

Document No. SMD044, Rev 5

### **Flowdowns for Prime Contract N00030-22-C-1025, CPS Zumwalt**

Where necessary, to identify the applicable parties under the following clauses, “Contractor” shall mean “Seller,” “Contracting Officer” shall mean “Lockheed Martin Procurement Representative,” “Contract” means this purchase order/subcontract and “Government” means “Lockheed Martin.”

#### **FULL TEXT**

#### **DISTRIBUTION STATEMENT F.**

In accordance with DoD Instruction 5230.24 and the Office of the Under Secretary of Defense Memorandum Use of Distribution F for Conventional Prompt Strike Program, dated March 11, 2019, all documents and materials that describe or in any way reference any aspect of the CPS program shall apply the following distribution statement on the cover of the document:

DISTRIBUTION STATEMENT F. Further dissemination only as directed by Assistant Director for Hypersonics Office (OUSD(R&E)/DDR&E(AC)/AD Hypersonics), 11 March 2019, or higher DoD authority. Forward requests to the Director of Defense Research and Engineering (Advanced Capabilities), 3015 Defense, Pentagon, Washington DC 20301-3015, or higher authority.

AND, every page or briefing slide shall contain the following:

DISTRIBUTION STATEMENT F. Further dissemination only as directed by Assistant Director for Hypersonics Office (OUSD(R&E)/DDR&E(AC)/AD Hypersonics), 11 March 2019, or higher DoD authority.

#### **SSP H-21.2 Disclosure, Use, and Protection of Proprietary Information (MAR 2021)**

1. The Contractor acknowledges that the Government may use an independent services contractor (ISC), who is neither an agent nor employee of the Government. The ISC may be used to conduct reviews, evaluations, or independent verification and validations of technical documents, or other information submitted to the Government in the performance of this contract, which is proprietary to the Contractor.
2. The use of an ISC is solely for the convenience of the Government. The ISC has no obligation to the Contractor or its subcontractors. The Contractor is required to provide full cooperation, working facilities and access to information or facilities to the ISC for the purposes stated in paragraph 1 above.
3. To protect any such proprietary information from unauthorized disclosure or unauthorized use, and to establish the respective rights and duties of both the ISC and the Contractor, the Contractor agrees to enter into a direct agreement with any ISC as the Government requires, which must authorize the Government to independently provide proprietary information to the ISC as required for the performance of Government contracts. A properly executed copy (per FAR 9.505-4) of the agreement will be provided to the Procuring Contracting Officer.
4. The Contractor shall include in each subcontract language requiring compliance by the subcontractor and succeeding levels of subcontractors with the terms and conditions herein.

#### **SSP H-32 Authorization for Access to Third-Party Proprietary Information Required for Contract Performance (MAR 2021)**

1. It is the Government's intent to ensure proper handling of sensitive planning, budgetary, acquisition, and contracting information that will be provided to, or developed by, the Contractor during contract performance. It is also the Government's intent to protect the proprietary rights of third-party contractors whose data the Contractor may receive in the performance of the contract.
2. Accordingly, the Contractor agrees that it will not disclose, divulge, discuss, or otherwise reveal information to anyone or any organization not authorized access to such information without the express written approval of the Contracting Officer. The Contractor shall require that each of its employees assigned to work under this contract, and each subcontractor and its employees assigned to work on subcontracts issued hereunder, execute nondisclosure agreements acknowledging the above restrictions before providing them access to such information. The Contractor shall also require all future company employees, subcontractors, and subcontractor employees needing similar access to such information to execute nondisclosure agreements prior to providing them access to the above identified information. The requirement for the Contractor to secure nondisclosure agreements from its employees may be satisfied by having each employee sign one nondisclosure agreement for the term of their employment, without the need to sign separate nondisclosure agreements for each individual contract which the employee will support. The Contractor will make copies of these individual agreements available to the Contracting Officer upon request.
3. The Contractor may be required to access information which is proprietary to the following third-party contractors in the performance of this contract:
4. The Contractor agrees to enter into agreements with the third-party contractors identified above to: (a) protect such proprietary information from unauthorized use or disclosure for as long as the information remains proprietary; (b) refrain from using the information for any other purpose other than support the Government contract for which it was furnished, and (c) permit the Government to independently provide such proprietary information to the Contractor subject to the restrictions of this SSP H-32 Authorization for Access to Third-Party Proprietary Information Required for Contract Performance. Prior to contract award, the Contractor shall provide a properly executed copy of such agreement(s) to the Contracting Officer in accordance with FAR 9.505-4.
5. The Contractor agrees to include in each subcontract language requiring compliance by the subcontractor and succeeding levels of subcontractors with the terms and conditions herein.
6. The Contractor agrees to indemnify and hold harmless the Government, its agents, and employees from every claim or liability, including attorney's fees, court costs, and expenses arising out of, or in any way related to, the misuse or unauthorized modification, reproduction, release, performance, display, or disclosure of data with restrictive legends received in the performance of this contract by the Contractor or any person to whom the Contractor has released or disclosed the data.
7. Any changes to the third-party contractor list above, which requires the Contractor to enter into a new direct agreement, will be communicated via contract modification. The Contractor will not be provided access to the additional third-party contractor's proprietary information until such time as a properly executed copy of the agreement is provided to the Procuring Contracting Officer in accordance with FAR 9.505-4.

### **SSP H-33 CROSS-UTILIZATION OF GOVERNMENT PROPERTY (GP) ON SSP CONVENTIONAL PROMPT STRIKE CONTRACTS (JUNE 2023)**

(a) Definitions. Definitions applicable to this contract are provided in the clause at FAR 52.245-1, Government Property and FAR 52.245-9, Use and Charges. Additional Definitions as used in this clause are: Cross Utilization means sharing GP on a rent-free non-interference use (RFNIU) basis between Authorized Contracts.

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

Originating Contract means the contract upon which the GP was initially furnished and to which ownership of the GP remains.

Gaining Contract means the contract to which GP from the Originating Contract will be furnished. Authorized Contracts are Contracts N00030-19-C-0025, N00030-22-C-1025, and AMTC-19-11-006 (to the extent paragraph (c) is satisfied).

For purposes of this clause, GP includes any equipment, special tooling, and special test equipment acquired or fabricated by the contractor, or any subcontractor.

(b) Cross Utilization of Government Property. This clause does not take precedence over FAR 52.245-9, Use and Charges, except to the extent this clause provides the authorizations required in FAR 52.245-9(b) between cost type contracts where consideration is not required. The Contractor shall not cross-utilize GP for use under any Fixed-Price type Contract Line Item Numbers (CLINs) using this clause. In accordance with FAR 52.245-9 (b), the Contracting Officer authorizes the Contractor to provide, on an RFNIU basis, GP accountable under the Authorized Contracts enumerated in paragraph (a).

(c) Reciprocal Provisions. Cross Utilization of GP accountable under another Authorized Contract is contingent upon inclusion of a clause effectively similar to this one in the respective Authorized Contract.

(d) Additional Rules. The Contractor will comply with the following rules when cross utilizing GP between Authorized Contracts:

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

(2) Cross Utilization will not interfere with the execution (in terms of cost, schedule, or performance) of the Originating Contract. In the event of a usage conflict, the Originating Contract maintains the right to use the GP.

(3) Since scheduling the Cross Utilization of GP accountable to the Authorized Contracts is controlled by the Contractor, no claim for late delivery or unavailability will be recognized by the Government as described under FAR 52.245-1(d).

(4) For the Cross Utilization of any GP between contracts identified within this SSP H-33 clause, the following shall apply:

(i) The cross utilized GP will be used on a rent-free non-interference basis.

(ii) All property will be kept in a high state of operational readiness through regular use, to include any maintenance and calibration as required.

(iii) No modifications, alterations, or cannibalization may occur to the GP without prior written Contracting Officer approval.

(iv) During cross utilization, the Gaining Contract assumes the risk for loss, damage, destruction, or theft of property during the periods of use identified in the RFNIU notification document sent to the Government in (d)(5) below.

(v) Costs for refurbishment, repair or replacement of GP are borne by the contract for which the Cross Utilization is authorized.

(vi) During Cross Utilization, the Gaining Contract is responsible for all costs associated with removing, transporting from store (if needed), cleaning and preserving property for storage, and returning the property to the designated storage once the GP is no longer needed.

(5) The Contractor shall submit a Rent-Free Non-Interference Use (RFNIU) notification document to the DCMA ACO, DCMA CA, and SSP COR at least 24 hours in advance of the start of any Cross Utilization, to identify to the Government the specific GP being cross utilized. The RFNIU notification document shall include, at a minimum: Dates of Cross Utilization, confirmation of Contractor management approval of the request, current location of GP as well as Cross Utilization location, a description of the GP, acquisition cost of the GP, serial number and/or IUID number of the property.

(e) General.

(1) This clause only gives the Contractor the authority to cross utilize GP amongst the listed contracts herein. This clause does not give the Contractor the authority to Transfer GP to any other contract without specific, written Government approval.

(2) The Government may revoke authorization provided under this clause at any time and require the Contractor to follow the formal process outlined in FAR 52.245-9, Use and Charges, when requesting to cross utilize GP on an RFNIU basis.

**REPORTING, REUTILIZATION, AND DISPOSAL (DEVIATION 2022-O0006) (NOV 2021)**

(a) Definitions. As used in this clause—

(1) “Demilitarization” means the act of eliminating the functional capabilities and inherent military design features from DoD personal property. Methods and degree range from removal and destruction of critical features to total destruction by cutting, tearing, crushing, mangling, shredding, melting, burning, etc.

(2) “Export-controlled items” means items subject to the Export Administration Regulations (EAR) (15 CFR parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR parts 120-130). The term includes—

(i) “Defense items,” defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, etc.; and

(ii) “Items,” defined in the EAR as “commodities,” “software,” and “technology,” terms that are also defined in the EAR, 15 CFR 772.1.

(3) “Ineligible transferees” means individuals, entities, or countries—

(i) Excluded from Federal programs by the General Services Administration as identified in the System for Award Management Exclusions located at <https://sam.gov>;

(ii) Delinquent on obligations to the U.S. Government under surplus sales contracts;

(iii) Designated by the Department of Defense as ineligible, debarred, or suspended from defense contracts; or

(iv) Subject to denial, debarment, or other sanctions under export control laws and related laws and regulations, and orders administered by the Department of State, the Department of Commerce, the Department of Homeland Security, or the Department of the Treasury.

(4) “Scrap” means property that has no value except for its basic material content. For purposes of demilitarization, scrap is defined as recyclable waste and discarded materials derived from items that have been rendered useless beyond repair, rehabilitation, or restoration such that the item's original identity, utility, form, fit, and function have been destroyed. Items can be classified as scrap if processed by cutting, tearing, crushing, mangling, shredding, or melting. Intact or recognizable components and parts are not “scrap.”

(5) “Serviceable or usable property” means property with potential for reutilization or sale “as is” or with minor repairs or alterations.

(b) Inventory disposal schedules. Unless disposition instructions are otherwise included in this contract, the Contractor shall complete the Plant Clearance Inventory Schedule using the Plant Clearance capability of the Government Furnished Property (GFP) Module of the Procurement Integrated Enterprise Environment (PIEE), an electronic equivalent of the SF form 1428, Inventory Disposal Schedule. Users may register for access and obtain training on the PIEE home page <https://wawf.eb.mil/piee-landing>.

(1) The Plant Clearance Inventory Schedule requires the following:

(i) If known, the applicable Federal Supply Code (FSC) for all items, except items in scrap condition.

(ii) If known, the manufacturer name for all aircraft components under Federal Supply Group (FSG) 16 or 17 and FSCs 2620, 2810, 2915, 2925, 2935, 2945, 2995, 4920, 5821, 5826, 5841, 6340, and 6615.

(iii) The manufacturer name, make, model number, model year, and serial number for all aircraft under FSCs 1510 and 1520.

(iv) Appropriate Federal Condition Codes. See Appendix 2.5 of Volume 2 of DLM 4000.25-2, Supply Standards and Procedures, edition in effect as of the date of this contract. Information on Federal Condition Codes can be obtained at <https://www.dla.mil/Portals/104/Documents/DLMS/manuals/dlm/v2/Volume2Change13Files.pdf>.

(2) If the schedules are acceptable, the plant clearance officer shall confirm acceptance in the GFP Module Plant Clearance capability, which will transmit an acceptance email to the contractor. The electronic acceptance is equivalent to the DD Form 1637, Notice of Acceptance of Inventory.

(c) Proceeds from sales of surplus property. Unless otherwise provided in the contract, the proceeds of any sale, purchase, or retention shall be—

- (1) Forwarded to the Contracting Officer;
- (2) Credited to the Government as part of the settlement agreement;
- (3) Credited to the price or cost of the contract; or
- (4) Applied as otherwise directed by the Contracting Officer.

(d) Demilitarization, mutilation, and destruction. If demilitarization, mutilation, or destruction of contractor inventory is required, the Contractor shall demilitarize, mutilate, or destroy contractor inventory, in accordance with the terms and conditions of the contract and consistent with Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. The plant clearance officer may authorize the purchaser to demilitarize, mutilate, or destroy as a condition of sale provided the property is not inherently dangerous to public health and safety.

(e) Classified Contractor inventory. The Contractor shall dispose of classified contractor inventory in accordance with applicable security guides and regulations or as directed by the Contracting Officer.

(f) Inherently dangerous Contractor inventory. Contractor inventory dangerous to public health or safety shall not be disposed of unless rendered innocuous or until adequate safeguards are provided.

(g) Contractor inventory located in foreign countries. Consistent with contract terms and conditions, property disposition shall be in accordance with foreign and U.S. laws and regulations, including laws and regulations involving export controls, host nation requirements, Final Governing Standards, and Government-to-Government agreements. The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.

(h) Disposal of scrap.

(1) Contractor with scrap procedures. (i) The Contractor shall include within its property management procedure, a process for the accountability and management of Government-owned scrap. The process shall, at a minimum, provide for the effective and efficient disposition of scrap, including sales to scrap dealers, so as to minimize costs, maximize sales proceeds, and, contain the necessary internal controls for mitigating the improper release of non-scrap property. (ii) The Contractor may commingle Government and contractor-owned scrap and provide routine disposal of scrap, with plant clearance officer concurrence, when determined to be effective and efficient.

(2) Scrap warranty. The plant clearance officer may require the Contractor to secure from scrap buyers a DD Form 1639, Scrap Warranty.

(i) Sale of surplus Contractor inventory. (1) The Contractor shall conduct sales of contractor inventory (both useable property and scrap) in accordance with the requirements of this contract and plant clearance officer direction. (2) Any sales contracts or other documents transferring title shall include the following statement:

“The Purchaser certifies that the property covered by this contract will be used in (name of country). In the event of resale or export by the Purchaser of any of the property, the Purchaser agrees to obtain the appropriate U.S. and foreign export or re-export license approval.”

(j) Restrictions on purchase or retention of Contractor inventory. (1) The Contractor may not knowingly sell the inventory to any person or that person's agent, employee, or household member if that person—

(i) Is a civilian employee of the DoD or the U.S. Coast Guard;

(ii) Is a member of the armed forces of the United States, including the U.S. Coast Guard;

or

(iii) Has any functional or supervisory responsibilities for or within the DoD's property disposal/disposition or plant clearance programs or for the disposal of contractor inventory.

(2) The Contractor may conduct Internet-based sales, to include use of a third party.

(3) If the Contractor wishes to bid on the sale, the Contractor or its employees shall submit bids to the plant clearance officer prior to soliciting bids from other prospective bidders.

(4) The Contractor shall solicit a sufficient number of bidders to obtain adequate competition. Informal bid procedures shall be used, unless the plant clearance officer directs otherwise. The Contractor shall include in its invitation for bids, the sales terms and conditions provided by the plant clearance officer.

(5) The Contractor shall solicit bids at least 15 calendar days before bid opening to allow adequate opportunity to inspect the property and prepare bids.

(6) For large sales, the Contractor may use summary lists of items offered as bid sheets with detailed descriptions attached.

(7) In addition to mailing or delivering notice of the proposed sale to prospective bidders, the Contractor may (when the results are expected to justify the additional expense) display a notice of the proposed sale in appropriate public places, e.g., publish a sales notice on the Internet in appropriate trade journals or magazines and local newspapers.

(8) The plant clearance officer or representative will witness the bid opening. The Contractor shall submit, either electronically or manually, two copies of the bid abstract.

(9) The following terms and conditions shall be included in sales contracts involving the demilitarization, mutilation, or destruction of property:

(i) Demilitarization, mutilation, or destruction on Contractor or subcontractor premises. Item(s) \_\_\_ require demilitarization, mutilation, or destruction by the Purchaser. Insert item number(s) and specific demilitarization, mutilation, or destruction requirements for item(s) shown in Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(ii) Demilitarization, mutilation, or destruction off Contractor or subcontractor premises.

(A) Item(s) \_\_\_ require demilitarization, mutilation, or destruction by the Purchaser. Insert item number(s) and specific demilitarization, mutilation, or destruction requirements for item(s) shown in Defense Demilitarization Manual, DoDM 4160.28-M, edition in effect as of the date of this contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(B) Property requiring demilitarization shall not be removed, and title shall not pass to the Purchaser, until demilitarization has been accomplished and verified by a Government representative. Demilitarization will be accomplished as specified in the sales contract. Demilitarization shall be witnessed and verified by a Government representative using DRMS Form 145 or equivalent.

(C) The Purchaser agrees to assume all costs incident to the demilitarization and to restore the working area to its present condition after removing the demilitarized property.

(iii) Failure to demilitarize. If the Purchaser fails to demilitarize, mutilate, or destroy the property as specified in the contract, the Contractor may, upon giving 10 days written notice from date of mailing to the Purchaser—

(A) Repossess, demilitarize, and return the property to the Purchaser, in which case the Purchaser hereby agrees to pay to the Contractor, prior to the return of the property, all costs incurred by the Contractor in repossessing, demilitarizing, and returning the property;

(B) Repossess, demilitarize, and resell the property, and charge the defaulting Purchaser with all costs incurred by the Contractor. The Contractor shall deduct these costs from the purchase price and refund the balance of the purchase price, if any, to the Purchaser. In the event the costs exceed the purchase price, the defaulting Purchaser hereby agrees to pay these costs to the Contractor; or

(C) Repossess and resell the property under similar terms and conditions. In the event this option is exercised, the Contractor shall charge the defaulting Purchaser with all costs incurred by the Contractor. The Contractor shall deduct these costs from the original purchase price and refund the balance of the purchase price, if any, to the defaulting Purchaser. Should the excess costs to the Contractor exceed the purchase price, the defaulting Purchaser hereby agrees to pay these costs to the Contractor.

(End of clause)

## FAR CLAUSES

**52.203-13 CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (NOV 2021)** *(Applies if this Contract exceeds the threshold specified in FAR 3.1004(b)(1) on the date of this Contract and has a period of performance of more than 120 days. Disclosures made under this clause shall be made directly to the Government entities identified in the clause)*

**52.204-21 Basic Safeguarding of Covered Contractor Information Systems (NOV 2021)** *(Applies unless Seller is furnishing commercially available off-the-shelf items.)*

**52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)** *(Note 4 applies in paragraph (b). Reports required by this clause will be made to LOCKHEED MARTIN.)*

**52.204-23 CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (NOV 2021)** *(Seller shall provide Lockheed Martin copies of any reports provided under this clause which relate to the performance of this contract.)*

**52.209-6 PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (NOV 2021)** (*Applies if this Contract exceeds the threshold in FAR 9.405-2(b). Does not apply if this contract is for commercial off the shelf items. Copies of notices provided by Seller to the Contracting Officer shall be provided to Lockheed Martin.*)

**52.215-11 (DEV) PRICE REDUCTION FOR DEFECTIVE CERTIFIED COST OR PRICING DATA-- MODIFICATIONS (DEVIATION 2022-O0001) (OCT 2021)** (*Applies if modifications to the subcontract involving a pricing adjustment expected to exceed \$2 million.*)

**52.215-12 (DEV) SUBCONTRACTOR CERTIFIED COST OR PRICING DATA (DEVIATION 2022-O0001) (OCT 2021)**

**52.215-13 (DEV) SUBCONTRACTOR CERTIFIED COST OR PRICING DATA - MODIFICATIONS (DEVIATION 2022-O0001) (OCT 2021)**

**52.215-14 ALT 1 INTEGRITY OF UNIT PRICES (NOV 2021)** (*As prescribed in 15.408(f)(2), substitute the following paragraph (b) for paragraph (b) of the basic clause: (b) The Offeror/Contractor shall also identify those supplies that it will not manufacture or to which it will not contribute significant value.*)

**52.216-16 INCENTIVE PRICE REVISION—FIRM TARGET (OCT 1997)** (*Applies if the contract type is an incentive contract with firm targets. "Contracting Officer," "contract administrative office" and "Government" mean "Lockheed Martin." Paragraph (i) is deleted. The blanks in the clause are completed with the amounts specified in the contract.*)

**52.219-9 SMALL BUSINESS SUBCONTRACTING PLAN ALTERNATE III (NOV 2021)** (*Applies if this contract exceeds the threshold at FAR 19.702(a). Does not apply if Seller is a small business concern. "Contracting Officer" means "Lockheed Martin" in paragraph (c). Seller's subcontracting plan is incorporated herein by reference.*)

**52.222-50 COMBATING TRAFFICKING IN PERSONS (NOV 2021)** (*Applies to all subcontracts and contracts with agents.)(Applies if this contract exceeds \$3,500, and is for commercial or noncommercial services (except for commercial services that are part of the purchase of a COTS item (or an item that would be a COTS item, but for minor modifications), performed by the COTS provider, and are normally provided for that COTS item); or is for construction.*)

**52.222-54 EMPLOYMENT ELIGIBILITY VERIFICATION (MAY 2022)** (*Applies in lieu of clause on the Corp Doc*)

**52.222-55 MINIMUM WAGES FOR CONTRACTOR WORKERS UNDER EXECUTIVE ORDER 14026. (JAN 2022)** (*Applies if this Contract is subject to the Service Contract Labor Standards statute or the Wage Rate Requirements (Construction) statute, and are to be performed in whole or in part in the United States. "Contracting Officer" means "Lockheed Martin."*)

**52.244-6 SUBCONTRACTS FOR COMMERCIAL ITEMS (JAN 2022)** (*Applies to all subcontracts*)  
**52.225-13, RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (FEB 2022)** (*Applies in lieu of clause on Corp Docs*)

**52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (NOV 2021)** (*Applies if Seller is a small business concern. "Government" means*



*"Lockheed Martin." This clause does not apply if Lockheed Martin does not receive accelerated payments under the prime contract. Not all agencies provide accelerated payments.)*

**52.224-01 PRIVACY ACT NOTIFICATION (APR 1984)** *(Applies when the SELLER will be required to design, develop, or operate a system of records on individuals required to accomplish an agency function.)*

**52.224-02 PRIVACY ACT (APR 1984)** *(Applies if this contract is for the design, development, or operation of such a system of records.)*

**52.227-01 AUTHORIZATION AND CONSENT ALTERNATE 1 (APR 1984)**

**52.228-03 WORKER'S COMPENSATION INSURANCE (DEFENSE BASE ACT) (JUL 2014)** *(Applies if Seller will perform work subject to the Defense Base Act 42 U.S.C. 1651 et seq.)*

**52.216-26 PAYMENTS OF ALLOWABLE COSTS BEFORE DEFINITIZATION (DEC 2002)**

**52.232-17 INTEREST (MAY 2014)** *("Government" means "Lockheed Martin.")*

**52.239-01 PRIVACY OR SECURITY SAFEGUARDS (AUG 1996)** *(Applies in Contracts for information technology which require security of information technology, and/or are for the design, development, or operation of a system of records using commercial information technology services or support services.)*

**52.243-1 CHANGES-FIXED PRICE ALTERNATE V (Apr 1984)** *("Contracting Officer" and "Government" mean "Lockheed Martin." In paragraph (a) add as subparagraph (4) "Delivery schedule." In paragraph (e) the reference to the disputes clause is deleted.)*

**52.243-2 CHANGES-COST REIMBURSEMENT (AUG 1987) ALTERNATE II (Apr 1984) ALTERNATE V (APR 1984)** *("Contracting Officer" and "Government" mean "Lockheed Martin." In paragraph (a) add as subparagraph (4) "Delivery schedule." In paragraph (d) the reference to the disputes clause is deleted.)*

**52.245-9 USE AND CHARGES (APR 2012)** *(Applies when Government property is provided under this contract. Communications with the Government under this clause will be made through Lockheed Martin.)*

**52.246-08 INSPECTION OF RESEARCH AND DEVELOPMENT COST REIMBURSEMENT (MAY 2001)** *(Applies if this Contract is for Research and Development. "Government" means "Lockheed Martin" except (1) in paragraphs (b), (c) and (d) where it means "Lockheed Martin and the Government." and (2) in paragraph (k) where the term is unchanged.)*

## **DFARS CLAUSES**

**252.204-7010 REQUIREMENT FOR CONTRACTOR TO NOTIFY DOD IF THE CONTRACTOR'S ACTIVITIES ARE SUBJECT TO REPORTING UNDER THE U.S. INTERNATIONAL ENERGY AGENCY ADDITIONAL PROTOCOL (JAN 2009)** *(Applies in Contracts that are subject to the provisions of the U.S. International Atomic Energy Agency Additional Protocol. The blank in the clause is completed with the following \_\_\_\_\_)*

**252.204-7012 (2024-O0013) SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING. (DEVIATION 2024-O0013)** (*Applies in lieu of the clause at DFARS 252.204-7012*)

SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (MAY 2024) (DEVIATION 2024-O0013)

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

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

***Compromise*** means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

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

***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 unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

***Covered defense information*** means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

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

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

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

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

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

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

***Media*** means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks,

magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

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

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

**Technical information** means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—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 Contractor shall provide adequate security on all covered contractor information systems.

To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

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

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

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

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

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

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

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

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

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (<https://www.fedramp.gov/resources/documents/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

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

(c) **Cyber incident reporting requirement.**

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

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

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

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

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

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

(e) **Media preservation and protection.** When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) **Access to additional information or equipment necessary for forensic analysis.** Upon request by DoD, the Contractor shall provide DoD with access to additional information equipment that is necessary to conduct a forensic analysis.

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

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

(i) **Use and release of contractor attributional/proprietary information not created by or for DoD.** Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD—

- (1) To entities with missions that may be affected by such information;
- (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- (3) To Government entities that conduct counterintelligence or law enforcement investigations;
- (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
- (5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) **Use and release of contractor attributional/proprietary information created by or for DoD.** Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government’s use and release of such information.

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

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

(m) **Subcontracts.** The Contractor shall—

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

(2) Require subcontractors to—

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

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

(End of clause)

**252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (JAN 2021)** (*Copies of reports provided by Seller under this clause will be provided to Lockheed Martin.*)

**252.208-7000 INTENT TO FURNISH PRECIOUS METALS AS GOVERNMENT FURNISHED MATERIAL (DEC 1991)** (*Applies if this contract involves precious metals.*)

**252.209-7009 ORGANIZATIONAL CONFLICT OF INTEREST MAJOR DEFENSE ACQUISITION PROGRAM (OCT 2015)**

**252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (MAR 2022)**

**252.217-7026 IDENTIFICATION OF SOURCES OF SUPPLY (NOV 1995)** *(The information required by this clause is limited to the identification of those items procured from lower tier sources where Contractor will provide those items as separate end items to Lockheed Martin. Items which are included as components of end items delivered by Contractor to Lockheed Martin do not need to be identified.)*

**252.219-7004 SMALL BUSINESS SUBCONTRACTING PLAN (TEST PROGRAM) (DEC 2022)**

**252.225-7001 BUY AMERICAN AND BALANCE OF PAYMENTS PROGRAM (JUN 2022)  
ALTERNATE 1 (JUN 2022)**

**252.225-7012 PREFERENCE FOR CERTAIN DOMESTIC COMMODITIES (APR 2022)**

**252.225-7013 DUTY FREE ENTRY (DEVIATION 2020-O0019) (MAR 2022)**

**252.225-7032 WAIVER OF UNITED KINGDOM LEVIES EVALUATION OF OFFERS (APR 2003)** *(Applies if Seller is a United Kingdom firm. "Contracting Officer means "Lockheed Martin.")*

**252.225-7036 BUY AMERICAN FREE TRADE AGREEMENTS BALANCE OF PAYMENTS PROGRAM (DEVIATION 2020-O0019) (MAR 2022) ALT I (MAR 2022)**

**252.227-7013 RIGHTS IN TECHNICAL DATA--OTHER THAN COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES (MAR 2023)**

**252.227-7015 TECHNICAL DATA COMMERCIAL ITEMS ALTERNATE 1 (MAR 2022)**

**252.227-7017 IDENTIFICATION AND ASSERTION OF USE, RELEASE, OR DISCLOSURE RESTRICTIONS (JAN 2023)**

**252.227-7037 VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (DEC 2022)**

**252.234-7003 NOTICE OF COST AND SOFTWARE DATA REPORTING SYSTEM (NOV 2014)** *(Applies if Contract exceeds \$50,000,000.)*

**252.237-7010 PROHIBITION ON INTERROGATION OF DETAINEES BY CONTRACTOR PERSONNEL (JUN 2013)** *(Applies if Contract requires SELLER personnel to interact with detainees in the course of their duties.)*

**252.239-7000 PROTECTION AGAINST COMPROMISING EMANATIONS (OCT 2019)** *(Applies if the Seller performs classified work. "Contracting Officer" means "Lockheed Martin." "Government" means "Lockheed Martin and the Government" in paragraphs (c) and (d).)*

**252.239-7001 INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION (JAN 2008)** *(Applies if Seller personnel accesses DoD information systems.)*

**252.239-7010 CLOUD COMPUTING RESOURCES (SEP 2022)** *(Applies if Contract involves cloud services.)*

**252.239-7016 TELECOMMUNICATIONS SECURITY EQUIPMENT, DEVICES, TECHNIQUES, AND SERVICES (DEC 1991)** *(Applies if Contract requires securing telecommunications.)*

**252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2022)** (*Applies if the contract is over \$150,000. "Government" means "Lockheed Martin"*)

**252.245-7001 TAGGING, LABELING, AND MARKING OF GOVERNMENT FURNISHED PROPERTY (APR 2012)** (*Applies when the items furnished by the Seller will be subject to serialized tracking.*)

**252.246-7001 WARRANTY OF DATA BASIC (MAR 2014)** (*Applies in the Contract if data will be acquired from the Contractor. "Government" means "Lockheed Martin or the Government." "Contracting Officer" means "Lockheed Martin." The last sentence in paragraph (b) is changed to read as follows: The warranty period shall extend for three years after completion of delivery of the data to Lockheed Martin, or if the data is delivered to the Government, either by Lockheed Martin or Seller, the warranty period shall extend for three years after delivery to the Government.*)