## DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT (DFARS)

The FAR and DFARS clauses referenced below are incorporated herein by reference, with the same force and effect as if they were given in full text, and are applicable, including any notes following the clause citation, to this Contract. If the date or substance of any of the clauses listed below is different from the date or substance of the clause actually incorporated in the Prime Contract referenced by number herein, the date or substance of the clause incorporated by said Prime Contract shall apply instead. The Contracts Disputes Act shall have no application to this Contract, and nothing in this Contract grants SELLER a direct claim or cause of action against the U.S. Government. Any reference to a "Disputes" clause shall mean the "Disputes" clause of this Contract. SELLER shall include in each lower-tier subcontract the appropriate flow down clauses as required by the FAR and FAR Supplement clauses included in this Contract.

## B. GOVERNMENT SUBCONTRACT

(a) This Contract is entered into by the parties in support of a U.S. Government contract.
(b) As used in the FAR and DFARS clauses referenced below and otherwise in this Contract:
1. "Commercial product" means any such product as defined in FAR 2.101.
2. "Commercial service" means any such service as defined in FAR 2.101.
3. "Commercially available off-the-shelf (COTS) item" means a COTS item as defined in FAR 2.101
4. "Contract" means this contract.
5. "Contracting Officer" shall mean the U.S. Government Contracting Officer for LOCKHEED MARTIN's government prime contract under which this Contract is entered.
6. "Contractor" and "Offeror" means the SELLER, which is the party identified on the face of the Contract with whom Lockheed Martin is contracting, acting as the immediate subcontractor to LOCKHEED MARTIN.
7. "Prime Contract" means the contract between LOCKHEED MARTIN and the U.S. Government or between LOCKHEED MARTIN and its higher-tier contractor who has a contract with the U.S. Government.
8. "Subcontract" means any contract placed by SELLER or lower-tier subcontractors under this Contract.

## C. INDEMNITY

SELLER shall indemnify and hold LOCKHEED MARTIN harmless from and against any cost, price reduction, withholding, offset, penalty, interest, claim, demand, determination of unallowability, unallocability or unreasonableness, or any other civil, criminal, or administrative liability, whether arising under statute, regulation, contract or common law, and shall reimburse LOCKHEED MARTIN for all of its damages and associated costs, including reasonable attorney fees and other expenses, if said liability is attributable to the SELLER or SELLER’s suppliers’ failure to comply with these U.S. Government Provisions and Clauses.

## D. AMENDMENTS REQUIRED BY PRIME CONTRACT

Reserved.

## E. PROVISIONS OF FAR/DFARS INCORPORATED BY REFERENCE

| Type | Clause | Date | Title | Needed Modificatoins |
|---|---|---|---|---|
| FAR | 52.203-16 | 6/1/2020 | Preventing Personal Conflicts of Interest. | None. |
| FAR | 52.204-14 | 10/1/2016 | Service Contract Reporting Requirements. | Applies if this Contract exceeds the thresholds in FAR 4.1703 except does not apply if the prime contract is funded by the Department of Defense. "Contractor" means "Lockheed Martin." The reports referred to in paragraph (f)(1) shall be furnished by Seller to Lockheed Martin by October 8 of each year. In paragraph (f)(2) the words "The Contractor shall advise the subcontractor" are changed to "Lockheed Martin advises Seller". |
| FAR | 52.204-23 | 12/1/2023 | Prohibition on Contracting for Hardware, Software, & Services Developed or Provided by Kaspersky Lab Covered Entities | |
| FAR | 52.204-27 | 6/1/2023 | Prohibition on a ByteDance Covered Application. | |
| FAR | 52.209-6 | 11/1/2021 | Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment | |
| FAR | 52.215-11dev2201 | 10/1/2021 | (DEVIATION 2022-O0001) Price Reduction for Defective Certified Cost or Pricing Data-Modifications (DEVIATION 2022-O0001) | |
| FAR | 52.215-12dfcd2201 | 10/1/2021 | (DEVIATION 2022-O0001) Subcontractor Certified Cost or Pricing Data (DEVIATION 2022-O0001) | |
| FAR | 52.215-13dfcd2201 | 10/1/2021 | (Deviation 2022-O0001) Subcontractor Certified Cost or Pricing Data-Modifications (Deviation 2022-O0001) | |
| FAR | 52.223-18 | 6/1/2020 | Encouraging Contractor Policies to Ban Text Messaging While Driving. | |
| FAR | 52.224-2 | 4/1/1984 | Privacy Act. | Applies if this contract is for the design, development, or operation of such a system of records. |
| FAR | 52.226-8 | 5/1/2024 | Encouraging Contractor Policies To Ban Text Messaging While Driving. (Re-designated from 52.223-18) | |
| FAR | 52.232-39 | 6/1/2013 | Unenforceability of Unauthorized Obligations. | None. |
| FAR | 52.239-1 | 8/1/1996 | Privacy or Security Safeguards. | N/A. |
| FAR | 52.242-15 ALT I | 4/1/1984 | Alternate I - Stop-Work Order. | |
| FAR | 52.243-2 | 8/1/1987 | Changes-Cost-Reimbursement. | |
| FAR | 52.244-6 | 12/1/2023 | Subcontracts for Commercial Products and Commercial Services. | |
| FAR | 52.245-2 | 4/1/2012 | Government Property Installation Operation Services. | Government includes Lockheed Martin except in the phrase "Government property." "Contracting Officer" means "Lockheed Martin." |
| FAR | 52.245-9 | 4/1/2012 | Use and Charges. | Communications with the Government under this clause will be made through Lockheed Martin. |
| FAR | 52.246-11 | 12/1/2014 | Higher-Level Contract Quality Requirement. | N/A. |

| | | | | |
|---|---|---|---|---|
| FAR | 52.249-6 | 5/1/2004 | Termination (Cost-Reimbursement). | "Government" and "Contracting Officer" mean "Lockheed Martin." In paragraph (d) "120" days" is changed to "60 days." In paragraph (e) "15 days" is changed to "30 days," and "45 days" is changed to "60 days." In paragraph (f) "1 year" is changed to "six months." Paragraph (j) is deleted. Alternate IV (SEP 1996) applies if this is a labor hour or time and materials contract. In Alternate IV, "90 days" is changed to "60 days." Settlements and payments under this clause may be subject to the approval of the Contracting Officer. |
| DFARS | 252.203-7004 | 1/1/2023 | Display of Hotline Posters. | |
| DFARS | 252.204-7000 | 10/1/2016 | Disclosure of Information. | In paragraph (b) "Contracting Officer" means "Lockheed Martin" and "10 days" means "20days." |
| DFARS | 252.204-7004 | 1/1/2023 | Antiterrorism Awareness Training for Contractors. | None. |
| DFARS | 252.204-7012B | 5/1/2024 | (DEVIATION 2024-o0013) Safeguarding Covered Defense Information and Cyber Incident Reporting. (DEVIATION 2024-o0013) | |
| DFARS | 252.225-7058 | 1/1/2023 | Postaward Disclosure of Employment of Individuals Who Work in the People's Republic of China. | |
| DFARS | 252.227-7014 | 3/1/2023 | Rights in Other Than Commercial Computer Software and Other Than Commercial Computer Software Documentation. | |
| DFARS | 252.239-7001 | 1/1/2008 | Information Assurance Contractor Training and Certification. | None. |
| DFARS | 252.243-7002 | 12/1/2022 | Requests for Equitable Adjustment. | "Government" means "LockheedMartin." |
| DFARS | 252.244-7000 | 11/1/2023 | Subcontracts for Commercial Products or Commercial Services. | None. |
| DFARS | 252.245-7001 | 4/1/2012 | Tagging, Labeling, and Marking of Government-Furnished Property. | |
| DFARS | 252.245-7005 | 1/1/2024 | Management and Reporting of Government Property. | |
| DFARS | 252.246-7001 | 3/1/2014 | Warranty of data. | "Government" means "Lockheed Martin orthe Government." "Contracting Officer" means "Lockheed Martin."The last sentence in paragraph (b) is changed to read as follows: Thewarranty period shall extend for three years after completion of delivery of the data to LockheedMartin, or if the data is delivered to the Government, either by LockheedMartin or Seller, the warranty period shall extend for three years afterdelivery to the Government." |

## F. GOVERNMENT CONTRACT CLAUSES INCORPORATED BY FULL-TEXT

## C-227-H009 ACCESS TO DATA OR COMPUTER SOFTWARE WITH RESTRICTIVE MARKINGS (NAVSEA) (JAN 2019)

(a) Performance under this contract may require that the SubSubcontractor have access to technical data, computer software, or other sensitive data of another party that contains restrictive markings. If access to such data or software is required or to be provided, the Subcontractor shall enter into a written agreement with such party prior to gaining access to such data or software. The agreement shall address, at a minimum, (1) access to, and use of, the restrictively marked data or software exclusively for the purposes of performance of the work required by this contract, and (2) safeguards to protect such data or software from unauthorized use or disclosure for so long as the data or software remains properly restrictively marked. In addition, the agreement shall not impose any limitation upon the Government or its employees with respect to such data or software. A copy of the executed agreement shall be provided to the Contracting Officer. The Government may unilaterally modify the contract to list those third parties with which the Subcontractor has agreement(s).

(b) The Subcontractor agrees to: (1) indoctrinate its personnel who will have access to the data or software as to the restrictions under which access is granted; (2) not disclose the data or software to another party or other Subcontractor personnel except as authorized by the Contracting Officer; (3) not engage in any other action, venture, or employment wherein this information will be used, other than under this contract, in any manner inconsistent with this requirement; (4) not disclose the data or software to any other party, including, but not limited to, joint venturer, affiliate, successor, or assign of the Subcontractor; and (5) reproduce the restrictive stamp, marking, or legend on each use of the data or software whether in whole or in part.

(c) These restrictions on use and disclosure of the data and software also apply to information received from the Government through any means to which the Subcontractor has access in the performance of this contract that contains restrictive markings.

(d) The Subcontractor agrees that it will promptly notify the Contracting Officer of any attempt to gain access to any information with restrictive markings. Such notification shall include the name and organization of the individual, company, or Government representative seeking access to such information.

(e) The Subcontractor shall include this requirement in subcontracts of any tier which involve access to information covered by paragraph (a), substituting "Subcontractor" for "Subcontractor" where appropriate.

(f) Compliance with this requirement is a material requirement of this contract.

(End of clause)

**C-227-H010 COMPUTER SOFTWARE AND COMPUTER DATA BASES DELIVERED TO OR RECEIVED FROM THE GOVERNMENT (NAVSEA) (JAN 2019)**

a) The Subcontractor agrees to test for viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4, in all computer software and

computer data bases (as defined in the clause entitled "Rights In Noncommercial Computer Software and Noncommercial Computer Software Documentation" (DFARS 252.227-7014)), before delivery of that computer software or computer data base in whatever media and on whatever system the computer software or data base is delivered whether delivered separately or imbedded within delivered equipment. The Subcontractor warrants that when delivered any such computer software and computer data base shall be free of viruses, malware, Trojan Horses, and other security threats such as those listed in NIST Special Publication 800-12 Rev 1.

b) The Subcontractor agrees that prior to use under this contract, it shall test any computer software and computer data base received from the Government for viruses, malware, Trojan Horses, and other security threats listed in NIST Special Publication 800-12 Rev 1, An Introduction to Computer Security, The NIST Handbook, Chapter 4.

c) Any license agreement governing the use of any computer software or computer software documentation delivered to the Government as a result of this contract must be paid-up, irrevocable, world-wide, royalty-free, perpetual and flexible (user licenses transferable among Government employees and personnel under Government contract).

d) The Subcontractor shall not include or permit to be included any routine to enable the Subcontractor or its subSubcontractor(s) or vendor(s) to disable the computer software or computer data base after delivery to the Government.

e) No copy protection devices or systems shall be used in any computer software or computer data base delivered under this contract with unlimited or Government purpose rights (as defined in DFARS 252.227-7013 and 252.227- 7014) to restrict or limit the Government from making copies.

f) It is agreed that, to the extent that any technical or other data is computer software by virtue of its delivery in digital form, the Government shall be licensed to use that digital-form data with exactly the same rights and limitations as if the data had been delivered as hard copy.

g) Any limited rights legends or other allowed legends placed by a Subcontractor on technical data or other data delivered in digital form shall be digitally included on the same media as the digital-form data and must be associated with the corresponding digital-form technical data to which the legend(s) apply to the extent possible. Such legends shall also be placed in human-readable form on a visible surface of the media carrying the digital-form data as delivered, to the extent possible.

(End of text)

**E-246-H020 QUALITY MANAGEMENT SYSTEM REQUIREMENTS (NAVSEA) (OCT 2018)**

The Contractor shall provide and maintain a quality management system that, as a minimum, adheres to the requirements of ASQ/ANSI/ISO 9001:2015 “Quality Management Systems – Requirements” and supplemental requirements imposed by this contract. The quality management system procedures, planning, and all other documentation and data that comprise the quality management system shall be made available to the Government for review. Existing quality documents that meet the requirements of this contract may continue to be used. The Government may perform any necessary inspections, verifications, and evaluations to ascertain conformance to requirements and the adequacy of the implementing procedures. The Contractor shall flow down such standards, as applicable, to lower-tier subcontractors under instances covered in FAR 52.246-11(b) or at the direction of the Contracting Officer. The Government reserves the right to disapprove the quality management system or portions thereof when it fails to meet the contractual requirements

## E-246-H023 QUALITY REQUIREMENT FOR SOFTWARE DEVELOPMENT OR PRODUCTION (NAVSEA) (JAN 2019)

The contractor's software quality program shall be an integral part of the overall Quality Management System. Software quality program controls shall be applicable to all project software that is developed, maintained, or modified within the following categories:

(a) All deliverable software

(b) All deliverable software that is included as part of deliverable hardware or firmware.

(c) Non deliverable software (commercially available or user-developed) used for development, fabrication, testing, or acceptance of deliverable software or hardware (includes automated fabrication, test, and inspection/acceptance equipment software and software design, test, and inspection tools).

(d) Commercially available, reusable, or Government software designated as part of a deliverable item.

## H-209-H003 REQUIRED DISCLOSURE OF ORGANIZATIONAL CONFLICT OF INTEREST (NAVSEA) (NOV 2022)

(a) "Organizational Conflict of Interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage. "Person" as used herein includes Corporations, Partnerships, Joint Ventures, and other business enterprises.

(b) The Subcontractor warrants that to the best of its knowledge and belief, and except as otherwise set forth in the contract, at the time of execution of this contract the Subcontractor does not have any organizational conflict of interest(s) as defined in paragraph (a).

(c) The Subcontractor agrees that, if after award, it discovers an actual or potential organizational conflict of interest, it shall make immediate and full disclosure in writing to the Contracting Officer. The notification shall include a description of the actual or potential organizational conflict of interest, a description of the action which the Subcontractor has taken or proposes to take to avoid, mitigate, or neutralize the conflict, and any other relevant information that would assist the Contracting Officer in making a determination on this matter. Notwithstanding this notification, the Government may terminate the contract for the convenience of the Government if determined to be in the best interest of the Government.

(d) Notwithstanding paragraph (c) above, if the Subcontractor was aware, or should have been aware, of an organizational conflict of interest prior to the award of this contract or becomes, or should become, aware of an organizational conflict of interest after award of this contract and does not make an immediate and full disclosure in writing to the Contracting Officer, the Government may terminate this contract for default.

(e) If the Subcontractor fails to take action required by this requirement, or required by the Contracting Officer upon receipt of the Subcontractor's disclosure required by paragraph (c), the Government may terminate this contract for default.

(f) The Contracting Officer's decision as to the existence or nonexistence of an actual or potential organizational conflict of interest shall be final.

(g) The Subcontractor shall promptly notify the Contracting Officer, in writing, if it has been tasked to evaluate or advise the Government concerning its own products or activities, those of its subSubcontractors, those of one of its prime Subcontractors (to which the Subcontractor is a subSubcontractor), or those of a competitor in order to ensure proper safeguards exist to guarantee objectivity and to protect the Government's interest.

(h) The Subcontractor shall include this requirement in subcontracts of any tier which involve access to information or situations/conditions covered by the preceding paragraphs, substituting "subSubcontractor" for "Subcontractor" where appropriate.

(i) The rights and remedies described herein shall not be exclusive and are in addition to other rights and remedies provided by law or elsewhere included in this contract.

(j) Compliance with this requirement is a material requirement of this contract.

(End of text)

**H-209-H004 RESTRICTIONS RESULTING FROM POTENTIAL ORGANIZATIONAL CONFLICT OF INTEREST (NAVSEA) (NOV 2022)**

(a) "Organizational Conflict of Interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

"Person" as used herein includes Corporations, Partnerships, Joint Ventures, and other business enterprises.

(b) It is recognized that the effort to be performed by the Subcontractor under this contract may create a potential organizational conflict of interest on the instant contract or on a future acquisition. In order to avoid this potential conflict of interest, and at the same time to avoid prejudicing the best interest of the Government, the right of the Subcontractor to participate in future procurement of equipment or services that are the subject of any work under this contract shall be limited in accordance with FAR 9.5.

(c) The Subcontractor agrees that to prevent the existence of conflicting roles and unfair competitive advantage, during the performance of this contract and for a period of three years after completion of performance of this contract, the Subcontractor, any affiliate, subSubcontractor, consultant, or employee of the Subcontractor, any joint venture, any entity into or with which it may subsequently merge or affiliate, or any other successor or assign of the Subcontractor, shall not furnish to the United States Government, either as a prime Subcontractor or as a subSubcontractor, or as a consultant to a prime Subcontractor or subSubcontractor, any system, component or services which is the subject of the work to be performed under this contract, unless an exception under FAR 9.505 exists. This exclusion also does not apply to any work covered by FAR 9.505-2 (a)(3) or (b)(3) or recompetition for those systems, components or services furnished pursuant to this contract.

(d) Nothing in this requirement is intended to prohibit or preclude the Subcontractor from marketing or selling to the United States Government its product lines in existence on the effective date of this contract; nor, shall this requirement preclude the Subcontractor from participating in any research and development or delivering any design development model or prototype of any such equipment. Additionally, sale of catalog or standard commercial items are exempt from this requirement.

(e) The Subcontractor shall include this requirement in subcontracts of any tier which involve access to information or situations/conditions covered by the preceding paragraphs, substituting "subSubcontractor" for "Subcontractor" where appropriate.

(f) The rights and remedies described herein shall not be exclusive and are in addition to other rights and remedies provided by law or elsewhere included in this contract.

(g) Compliance with this requirement is a material requirement of this contract.

(End of text)

**52.215-12 SUBSUBCONTRACTOR CERTIFIED COST OR PRICING DATA (DEVIATION 2022-O0001) (OCT2021)**

(a) Before awarding any subcontract expected to exceed $2 million, on the date of agreement on price or the date of award, whichever is later; or before pricing any subcontract modification involving a pricing adjustment expected to exceed $2 million, the Subcontractor shall require the

subSubcontractor to submit certified cost or pricing data (actually or by specific identification in writing), in accordance with Federal Acquisition Regulation (FAR) 15.408, Table 15-2 (to include any information reasonably required to explain the subSubcontractor's estimating process such as the judgmental factors applied and the mathematical or other methods used in the estimate, including those used in projecting from known data, and the nature and amount of any contingencies included in the price), unless an exception under FAR 15.403-1(b) applies. If the $2 million threshold for submission of certified cost or pricing data is adjusted for inflation as set forth in FAR 1.109(a), then pursuant to FAR 1.109(d) the changed threshold applies throughout the remaining term of the contract, unless there is a subsequent threshold adjustment.

(b) The Subcontractor shall require the subSubcontractor to certify in substantially the form prescribed in FAR 15.406-2 that, to the best of its knowledge and belief, the data submitted under paragraph (a) of this clause were accurate, complete, and current as of the date of agreement on the negotiated price of the subcontract or subcontract modification.

(c) In each subcontract that, when entered into, exceeds $2 million, the Subcontractor shall insert either—

(1) The substance of this clause, including this paragraph (c), if paragraph (a) of this clause requires submission of certified cost or pricing data for the subcontract; or

(2) The substance of the clause at 52.215-13, SubSubcontractor Certified Cost or Pricing Data—

Modifications (DEVIATION 2022-O0001).

(End of clause)

**FAR 52.243-2 CHANGES -- COST-REIMBURSEMENT Alternate I (APR 1984)**

(a) The Contracting Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in any one or more of the following:

(1) Description of services to be performed.

(2) Time of performance (i.e., hours of the day, days of the week, etc.).

(3) Place of performance of the services.

(b) If any such change causes an increase or decrease in the estimated cost of, or the time required for, performance of any part of the work under this contract, whether or not changed by the order, or otherwise affects any other terms and conditions of this contract, the Contracting Officer shall make an equitable adjustment in the (1) estimated cost, delivery or completion schedule, or both; (2) amount of any fixed fee; and (3) other affected terms and shall modify the contract accordingly.

(c) The Subcontractor must assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.

(d) Failure to agree to any adjustment shall be a dispute under the Disputes clause. However, nothing in this clause shall excuse the Subcontractor from proceeding with the contract as changed.

(e) Notwithstanding the terms and conditions of paragraphs (a) and (b) above, the estimated cost of this contract and, if this contract is incrementally funded, the funds allotted for the performance of this contract, shall not be increased or considered to be increased except by specific written modification of the contract indicating the new contract estimated cost and, if this contract is incrementally funded, the new amount allotted to the contract. Until this modification is made, the Subcontractor shall not be obligated to continue performance or incur costs beyond the point established in the Limitation of Cost or Limitation of Funds clause of this contract.

(End of clause)

**252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (JAN 2023)**

(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.

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

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution 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 Subcontractor information system means an unclassified information system that is owned, or operated by or for, a Subcontractor 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 Subcontractor 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 Subcontractor 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 Subcontractor 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--Other Than Commercial Products and Commercial Services, 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 Subcontractor shall provide adequate security on all covered Subcontractor information systems. To provide adequate security, the Subcontractor shall implement, at a minimum, the following information security protections:

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

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered Subcontractor 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 Subcontractor 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 Subcontractor 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 Subcontractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Subcontractor 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 Subcontractor'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 Subcontractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Subcontractor 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 Subcontractor 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 Subcontractor discovers a cyber incident that affects a covered Subcontractor information system or the covered defense information residing therein, or that affects the Subcontractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Subcontractor 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 Subcontractor information system(s) that were part of the cyber incident, as well as other information systems on the Subcontractor'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 Subcontractor's ability to provide operationally critical support; and

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

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

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

(d) Malicious software. When the Subcontractor or subSubcontractors 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 Subcontractor discovers a cyber incident has occurred, the Subcontractor 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 Subcontractor 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 Subcontractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of Subcontractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the Subcontractor (or derived from information obtained from the Subcontractor) under this clause that includes Subcontractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Subcontractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the Subcontractor 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 Subcontractor attributional/proprietary information not created by or for DoD. Information that is obtained from the Subcontractor (or derived from information obtained from the Subcontractor) 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 Subcontractor (“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 Subcontractor Reported Cyber Incident Information.

(j) Use and release of Subcontractor attributional/proprietary information created by or for DoD. Information that is obtained from the Subcontractor (or derived from information obtained from the Subcontractor) 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 Subcontractor 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 Subcontractor'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 Subcontractor 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 products or commercial services, without alteration, except to identify the parties. The Subcontractor shall determine if the information required for subSubcontractor 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 subSubcontractors to--

(i) Notify the prime Subcontractor (or next higher-tier subSubcontractor) 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 Subcontractor (or next higher-tier subSubcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

(End of clause)