**3275 (5/24/22)**

The following additional clauses apply to this Contract. If any of the clauses are expressly made inapplicable by a threshold amount or other limitation, they shall be self-deleting.

ARTICLE I: DATA RIGHTS AND COPYRIGHTS

Technical Data and Computer Software Rights under this Contract shall be determined in accordance with DFARS 252.227-7013 (Rights in Technical Data—Noncommercial Items (Feb 2014)) and DFARS 252.227-7014 (Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb 2014)), except as otherwise specified herein. The definitions included in this Article shall replace the definitions found in the referenced DFARS clauses.

A. Definitions

“Government” refers to the government of the United States.

“Government Purpose” means any activity in which the Government is a party. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so.

“Government Purpose Rights” means the right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and to release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for Government purposes. This is a middle path unique to defense contracts that allows contractors to have the exclusive right to use the technical data in the commercial market. Unless otherwise agreed, Government Purpose Rights convert to Unlimited Rights five years after execution of the Project.

“Limited Rights” means the right to use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government. The Government may not, without the written permission of the party asserting limited rights, release or disclose the technical data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another party. However, the Government may reproduce, release, or disclose such data or authorize the use or reproduction of the data by persons outside the Government if it is necessary for emergency repair and overhaul, or a release or disclosure to a covered Government support contractor in performance of its covered Government support contract (management and administrative support). The recipient of the technical data is subject to prohibition on the further reproduction, release, disclosure, or use of the technical data, and the contractor or subcontractor asserting the restriction shall be notified of such reproduction, release, disclosure, or use.

“Restricted Rights” applies only to noncommercial computer software and means the Government’s right to use a computer program on a limited number of computers and make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes. However, the Government may allow the use of the noncommercial computer software outside of the Government under a limited set of circumstances, including use by a covered Government support contractor in performance of its covered Government support contract (management and administrative support), and after the contractor or subcontractor asserting the restriction is notified.

“SBIR Data Rights” refers to a Small Business Innovation Research contract and applies to both technical data and computer software. The contractor is entitled the SBIR data protection to all technical data and computer software developed during performance of a SBIR Phase III agreement, regardless of the funding source. SBIR Data Rights are generally equivalent to Limited Rights for technical data and Restricted Rights for computer software. In the DOD, SBIR Data Rights survive for five years from the completion of the Contract, at which point they will convert to Unlimited Rights. SBIR efforts are divided into three successive phases (I, II, III), with the ultimate goal of commercializing the technology in question. The Government can award an unlimited number of SBIR Phase III agreements as long as they are a logical follow-on to the technology being developed, and with the understanding that the five-year clock restarts with every award.

“Specifically Negotiated License Rights” means any modification by mutual agreement to the standard DFARS noncommercial data rights categories (Unlimited Rights, Government Purpose Rights, Limited/Restricted Rights) laid out in this Article that the parties consider appropriate to the specific contract action but shall not provide rights less than that provided by Limited Rights. Any rights so negotiated shall be identified in a license agreement written into or made part of this Contract.

“Technical Data” means recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial or management information.

“Unlimited Rights” means the right to use, modify, reproduce, perform, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

B. Allocation of Principal Rights

The Government shall receive a Government Purpose Rights license or an Unlimited Rights license to all technical data and computer software developed and delivered under the prime Contract, except for the technical data and computer software that was previously developed exclusively at private expense and identified in a Statement of Work. To the maximum extent practicable, segregable portions of deliverables that will be restricted shall be clearly identified and labeled by Seller.

C. Handling of Data

If Seller wishes to deliver its internally developed technical data or computer software to Lockheed Martin for purposes of delivery to the prime government customer, the Government customer will obtain license rights in accordance with Section B above, Allocation of Principal Rights, unless Seller substantiates that the technical data or computer software were not developed in performance of the Contract.

Technical Data and Computer Software Provided by Lockheed Martin (to include such technical data and computer software of the Government providing by Lockheed Martin on the Government’s behalf): Technical data and computer software provided by Lockheed Martin under this Contract shall be appropriately marked with a suitable notice or legend and maintained in confidence and disclosed and used by Seller only for the purpose of carrying out its responsibilities under this Contract. At no time will technical data and computer software provided by Lockheed Martin under this Contract become the property of Seller, nor does its use in carrying out its responsibilities grant any form of license to Seller to disclose or use that technical data or computer software for any other purpose, unless specifically agreed to in writing by Lockheed Martin. This includes all technical data and computer software first produced by Lockheed Martin under this Contract. . Upon completion of a Contract, the aforementioned technical data and computer software shall be disposed of as requested by Lockheed Martin.

Oral and Visual Information: If information which Seller considers to embody trade secrets or to comprise commercial or financial information which is privileged or confidential is disclosed orally or visually to the Lockheed Martin, the exchange of such information must be reduced to a tangible, recorded form and marked with a suitable notice or legend, and furnished to Lockheed Martin within ten (10) calendar days after such oral or visual disclosure, or Lockheed Martin shall have no duty to limit or restrict, and shall not incur any liability for any disclosure and use of such information.

Disclaimer of Liability: Notwithstanding the above, Lockheed Martin shall not be restricted in, nor incur any liability for, the disclosure and use of:

(1) Data or software not identified with a suitable notice or legend as set forth in this Article; nor

(2) Information contained in any data or software for which disclosure and use is restricted under a proprietary information agreement, if such information is or becomes generally known without breach of the above, is known to or is generated by Lockheed Martin independently of carrying out responsibilities under this Contract, is rightfully received from a third party without restriction, or is included in data or software which Seller is required to furnish to Lockheed Martin without restriction on disclosure and use.

D. Marking of Data

Except for technical data and computer software developed or delivered with Unlimited Rights, all technical data and computer software developed and delivered under this Contract shall have appropriate Data Rights Markings in accordance with DFARS 252.227-7013(f) and 252.227-7014(f). Lockheed Martin will have Unlimited Rights to all unmarked technical data or computer software delivered by the Seller. In the event that unmarked technical data or computer software should have contained a restrictive legend, Seller can cure the omission by providing written notice to Lockheed Martin within thirty (30) calendar days of the erroneous disclosure. Lockheed Martin will not be responsible for any additional disclosures of the inappropriately marked technical data or computer software prior to that written notice.

E. Lower Tier Agreements

Seller shall include this Article, suitably modified, in all of Seller’s lower tier agreements, regardless of tier, for work performed under this Contract.

The provisions of this Article shall survive termination of this Contract.

ARTICLE II: EXPORT CONTROL AND FOREIGN ACCESS TO TECHNOLOGY

This Article shall remain in effect during the term of this Contract and for 25 years thereafter and supplement the export control provisions of the CorpDoc1

A. General

The Parties agree that research findings and technology developments arising under this Contract may constitute a significant enhancement to the national defense, and to the economic vitality of the United States. Accordingly, access to important technology developments under this Contract by Foreign Firms or Institutions must be carefully controlled. The controls contemplated in this Article are in addition to, and are not intended to change or supersede, the provisions of the International Traffic in Arms Regulations (22 C.F.R. Part 120, et seq.), the National Security Program Operating Manual (NISPOM) (DoD 5220.22-M), and the Department of Commerce’s Export Administration Regulations (15 C.F.R. Part 730, et seq.).

B. Restrictions on Sale or Transfer of Technology to Foreign Firms or Institutions

In order to promote the national security interests of the United States and to effectuate the policies that underlie the regulations cited above, the procedures stated below shall apply to any transfer of Technology. For purposes of this paragraph, a transfer includes a sale of the company, and sales or licensing of Technology. Transfers do not include:

--Sales of products or components; or

--Licenses of software or documentation related to sales of products or components; or

--Transfer to foreign subsidiaries of Seller for purposes related to this Contract; or

--Transfer which provides access to Technology to a Foreign Firm or Institution which is an approved source of supply or source for the conduct of research under this Contract provided that such transfer shall be limited to that necessary to allow the firm or institution to perform its approved role under this Contract.

Seller shall provide timely notice to Lockheed Martin of any proposed transfers from Seller of Technology developed under this Contract to Foreign Firms or Institutions. If the united States government determines that the transfer may have adverse consequences to the national security interests of the United States, Seller, its vendors, and Lockheed Martin, and the government shall jointly endeavor to find alternatives to the proposed transfer which obviate or mitigate potential adverse consequences of the transfer but which provide substantially equivalent benefits to Seller.

In any event, Seller shall provide written notice to Lockheed Martin of any proposed transfer to a Foreign Firm or Institution at least sixty (60) calendar days prior to the proposed date of transfer. Such notice shall cite this Article and shall state specifically what is to be transferred and the general terms of the transfer. Within thirty (30) calendar days of receipt of the written notification, Lockheed Martin shall advise Seller whether it consents to the proposed transfer. In cases where Lockheed Martin does not concur or ninety (90) calendar days after receipt and Lockheed Martin provides no decision, Seller may utilize the procedures under the Disputes clause. No transfer shall take place until a decision is rendered.

In the event a transfer of Technology to Foreign Firms or Institutions which is NOT approved by Lockheed Martin takes place, Seller shall (a) refund to Lockheed Martin funds paid for the development of the Technology and (b) Lockheed Martin shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice, or to have practiced on behalf of the United States, the Technology throughout the world for any and all purposes, particularly to effectuate the intent of this Contract. Upon request of Lockheed Martin, Seller shall provide written confirmation of such licenses.

C. Lower Tier Agreements

Seller shall include this Article, suitably modified in all of Seller’s lower tier agreements, regardless of tier, for work performed under this Contract

ARTICLE III: ENVIRONMENTAL REQUIREMENTS

Seller shall adhere to the following:

1) Pollution Prevention: Consideration should be given to alternative materials and processes in order to eliminate, reduce or minimize hazardous waste being generated. This is to be accomplished while minimizing item cost and risk to item performance.

2) Environmental Compliance: All activities must be in compliance with Federal, state, and local environmental laws and regulations, as well as Executive orders, treaties, and international agreements. Seller shall evaluate the environmental consequences and identify the specific types and amounts of hazardous waste being generated during activities undertaken to perform under this Contract.

3) Hazardous Waste Report: Seller shall submit a Hazardous Waste Report IAW DI-MGMT- 80899, as applicable.

4) Disposal Instructions for Residual/Scrap Materials: Seller shall dispose of all residual and scrap materials generated during performance of this Contract, including high explosives. Seller shall notify Lockheed Martin of the anticipated quantities, methods of disposal and disposal costs.

ARTICLE IV: OPSEC & SECURITY

A. Security Requirements

1) The security level for this agreement is UNCLASSIFIED. Seller does not receive, generate or store any classified information or material at its locations.

2) Work performed by Seller may involve access to Controlled Unclassified Information (CUI) as well as information classified as CONFIDENTIAL, SECRET, or TOP SECRET (pending facility clearance approval by Defense Security Services.). Seller shall comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operation Manual (DOD 5220.22M), Security Classification Specification (DD Form 254), and (2) any revisions to that manual that may be issued. During the course of this Contract, the parties may determine that information developed by Seller and/or Lockheed Martin pursuant to this Contract shall be treated as classified. Such information shall be classified in accordance with DOD 5220.22M.

3) Lockheed Martin will provide the Security Classification Specification (DD form 254) for this Contract.

4) If Seller performs on a classified Contract, Seller shall obtain and maintain a Facility Clearance from the Defense Security Service. Seller shall receive classified material at the actual performance location(s) only as identified in block 8a of the DD254 issued for this Contract.

5) Seller shall issue all subcontract Security Classification Specifications (DD Form 254) to lower tier awards.

6) Seller shall have a Non-Disclosure Agreement signed by all Seller employees working under this Contract and returned to Lockheed Martin. Seller shall not release any information or data without the approval of Lockheed Martin.

7) Seller personnel shall have the appropriate level of investigation and/or security clearance for this Contract. Seller shall observe and comply with all security provisions in effect at each selected site. Only U.S. Citizens are authorized to work classified Contracts. All Seller personnel that require access to classified information and/or material will be required to have the appropriate level clearance and must maintain the level of security clearance for the life of this Contract. Seller shall notify Lockheed Martin the same day as an employee receives notice that they will be released, have been fired, or have had their security clearance revoked or suspended.

8) Within this Contract, sharing of classified information shall be on a need-to-know basis, as required by this Contract.

9) Lockheed Martin will make the decision and/or final determination as to the disposition of any classified information and/or material held by Seller at the completion of this Contract. Upon completion or termination, Seller shall:

a. Return ALL classified material received or generated under this Contract;

b. Destroy all classified material; or

c. Request retention for a specific period of time

10) If this Contract involves a classified effort or a Controlled Unclassified Information (CUI) effort, the below listed Department of Defense Directives, Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), and other clauses shall be incorporated into this Contract by reference with the same force and effect as if they were given in full text. Specific applicable security classification guides, policies, instructions, and regulations will be identified in this Contract. Throughout the life of this Contract, if any policy, instruction, or regulation is replaced or superseded, the replacement or superseding version shall apply.

a. DoDM 5200.01 DoD Information Security Program, 24 Feb 12

b. DoD 5200.2-R Personnel Security Regulation, Jan 87

c. DoD 5220.22-M National Industrial Security Program, 28 Feb 06

d. DoDI 5200.01, Information Security Program and Protection of Sensitive Compartmented Information, 21 Apr 2016

e. DoDM 5400.7-R, DOD Freedom of Information Act Program, 25 Jan 2017

f. DoDI 2000.12, Antiterrorism Program, 1 Mar 12

g. DODD 5205.02E, DOD Operations Security (OPSEC) Program, 20 Jun 2012

h. DODI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research,

i. Development, Test, and Evaluation (RDT&E), 28 May 2015

j. AR 380-5, Department of the Army Information Security, 29 Sep 2000

k. AR 380-49, Industrial Security Program, 20 Mar 2013

l. AR 530-1, Operations Security, 26 Sep 2014

m. FAR Clause 4.402, Safeguarding Classified Information Within Industry

n. FAR Clause 52.204-2, Security Requirements, Aug 1996

11) The following security clauses are applicable only if Seller will be onsite at Fort Carson:

1. All Seller employees, to include subcontractor employees, requiring access to Army installations, facilities, controlled access areas, or require network access, shall complete AT Level I awareness training within 30 calendar days after Contract start date or effective date of incorporation of this requirement into this Contract, whichever is applicable. Upon request, Seller shall submit certificates of completion for each affected Seller employee and subcontractor employee, to Lockheed Martin, within 5 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: http://jko.jten.mil/courses/atl1/launch.html; or it can be provided in presentation form which will be documented via memorandum.

2. All Seller’s and Seller’s sub-contractors’ employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). Seller shall also provide all information required for background checks to meet installation/facility access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Seller’s workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this Contract, should the Force Protection Condition (FPCON) at any installation or facility change, the Government may require changes in contractor security matters or processes.

3. Seller’s and Seller’s sub-contractors’ employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05 / AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative, as NCIC and TSDB are available), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

4. All Seller employees, including subcontractor employees who are not in possession of the appropriate security clearance or access privileges, will be escorted in areas where they may be exposed to classified and/or sensitive materials and/or sensitive or restricted areas.

5. Seller must have a Facility Clearance (FCL) at the appropriate level (IAW the NISPOM DOD 5220.22-M and AR 380-49) prior to the start of the Contract awarded period of performance. Seller personnel performing work under this Contract must have the required security clearance, per AR 380-67, at the appropriate level at the start of the period of performance. Security Clearances and FCL requirements are required to be maintained for the life of this Contract IAW the DD Form 254 attached to this Contract. If Seller does not have an FCL, the supporting Government Contracting Activity will sponsor Seller in obtaining the FCL.

B. Reserved.

ARTICLE V: PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

This provision only applies if the delivered part or the part being ordered contains telecommunications equipment.

(a) Definitions. As used in this clause

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Seller is prohibited from providing to Lockheed Martin any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event Seller identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or Seller is notified of such by a subcontractor at any tier or by any other source, Seller shall report the information in paragraph (d)(2) of this clause to the Contracting Officer and to Lockheed Martin, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, Seller shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, Seller shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) Seller shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, Seller shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. Seller shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

ARTICLE VI: DUTY FREE ENTRY CLAUSES

The United States Government has approved the waiver of duties for importing goods into the United States of America on this program. The following Federal Regulations are incorporated:

FAR 52.225-8 Duty-Free Entry (Oct 2010)

DFAR 252.225-7013 Duty-Free Entry (Apr 2020)

3275 (3/1/22)

The following additional clauses apply to this Contract.

ARTICLE I: DATA RIGHTS AND COPYRIGHTS

Technical Data and Computer Software Rights under this Contract shall be determined in accordance with DFARS 252.227-7013 (Rights in Technical Data—Noncommercial Items (Feb 2014)) and DFARS 252.227-7014 (Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb 2014)), except as otherwise specified herein. The definitions included in this Article shall replace the definitions found in the referenced DFARS clauses.

A. Definitions

“Government Purpose” means any activity in which the Government is a party. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data for commercial purposes or authorize others to do so.

“Government Purpose Rights” means the right to use, modify, reproduce, release, perform, display, or disclose technical data within the Government without restriction; and to release or disclose technical data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose that data for Government purposes. This is a middle path unique to defense contracts that allows contractors to have the exclusive right to use the technical data in the commercial market. Unless otherwise agreed, Government Purpose Rights convert to Unlimited Rights five years after execution of the Project.

“Limited Rights” means the right to use, modify, reproduce, release, perform, display, or disclose technical data, in whole or in part, within the Government. The Government may not, without the written permission of the party asserting limited rights, release or disclose the technical data outside the Government, use the technical data for manufacture, or authorize the technical data to be used by another party. However, the Government may reproduce, release, or disclose such data or authorize the use or reproduction of the data by persons outside the Government if it is necessary for emergency repair and overhaul, or a release or disclosure to a covered Government support contractor in performance of its covered Government support contract (management and administrative support). The recipient of the technical data is subject to prohibition on the further reproduction, release, disclosure, or use of the technical data, and the contractor or subcontractor asserting the restriction shall be notified of such reproduction, release, disclosure, or use.

“Restricted Rights” applies only to noncommercial computer software and means the Government’s right to use a computer program on a limited number of computers and make the minimum number of copies of the computer software required for safekeeping (archive), backup, or modification purposes. However, the Government may allow the use of the noncommercial computer software outside of the Government under a limited set of circumstances, including use by a covered Government support contractor in performance of its covered Government support contract (management and administrative support), and after the contractor or subcontractor asserting the restriction is notified.

“SBIR Data Rights” refers to a Small Business Innovation Research contract and applies to both technical data and computer software. The contractor is entitled the SBIR data protection to all technical data and computer software developed during performance of a SBIR Phase III agreement, regardless of the funding source. SBIR Data Rights are generally equivalent to Limited Rights for technical data and Restricted Rights for computer software. In the DOD, SBIR Data Rights survive for five years from the completion of the Contract, at which point they will convert to Unlimited Rights. SBIR efforts are divided into three successive phases (I, II, III), with the ultimate goal of commercializing the technology in question. The Government can award an unlimited number of SBIR Phase III agreements as long as they are a logical follow-on to the technology being developed, and with the understanding that the five-year clock restarts with every award.

“Specifically Negotiated License Rights” means any modification by mutual agreement to the standard DFARS noncommercial data rights categories (Unlimited Rights, Government Purpose Rights, Limited/Restricted Rights) laid out in this Article that the parties consider appropriate to the specific contract action but shall not provide rights less than that provided by Limited Rights. Any rights so negotiated shall be identified in a license agreement written into or made part of this Contract.

“Technical Data” means recorded information, regardless of the form or method of recording, of a scientific or technical nature (including computer software documentation). The term does not include computer software or data incidental to contract administration, such as financial or management information.

“Unlimited Rights” means the right to use, modify, reproduce, perform, display, release, or disclose technical data in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so.

B. Allocation of Principal Rights

The Government shall receive a Government Purpose Rights license or an Unlimited Rights license to all technical data and computer software developed and delivered under this Contract, except for the technical data and computer software that was previously developed exclusively at private expense and identified in a Statement of Work. To the maximum extent practicable, segregable portions of deliverables that will be restricted shall be clearly identified and labeled by Seller.

If Lockheed Martin and Seller agree to engage in a Cost Share Project, and Seller desires to contribute more than 50% of the total costs of the project, Lockheed Martin may agree to a Limited or Restricted Rights license to all technical data and computer software developed and delivered under this Contract, or any other mutually agreed upon level of rights to a distinct subset of the technical data and computer software developed and delivered under this Contract.

C. Handling of Data

Seller shall clearly identify, prior to award, the technical data and computer software (and the items, components or processes to which they pertain) that will have asserted restrictions in the Statement of Work. If, after award, Seller wishes to use any other internally developed technical data or computer software, or any other pre-existing proprietary information not previously identified in the Statement of Work, then Seller shall disclose its intent in writing prior to its use and shall receive written approval from Lockheed Martin prior to its use or incorporation. The asserted restrictions in the Statement of Work are the unilateral claims of Seller, and the inclusion of those restrictions in the Statement of Work does not equate to Lockheed Martin’s agreement to those claims. At any time, Lockheed Martin has the right to request substantiating information supporting those claims and can challenge or reject those claims if they are unsupported.

Technical Data and Computer Software Provided by Lockheed Martin: Technical data and computer software provided by Lockheed Martin under this Contract shall be appropriately marked with a suitable notice or legend and maintained in confidence and disclosed and used by Seller only for the purpose of carrying out its responsibilities under this Contract. At no time will technical data and computer software provided by Lockheed Martin under this Contract become the property of Seller, nor does its use in carrying out its responsibilities grant any form of license to Seller to disclose or use that technical data or computer software for any other purpose, unless specifically agreed to in writing by Lockheed Martin. This includes all technical data and computer software first produced by Lockheed Martin under this Contract. All Contracts that contain technical data or computer software provided by the Lockheed Martin shall have appropriate non-disclosure agreements signed by Seller. Upon completion of a Contract, the aforementioned technical data and computer software shall be disposed of as requested by Lockheed Martin.

Oral and Visual Information: If information which Seller considers to embody trade secrets or to comprise commercial or financial information which is privileged or confidential is disclosed orally or visually to the Lockheed Martin, the exchange of such information must be reduced to a tangible, recorded form and marked with a suitable notice or legend, and furnished to Lockheed Martin within ten (10) calendar days after such oral or visual disclosure, or Lockheed Martin shall have no duty to limit or restrict, and shall not incur any liability for any disclosure and use of such information.

Disclaimer of Liability: Notwithstanding the above, Lockheed Martin shall not be restricted in, nor incur any liability for, the disclosure and use of:

(1) Data or software not identified with a suitable notice or legend as set forth in this Article; nor

(2) Information contained in any data or software for which disclosure and use is restricted under a proprietary information agreement, if such information is or becomes generally known without breach of the above, is known to or is generated by Lockheed Martin independently of carrying out responsibilities under this Contract, is rightfully received from a third party without restriction, or is included in data or software which Seller is required to furnish to Lockheed Martin without restriction on disclosure and use.

D. Marking of Data

Except for technical data and computer software developed or delivered with Unlimited Rights, all technical data and computer software developed and delivered under this Contract shall have appropriate Data Rights Markings in accordance with DFARS 252.227-7013(f) and 252.227-7014(f). Lockheed Martin will have Unlimited Rights to all unmarked technical data or computer software. In the event that unmarked technical data or computer software should have contained a restrictive legend, Seller can cure the omission by providing written notice to Lockheed Martin within thirty (30) calendar days of the erroneous disclosure. Lockheed Martin will not be responsible for any additional disclosures of the inappropriately marked technical data or computer software prior to that written notice.

E. Lower Tier Agreements

Seller shall include this Article, suitably modified, in all of Seller’s lower tier agreements, regardless of tier, for work performed under this Contract.

The provisions of this Article shall survive termination of this Contract.

ARTICLE II: EXPORT CONTROL AND FOREIGN ACCESS TO TECHNOLOGY

This Article shall remain in effect during the term of this Contract and for 25 years thereafter.

A. General

The Parties agree that research findings and technology developments arising under this Contract may constitute a significant enhancement to the national defense, and to the economic vitality of the United States. Accordingly, access to important technology developments under this Contract by Foreign Firms or Institutions must be carefully controlled. The controls contemplated in this Article are in addition to, and are not intended to change or supersede, the provisions of the International Traffic in Arms Regulations (22 C.F.R. Part 120, et seq.), the National Security Program Operating Manual (NISPOM) (DoD 5220.22-M), and the Department of Commerce’s Export Administration Regulations (15 C.F.R. Part 730, et seq.).

B. Restrictions on Sale or Transfer of Technology to Foreign Firms or Institutions

In order to promote the national security interests of the United States and to effectuate the policies that underlie the regulations cited above, the procedures stated below shall apply to any transfer of Technology. For purposes of this paragraph, a transfer includes a sale of the company, and sales or licensing of Technology. Transfers do not include:

--Sales of products or components; or

--Licenses of software or documentation related to sales of products or components; or

--Transfer to foreign subsidiaries of Seller for purposes related to this Contract; or

--Transfer which provides access to Technology to a Foreign Firm or Institution which is an approved source of supply or source for the conduct of research under this Contract provided that such transfer shall be limited to that necessary to allow the firm or institution to perform its approved role under this Contract.

Seller shall provide timely notice to Lockheed Martin of any proposed transfers from Seller of Technology developed under this Contract to Foreign Firms or Institutions. If Lockheed Martin determines that the transfer may have adverse consequences to the national security interests of the United States, Seller, its vendors, and Lockheed Martin shall jointly endeavor to find alternatives to the proposed transfer which obviate or mitigate potential adverse consequences of the transfer but which provide substantially equivalent benefits to Seller.

In any event, Seller shall provide written notice to Lockheed Martin of any proposed transfer to a Foreign Firm or Institution at least sixty (60) calendar days prior to the proposed date of transfer. Such notice shall cite this Article and shall state specifically what is to be transferred and the general terms of the transfer. Within thirty (30) calendar days of receipt of the written notification, Lockheed Martin shall advise Seller whether it consents to the proposed transfer. In cases where Lockheed Martin does not concur or ninety (90) calendar days after receipt and Lockheed Martin provides no decision, Seller may utilize the procedures under the Disputes clause. No transfer shall take place until a decision is rendered.

In the event a transfer of Technology to Foreign Firms or Institutions which is NOT approved by Lockheed Martin takes place, Seller shall (a) refund to Lockheed Martin funds paid for the development of the Technology and (b) Lockheed Martin shall have a non-exclusive, nontransferable, irrevocable, paid-up license to practice, or to have practiced on behalf of the United States, the Technology throughout the world for any and all purposes, particularly to effectuate the intent of this Contract. Upon request of Lockheed Martin, Seller shall provide written confirmation of such licenses.

C. Lower Tier Agreements

Seller shall include this Article, suitably modified in all of Seller’s lower tier agreements, regardless of tier, for work performed under this Contract

ARTICLE III: ENVIRONMENTAL REQUIREMENTS

Seller shall adhere to the following:

1) Pollution Prevention: Consideration should be given to alternative materials and processes in order to eliminate, reduce or minimize hazardous waste being generated. This is to be accomplished while minimizing item cost and risk to item performance.

2) Environmental Compliance: All activities must be in compliance with Federal, state, and local environmental laws and regulations, as well as Executive orders, treaties, and international agreements. Seller shall evaluate the environmental consequences and identify the specific types and amounts of hazardous waste being generated during activities undertaken to perform under this Contract.

3) Hazardous Waste Report: Seller shall submit a Hazardous Waste Report IAW DI-MGMT- 80899, as applicable.

4) Disposal Instructions for Residual/Scrap Materials: Seller shall dispose of all residual and scrap materials generated during performance of this Contract, including high explosives. Seller shall notify Lockheed Martin of the anticipated quantities, methods of disposal and disposal costs.

ARTICLE IV: OPSEC & SECURITY

A. Security Requirements

1) The security level for this agreement is UNCLASSIFIED. Seller does not receive, generate or store any classified information or material at its locations.

2) Work performed by Seller may involve access to Controlled Unclassified Information (CUI) as well as information classified as CONFIDENTIAL, SECRET, or TOP SECRET (pending facility clearance approval by Defense Security Services.). Seller shall comply with (1) the Security Agreement (DD Form 441), including the National Industrial Security Program Operation Manual (DOD 5220.22M), Security Classification Specification (DD Form 254), and (2) any revisions to that manual that may be issued. During the course of this Contract, the parties may determine that information developed by Seller and/or Lockheed Martin pursuant to this Contract shall be treated as classified. Such information shall be classified in accordance with DOD 5220.22M.

3) Lockheed Martin will provide the Security Classification Specification (DD form 254) for this Contract.

4) If Seller performs on a classified Contract, Seller shall obtain and maintain a Facility Clearance from the Defense Security Service. Seller shall receive classified material at the actual performance location(s) only as identified in block 8a of the DD254 issued for this Contract.

5) Seller shall issue all subcontract Security Classification Specifications (DD Form 254) to lower tier awards.

6) Seller shall have a Non-Disclosure Agreement signed by all Seller employees working under this Contract and returned to Lockheed Martin. Seller shall not release any information or data without the approval of Lockheed Martin.

7) Seller personnel shall have the appropriate level of investigation and/or security clearance for this Contract. Seller shall observe and comply with all security provisions in effect at each selected site. Only U.S. Citizens are authorized to work classified Contracts. All Seller personnel that require access to classified information and/or material will be required to have the appropriate level clearance and must maintain the level of security clearance for the life of this Contract. Seller shall notify Lockheed Martin the same day as an employee receives notice that they will be released, have been fired, or have had their security clearance revoked or suspended.

8) Within this Contract, sharing of classified information shall be on a need-to-know basis, as required by this Contract.

9) Lockheed Martin will make the decision and/or final determination as to the disposition of any classified information and/or material held by Seller at the completion of this Contract. Upon completion or termination, Seller shall:

a. Return ALL classified material received or generated under this Contract;

b. Destroy all classified material; or

c. Request retention for a specific period of time

10) If this Contract involves a classified effort or a Controlled Unclassified Information (CUI) effort, the below listed Department of Defense Directives, Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement (DFARS), and other clauses shall be incorporated into this Contract by reference with the same force and effect as if they were given in full text. Specific applicable security classification guides, policies, instructions, and regulations will be identified in this Contract. Throughout the life of this Contract, if any policy, instruction, or regulation is replaced or superseded, the replacement or superseding version shall apply.

a. DoDM 5200.01 DoD Information Security Program, 24 Feb 12

b. DoD 5200.2-R Personnel Security Regulation, Jan 87

c. DoD 5220.22-M National Industrial Security Program, 28 Feb 06

d. DoDI 5200.01, Information Security Program and Protection of Sensitive Compartmented Information, 21 Apr 2016

e. DoDM 5400.7-R, DOD Freedom of Information Act Program, 25 Jan 2017

f. DoDI 2000.12, Antiterrorism Program, 1 Mar 12

g. DODD 5205.02E, DOD Operations Security (OPSEC) Program, 20 Jun 2012

h. DODI 5200.39, Critical Program Information (CPI) Identification and Protection Within Research,

i. Development, Test, and Evaluation (RDT&E), 28 May 2015

j. AR 380-5, Department of the Army Information Security, 29 Sep 2000

k. AR 380-49, Industrial Security Program, 20 Mar 2013

l. AR 530-1, Operations Security, 26 Sep 2014

m. FAR Clause 4.402, Safeguarding Classified Information Within Industry

n. FAR Clause 52.204-2, Security Requirements, Aug 1996

11) The following security clauses are applicable only if Seller will be onsite at Fort Carson:

1. All Seller employees, to include subcontractor employees, requiring access to Army installations, facilities, controlled access areas, or require network access, shall complete AT Level I awareness training within 30 calendar days after Contract start date or effective date of incorporation of this requirement into this Contract, whichever is applicable. Upon request, Seller shall submit certificates of completion for each affected Seller employee and subcontractor employee, to Lockheed Martin, within 5 calendar days after completion of training by all employees and subcontractor personnel. AT Level I awareness training is available at the following website: http://jko.jten.mil/courses/atl1/launch.html; or it can be provided by the RA ATO in presentation form which will be documented via memorandum.

2. All Seller’s and Seller’s sub-contractors’ employees shall comply with applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative). Seller shall also provide all information required for background checks to meet installation/facility access requirements to be accomplished by installation Provost Marshal Office, Director of Emergency Services or Security Office. Seller’s workforce must comply with all personal identity verification requirements (FAR clause 52.204-9, Personal Identity Verification of Contractor Personnel) as directed by DOD, HQDA and/or local policy. In addition to the changes otherwise authorized by the changes clause of this Contract, should the Force Protection Condition (FPCON) at any installation or facility change, the Government may require changes in contractor security matters or processes.

3. Seller’s and Seller’s sub-contractors’ employees shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (TSDB) (Army Directive 2014-05 / AR 190-13), applicable installation, facility and area commander installation/facility access and local security policies and procedures (provided by government representative, as NCIC and TSDB are available), or, at OCONUS locations, in accordance with status of forces agreements and other theater regulations.

4. All Seller employees, including subcontractor employees who are not in possession of the appropriate security clearance or access privileges, will be escorted in areas where they may be exposed to classified and/or sensitive materials and/or sensitive or restricted areas.

5. Seller must have a Facility Clearance (FCL) at the appropriate level (IAW the NISPOM DOD 5220.22-M and AR 380-49) prior to the start of the Contract awarded period of performance. Seller personnel performing work under this Contract must have the required security clearance, per AR 380-67, at the appropriate level at the start of the period of performance. Security Clearances and FCL requirements are required to be maintained for the life of this Contract IAW the DD Form 254 attached to this Contract. If Seller does not have an FCL, the supporting Government Contracting Activity will sponsor Seller in obtaining the FCL.

B. Safeguarding Covered Defense Information and Cyber Incident Reporting

1) Definitions. As used in this Article—

“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 information system belonging to, or operated by or for, Seller.

“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 information that—

(i) Is—

a) Provided to Seller by or on behalf of DoD in connection with the performance of this Contract; or

b) Collected, developed, received, transmitted, used, or stored by or on behalf of Seller in support of the performance of this Contract; and

(ii) Falls in any of the following categories:

a) Controlled technical information.

b) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process).

c) Export control. Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.

d) Any other information, marked or otherwise identified in this Contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies (e.g., privacy, proprietary business information).

“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.

“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 information is recorded, stored, or printed within an 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.

“Rapid(ly) report(ing)” 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 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.

2) Adequate security

Seller shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this Contract. To provide adequate security, Seller shall implement information systems security protections on all covered information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

a) Cloud computing services shall be subject to the security requirements specified in DFARS clause 252.239-7010, Cloud Computing Services; and

b) 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; or

(ii) 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 above—

a) 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,” http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by Lockheed Martin, as soon as practical, but not later than December 31, 2017. Seller shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, and Lockheed Martin, within 30 days of Contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of Contract award; or

b) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of Lockheed Martin; and

c) Apply other information systems security measures when Seller reasonably determines that information systems security measures, in addition to those identified in this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

3) Cyber incident reporting requirement

When Seller discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects Seller’s ability to perform the requirements of this Contract that are designated as operationally critical support, Seller 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 Seller’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 Seller’s ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <http://dibnet.dod.mil> and provide a copy to Lockheed Martin.

(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, Seller or its subcontractor(s) 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>.

4) Malicious software

Seller or its subcontractor(s) that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the AO.

5) Media preservation and protection

When Seller discovers a cyber incident has occurred, Seller shall preserve and protect images of all known affected information systems identified in 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.

6) Access to additional information or equipment necessary for forensic analysis.

Upon request by DoD, Seller shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

7) Cyber incident damage assessment activities.

If DoD elects to conduct a damage assessment, the AO will request that Seller provide all of the damage assessment information gathered in accordance with this clause.

8) DoD safeguarding and use of attributional/proprietary information

The Government will protect against the unauthorized use or release of information obtained from Seller (or derived from information obtained from Seller) under this clause that includes Seller attributional/proprietary information, including such information submitted in accordance with this clause. To the maximum extent practicable, Seller shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize Seller 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.

9) Use and release of attributional/proprietary information not created by or for DoD.

Information that is obtained from Seller (or derived from information obtained from Seller) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

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

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

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

d) 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

e) 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.

10) Use and release of attributional/proprietary information created by or for DoD.

Information that is obtained from Seller (or derived from information obtained from Seller) under this clause that is created by or for DoD (including the information submitted pursuant to this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by 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.

11) Seller 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.

12) Other safeguarding or reporting requirements

The safeguarding and cyber incident reporting required by this clause in no way abrogates Seller 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.

13) Subcontracts

Seller shall—

a) Include this clause, including this paragraph, in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and

b) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and to Lockheed Martin. This includes providing the incident report number, automatically assigned by DoD, to Lockheed Martin as soon as practicable.

ARTICLE V: PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

(a) Definitions. As used in this clause

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Seller is prohibited from providing to Lockheed Martin any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event Seller identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or Seller is notified of such by a subcontractor at any tier or by any other source, Seller shall report the information in paragraph (d)(2) of this clause to the Contracting Officer and to Lockheed Martin, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, Seller shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, Seller shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) Seller shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, Seller shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. Seller shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.