process, requirements compliance, architecture development, horizontal integration and communication across the program, training,

repository for program office data, and business operations support to include acquisition and financial management activities. Service contracts contain an organizational conflict of interest clause that requires the service Contractors to protect the data and prohibits the service Contractors from using the data for any purpose other than that for which the data was presented. Service Contractor personnel are not authorized to direct a Contractor in any manner.

2. In the performance of this contract, the Contractor shall cooperate with SMC/RS Support Contractors and non-Aerospace FFRDC by: responding to invitations from authorized personnel to attend meetings; providing access to technical information and research, development and planning data, test data and results, schedule and milestone data, financial data including the Contractor's cost/schedule management system/records and accounting system, all in original form or reproduced; discussing technical matters related to the program;

providing access to Contractor facilities utilized in the performance of this contract; and allowing observation of technical activities by appropriate support Contractor technical personnel.

3. The Contractor shall include in each of their subcontracts over $1 million or 10 percent of prime contract value, whichever is less, a clause requiring compliance by a subcontractor and succeeding lower levels of subcontractors with the response and access provisions of paragraph (b) above, subject to coordination with the Contractor. This agreement does not relieve the Contractor of responsibility to manage subcontracts effectively and efficiently, nor is it intended to establish privity of contracts between the Government or the service Contractor(s) and such subcontractors.

4. Neither the Contractor nor their subcontractors shall be required to perform any effort or supply any documentation not otherwise required by their contract or subcontract.

**Impact of Industry Parts Notification/Alerts** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items. Communications with the Government under this clause will be made through Lockheed Martin.)

The Contractor shall identify and assess Industry parts notifications and alerts. Industry parts notifications and alerts include, but are not limited to, Government Industry Data Exchange Program (GIDEP), Space Quality Improvement Council (SQIC), DOD Alerts, or Contractor internal alerts. The Contractor shall notify the Government upon disposition of GIDEP alert that affects this program to include lower-tier Subcontractors and vendor parts.

# FAR Clauses

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

**52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Oct 2018)**

**52.215-12, Subcontractor Certified Cost or Pricing Data (DEVIATION) (May 2018)** (The version of the clause in 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 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.)

**52.219-9, Business Subcontracting Plan (Jan 2017)**

**52.222-54 EMPLOYMENT ELIGIBILITY VERIFICATION (OCT 2015)**

This clause applies in lieu of 52.222-54 (Nov 2021)

**52.222-99, Establishing a Minimum Wage for Contractors (DEVIATION** [**2014-O0017**](https://cyberguide.global.lmco.com/source-dod-cd-2014-o0017.pdf)**) (Jun 2014)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items.)

**52.223-15, Energy Efficiency in Energy – Consuming Products (Dec 2007)** (Applicable if Seller will be delivering energy consuming products to the Government, acquired by the Contractor for use in performing services at a Federally-controlled facility; furnished under the prime contract for use by the Government; or specified in the design of a building or work, or incorporated during its construction, renovation, or maintenance.)

**52.225-3, Buy American -- Free Trade Agreements -- Israeli Trade Act (May 2014)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items, that exceed $25,000.)

**52.227-1, Authorization and Consent (Dec 2007) and Alternate I (Apr 1984)** (Alternate I also applies.)

**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 (DEVIATION) (May 2018)** (The version of the clause in 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.)

**52.232-17, 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, including purchase orders/subcontracts for commercial items, where software or services will be retransferred to the Government.)

**52.237-11, Accepting and Dispensing of $1 Coin (Sep 2008)** (Applicable if this purchase order/subcontract, including purchase orders/subcontracts for commercial items, involves services that involve business operations conducted in U.S. coins and currency, including vending machines, on any premises owned by the United States or under the control of any agency or instrumentality of the United States.)

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

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

# DFARS Clauses

**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.")

**252.204-7008, Compliance With Safeguarding Covered Defense Information Controls (Oct 2016)** (This clause is only applicable to solicitations for POs/subcontracts, including purchase orders/subcontracts for commercial items.)

**252.209-7010, Critical Safety Items (Aug 2011)** (Applicable when this purchase order/subcontract, including purchase orders/subcontracts for commercial items, includes one or more items designated by the design control activity as critical safety items.)

**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, including purchase orders/subcontracts for commercial items.)

**252.215-7000, Pricing Adjustments (Dec 2012)** (Applicable if the FAR clause entitled "Subcontractor Certified Cost or Pricing Data" or "Subcontractor Certified Cost or Pricing Data - Modifications" apply to this purchase order/ subcontract.)

**252.216-7009, Allowability of Legal Costs Incurred in Connection With a Whistleblower Proceeding (Sep 2013)** (Does not apply to fixed price purchase orders/subcontracts.)

**252.219-7004, Small Business Subcontracting Plan (Test Program) (May 2019)** (Applicable if Seller participates in the DoD test program described in DFARS 219.702-70.)

**252.225-7009, Restriction on Acquisition of Certain Articles Containing Specialty Metals (Oct 2014)**

**252.225-7013 DUTY-FREE ENTRY (DEVIATION 2020-O0019) (JUL 2020)**

**252.225-7047 Exports by Approved Community Members in Performance of the Contract (June 2013)** (Applicable for all purchase orders/subcontracts, including purchase orders/subcontracts for commercial items, that may require exports or transfers of qualifying defense articles in connection with deliveries under the contract. Insert “N/A” in the blank in paragraph (b).)

**252.226-7001, Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns (Sep 2004)**

**252.234-7004, Cost and Software Data Reporting System--Basic (Nov 2014)** (Applicable if this purchase order/subcontract is in excess of $50,000,000. In paragraph (b), "Government" means “Lockheed Martin.”)

**252.239-7000, Protection Against Compromising Emanations (****Oct 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.)

**252.243-7002, 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, containing the clause at 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.)

**AFFARS Clauses**

**5352.223-9000, Elimination of Use of Class I Ozone Depleting Substances (ODS) (Nov 2012)** (Applicable for all purchase orders/subcontracts. The blank in paragraph (d) is completed with "None."  In paragraph (d) "Contracting Officer" means "Lockheed Martin.")