AWARD/CONTRACT J

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) ▶ | RATING | **PAGE 1 OF 11**

2. CONTRACT *(Proc. Inst. Ident.)* NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
SPE3S1-18-D-Z112	2018 APR 13	1000054852

5. ISSUED BY	CODE SPE3S1	6. ADMINISTERED BY (*If other than Item 5*)	CODE S3605A
DLA TROOP SUPPORT SUBSISTENCE SUPPLY CHAIN 700 ROBBINS AVENUE PHILADELPHIA PA 19111-5096 USA Local Admin: Matthew Conroy DMC0025 Tel: DSN-444-2183 Email: Matthew.Conroy@dla.mil		DCMA DAYTON BUILDING 30 AREA A 1725 VAN PATTON DR WRIGHT PATTERSON AFB OH 45433-5302 USA Criticality: PAS: None	

7. NAME AND ADDRESS OF CONTRACTOR (*No., street, city, county, State and ZIP Code*)	8. DELIVERY	
SO-PAK-CO, INC. DBA SOPAKCO PACKAGING 118 S Cypress St MULLINS SC 29574-3004 USA	[X] FOB ORIGIN [ ] OTHER (*See below*) 9. DISCOUNT FOR PROMPT PAYMENT Net 30 (Do not Use)	
CODE 6D623 FACILITY CODE	10. SUBMIT INVOICES *(4 copies unless otherwise specified)* TO THE ADDRESS SHOWN IN ▶	ITEM 12

11. SHIP TO/MARK FOR	CODE	12. PAYMENT WILL BE MADE BY	CODE SL4701
SEE SCHEDULE, DO NOT SHIP TO ADDRESS ON THIS PAGE		DEF FIN AND ACCOUNTING SVC BSM P O BOX 182317 COLUMBUS OH 43218-2317 USA	

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
[ ] 10 U.S.C. 2304(c) [ ] 41 U.S.C. 253(c)	

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	See Schedule	375000.000			
				15G. TOTAL AMOUNT OF CONTRACT ▶	[redacted]

16. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE	
X	A	SOLICITATION/CONTRACT FORM	1
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2
	C	DESCRIPTION/SPECS./WORK STATEMENT	
	D	PACKAGING AND MARKING	
	E	INSPECTION AND ACCEPTANCE	
	F	DELIVERIES OR PERFORMANCE	
	G	CONTRACT ADMINISTRATION DATA	
	H	SPECIAL CONTRACT REQUIREMENTS	

(X)	SEC.	DESCRIPTION	PAGE(S)
		PART II - CONTRACT CLAUSES	
X	I	CONTRACT CLAUSES	4
		PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	J	LIST OF ATTACHMENTS	11
		PART IV - REPRESENTATIONS AND INSTRUCTIONS	
	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. [ ] CONTRACTOR'S NEGOTIATED AGREEMENT *(Contractor is required to sign this document and return* 1 *copies to issuing office.)* Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (*Attachments are listed herein.*)

18. [ ] SEALED-BID AWARD *(Contractor is not required to sign this document.)* Your bid on Solicitation Number _____, including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)

19A. NAME AND TITLE OF SIGNER *(Type or Print)*	20A. NAME OF CONTRACTING OFFICER
	Harry Streibich HARRY.STREIBICH@DLA.MIL PSPTR01

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
BY _____ *(Signature of person authorized to sign)*		BY _____ *(Signature of Contracting Officer)*	2018 APR 13

SECTION B - SUPPLIES OR SERVICES AND PRICES OR COSTS

PID Data - Custom Clause

The following documents are hereby incorporated by reference into this contract: Solicitation SPE3S1-17-R-0007, all solicitation amendments 0001 through 0007, and your final offer, which is being accepted by the Government to form this contract.

Tiendung Nguyen is the administrative Contracting Officer of the resultant contract.

Effective period of performance.

Tier 1: April 13, 2018 - April 12, 2019
Tier 2: April 13, 2019 - April 11, 2020
Tier 3: April 12, 2020 - April 11, 2021
Tier 4: April 12, 2021 - April 11, 2022
Tier 5: April 12, 2022 - April 11, 2023

Guaranteed Minimum quantity: 15,000 cases
Estimated quantity: 50,146 cases per year
Maximum quantity (incl. surge): 375,000 cases

Delivery Terms: F.O.B. Origin
Inspection and Acceptance Points: Origin

Place of Performance:
SOPAKCO, Inc.
118 South Cypress Street
Mullins, SC 29574-3001

Offered Prices per Tier (Does not include RNC component prices)
Tier 1 Unit Price: [redacted]
Tier 2 Unit Price:
Tier 3 Unit Price:
Tier 4 Unit Price:
Tier 5 Unit Price:

Prior to issuance of delivery orders, the First Strike Ration will be adjusted to include RNC prices. Current RNC prices as stated in their respective contracts will be applied to the current First Strike Ration Tier prices. Start and end dates for the RNC contract tiers are not on the same schedule as the First Strike Ration Tiers.

Schedule of Items:
8970-01-584-8759 First Strike Ration (FSR)

PDM:

Bagel, Lot 7184
Baked Snack Cracker, Hot and Spicy Cheese, Lot 6333
Beef Snack, Strips, BBQ, Lot 7300
Beef Snack, Strips, Teriyaki, Lot 7128
Beef Snack, Sticks, Teriyaki, Lot 7118
Beverage Base, Type II, Lemon-Lime, Lot 7100
Beverage Base, Type II, Grape, Lot 7107

CONTINUED ON NEXT PAGE

SECTION B - SUPPLIES OR SERVICES AND PRICES OR COSTS (CONTINUED)

Beverage Base, Type II, Fruit Punch, Lot 7104
Beverage Base, Type II, Lemonade, Lot 7101
Beverage Base, Type II, Tropical Punch, Lot 7103
Beverage Base, Type II, Orange, Lot 7102
Caffeinated Chocolate Pudding, Lot 7125H
Candy, Caffeinated Mints, Peppermint, Lot 16HOS
Chewing Gum, Xylitol, Peppermint, Lot 17167
Chewing Gum, Xylitol, Cinnamon, Lot 17177
Chicken, BBQ, Lot 7054A
Chicken, Garlic Herb, Lot 7214H
Chicken Chunks, Lot 7041
Chocolate Protein Shake, Lot 7202
Coffee, Lot 6258
Crackers, Plain, Lot 6328
Dairy Shake, Strawberry Banana, Lot 7109
Dairy Shake, Vanilla, Lot 7110
Dessert Bar, Mocha, Lot 6327
Dessert Bar, Chocolate Banana Nut, Lot 7096
Dessert Bar, Peanut Butter, Lot 6328
Energy Gel, Mixed Berry, Lot 7049
Filled Apple Turnover, Lot 7123
Filled Blueberry Turnover, Lot 7200
Filled Cinnamon Bun, Lot 7153
Filled French Toast, Lot 7153
Filled Snack Cracker, Cheddar, Lot 6327
Filled Snack Pretzel, Cheddar, Lot 6327
Filled Wrap, BBQ Pork, Lot 7142
FIRST STRIKE BAR® Bar, Mini, Apple-Cinnamon, Lot 7115
FIRST STRIKE BAR® Bar, Mini, Chocolate, Lot 7102
FIRST STRIKE BAR® Bar, Mini, Cran-Raspberry, Lot 7081
FIRST STRIKE BAR® Bar, Mini, Mocha, Lot 7208
Fruit, Applesauce Cinnamon, Lot 7132H
Fruit, Dried Cranberries, Lot 6308
Fruit, Raisins, Lot 6314
Gum, Caffeinated Peppermint, Lot 7054
Gum, Caffeinated Cinnamon, Lot 2/2/2022
Hand and Body Wipes, Lot 16042
Hot Sauce, Extra Hot, Lot 7151
Hot Sauce, Buffalo Style, Lot 7216
Matches, Lot 01-01601348
Nut Fruit Mix, Type II, Lot 7046
Nuts, Almonds, Smoked, Lot 7109
Re-Closeable Plastic Bag, Lot 7100
Salt, Lot G172H
Sandwich, BBQ Chicken, Lot 7110
Sandwich, Beef Nacho, Lot 7107
Sandwich, Honey BQQ Beef, Lot 7153
Sandwich, Pepperoni, Lot 7102
Sandwich, Italian Style, Lot 7156
Snack Bread, Italian, Single, Lot 7108
Snack Bread, Multigrain, Single, Lot 7114
Snack, Corn Kernels, Plain, Lot 7003
Snack, Corn Kernels, BBQ, Lot 7004

CONTINUED ON NEXT PAGE

SECTION B - SUPPLIES OR SERVICES AND PRICES OR COSTS (CONTINUED)

Snack, Pretzels, Sticks, Lot 6324A
Spoon (Ability One Mandatory Item)
Spread, Cheddar Potato Bacon, Lot 7956
Sugar, Lot G172H
Toaster Pastry, Brown Sugar Cinnamon, Whole Wheat, Lot 7125
Toaster Pastry, Frosted Chocolate Chip, With Swirled or Drizzled Icing, Lot 7203
Toilet Tissue (Ability One Mandatory Item)
Trail Mix, Recovery, Lot 7138
Tuna, Albacore, Lot 7048A
Tuna, Lemon Pepper, Lot 7047A
Tuna, Sweet and Spicy, Lot 7047B
Turkey Snack, Smoked, Lot 7139

PDMs for Filled Wrap, Mexican Beef and Sandwich, Breakfast Bacon Cheddar must be submitted and accepted prior to production. Refer to Amendment 0006 of SPE3S1-17-R-0007 for further details.

SECTION I - CONTRACT CLAUSES

52.204-19 INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014) FAR

52.222-26 EQUAL OPPORTUNITY (SEP 2016) FAR

252.211-7006 RADIO FREQUENCY IDENTIFICATION (SEP 2011) DFARS

****

(b)(1) Except as provided in paragraph (b)(2) of this clause, the Contractor shall affix passive RFID tags, at the case- and palletized-unit-load packaging levels, for shipments of items that-

(i) Are in any of the following classes of supply, as defined in DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation, AP1.1.11:

(A) Subclass of Class I - Packaged operational rations.

(B) Class II - Clothing, individual equipment, tentage, organizational tool kits, hand tools, and administrative and housekeeping supplies and equipment.

(C) Class IIIP - Packaged petroleum, lubricants, oils, preservatives, chemicals, and additives.

(D) Class IV - Construction and barrier materials.

(E) Class VI - Personal demand items (non-military sales items).

(F) Subclass of Class VIII - Medical materials (excluding pharmaceuticals, biologicals, and reagents - suppliers should limit the mixing of excluded and non-excluded materials).

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(G) Class IX - Repair parts and components including kits, assemblies and subassemblies, reparable and consumable items required for maintenance support of all equipment, excluding medical-peculiar repair parts; and
(ii) Are being shipped to one of the locations listed at http://www.acq.osd.mil/log/rfid/ or to-
(A) A location outside the contiguous United States when the shipment has been assigned Transportation Priority 1, or to-
(B) The following location(s) deemed necessary by the requiring activity:

Contract Line, Subline, or Exhibit Line Item Number	Location Name	City	State	DoDAAC

(2) The following are excluded from the requirements of paragraph (b)(1) of this clause:
(i) Shipments of bulk commodities.
(ii) Shipments to locations other than Defense Distribution Depots when the contract includes the clause at FAR 52.213-1, Fast Payment Procedures.
(c) The Contractor shall-
(1) Ensure that the data encoded on each passive RFID tag are globally unique (i.e., the tag ID is never repeated across two or more RFID tags and conforms to the requirements in paragraph (d) of this clause;
(2) Use passive tags that are readable; and
(3) Ensure that the passive tag is affixed at the appropriate location on the specific level of packaging, in accordance with MIL-STD-129 (Section 4.9.2) tag placement specifications.
(d) Data syntax and standards. The Contractor shall encode an approved RFID tag using the instructions provided in the EPC™ Tag Data Standards in effect at the time of contract award. The EPC™ Tag Data Standards are available at http://www.epcglobalinc.org/standards/.
(1) If the Contractor is an EPCglobal™ subscriber and possesses a unique EPC™ company prefix, the Contractor may use any of the identifiers and encoding instructions described in the most recent EPC™ Tag Data Standards document to encode tags.
(2) If the Contractor chooses to employ the DoD identifier, the Contractor shall use its previously assigned Commercial and Government Entity (CAGE) code and shall encode the tags in accordance with the tag identifier details located at http://www.acq.osd.mil/log/rfid/tag_data.htm. If the Contractor uses a third-party packaging house to encode its tags, the CAGE code of the third-party packaging house is acceptable.
(3) Regardless of the selected encoding scheme, the Contractor with which the Department holds the contract is responsible for ensuring that the tag ID encoded on each passive RFID tag is globally unique, per the requirements in paragraph (c)(1).
(e) Advance shipment notice. The Contractor shall use Wide Area WorkFlow (WAWF), as required by DFARS 252.232-7003, Electronic Submission of Payment Requests, to electronically submit advance shipment notice(s) with the RFID tag ID(s) (specified in paragraph (d) of this clause) in advance of the shipment in accordance with the procedures at https://wawf.eb.mil/.
(End of clause)

52.222-37 EMPLOYMENT REPORTS ON VETERANS (FEB 2016) FAR

52.244-6 SUBCONTRACTS FOR COMMERCIAL ITEMS (JAN 2017) FAR

252.225-7002 QUALIFYING COUNTRY SOURCES AS SUBCONTRACTORS (DEC 2016) DFARS

52.223-11 OZONE-DEPLETING SUBSTANCES AND HIGH GLOBAL WARNING POTENTIAL HYDROFLUOROCARBONS (JUN 2016) FAR

As prescribed in 23.804(a)(1), insert the following clause:

Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016)

(a) *Definition*. As used in this clause -
"Global warming potential" means how much a given mass of a chemical contributes to global warming over a given time period compared to the same mass of carbon dioxide. Carbon dioxide's global warming potential is defined as 1.0.
"High global warming potential hydrofluorocarbons" means any hydrofluorocarbons in a particular end use for which EPA's Significant New Alternatives

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

Policy (SNAP) program has identified other acceptable alternatives that have lower global warming potential. The SNAP list of alternatives is found at 40 CFR Part 82 subpart G with supplemental tables of alternatives available at (http://www.epa.gov/snap/).

"Hydrofluorocarbons" means compounds that only contain hydrogen, fluorine, and carbon.

"Ozone-depleting substance," means any substance the Environmental Protection Agency designates in 40 CFR Part 82 as -

(1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or

(2) Class II, including, but not limited to, hydrochlorofluorocarbons.

(b) The Contractor shall label products that contain or are manufactured with ozone-depleting substances in the manner and to the extent required by 42 U.S. C. 7671j (b), (c), (d), and (e) and 40 CFR part 82, subpart E, as follows:

WARNING

Contains (or manufactured with, if applicable) *_ , a substance(s) which harm(s) public health and environment by destroying ozone in the upper atmosphere.

* The Contractor shall insert the name of the substance(s).

(c) *Reporting*. For equipment and appliances that normally each contain 50 or more pounds of hydrofluorocarbons or refrigerant blends containing hydrofluorocarbons, the Contractor shall -

(1) Track on an annual basis, between October 1 and September 30, the amount in pounds of hydrofluorocarbons or refrigerant blends containing hydrofluorocarbons contained in the equipment and appliances delivered to the Government under this contract by -

(i) Type of hydrofluorocarbon (*e.g.*, HFC-134a, HFC-125, R-410A, R-404A, *etc.*);

(ii) Contract number; and

(iii) Equipment/appliance;

(2) Report that information to the Contracting Officer for FY16 and to www.sam.gov, for FY17 and after -

(i) Annually by November 30 of each year during contract performance; and

(ii) At the end of contract performance.

(d) The Contractor shall refer to EPA's SNAP program (available at http://www.epa.gov/snap) to identify alternatives. The SNAP list of alternatives is found at 40 CFR part 82 subpart G with supplemental tables available at http://www.epa.gov/snap.

(End of clause)

252.225-7001 BUY AMERICAN AND BALANCE OF PAYMENTS PROGRAM—BASIC (DEC 2016) DFARS

52.225-1 BUY AMERICAN - SUPPLIES (MAY 2014) FAR

252.225-7012 PREFERENCE FOR CERTAIN DOMESTIC COMMODITIES (DEC 2016) DFARS

252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016) DFARS

As prescribed in 204.7304(a), use the following provision:

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

"Controlled technical information," "covered contractor information system," "covered defense information," "cyber incident," "information system," and "technical information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2) --

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of --

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(A) Why a particular security requirement is not applicable; or

(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016) DFARS

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

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

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered defense information” means unclassified information that -

(1) Is -

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(2) Falls in any of the following categories:

(i) Controlled technical information.

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

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

(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

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

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

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

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

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

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

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

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

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

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

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

(End of clause)

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016) DFARS

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

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

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

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

“Contractor information system” means an information system belonging to, or operated by or for, the Contractor.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

“Covered defense information” means unclassified information that -

(i) Is --

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or

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

(ii) Falls in any of the following categories:

(A) *Controlled technical information*.

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

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

(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

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

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

“Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system.

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

“Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this 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 for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall -

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum -

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

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

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

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause -

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,” http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD 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; or

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

(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement.*

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

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

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

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

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

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

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

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

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

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

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

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

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

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (“recipient”) that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

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

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

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

(m) *Subcontracts*. The Contractor shall -

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

(2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at http://dibnet.dod.mil and the prime Contractor. This includes providing the incident report number, automatically assigned by DoD, to the prime Contractor (or

CONTINUED ON NEXT PAGE

SECTION I - CONTRACT CLAUSES (CONTINUED)

next higher-tier subcontractor) as soon as practicable.

(End of clause)

52.223-14 TOXIC CHEMICAL RELEASE REPORTING (JUN 2014) FAR

52.232-40 PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013) FAR

52.233-3 PROTEST AFTER AWARD (AUG 1996) FAR

252.244-7000 SUBCONTRACTS FOR COMMERCIAL ITEMS AND COMMERCIAL COMPONENTS (DOD CONTRACTS) (JUN 2013) DFARS

52.246-18 WARRANTY OF SUPPLIES OF A COMPLEX NATURE (MAY 2001) FAR

****
(b) Contractor's obligations.
(1) The Contractor warrants that for [Contracting Officer shall state the specific warranty period after delivery, or the specified event whose occurrence will terminate the warranty period; e.g., the number of miles or hours of use, or combinations of any applicable events or periods of time] all supplies furnished under this contract will be free from defects in material and workmanship and will conform with all requirements of this contract; provided, however, that with respect to Government-furnished property, the Contractor's warranty shall extend only to its proper installation, unless the Contractor performs some modification or other work on the property, in which case the Contractor's warranty shall extend to the modification or other work.
****
(3) The Contracting Officer shall notify the Contractor in writing of any breach of the warranty in paragraph (b) of this clause within . [Contracting Officer shall insert specific period of time in which notice shall be given to the Contractor; e.g., “45 days after delivery of the nonconforming supplies.”; “45 days of the last delivery under this contract.”; or “45 days after discovery of the defect.”] The Contractor shall submit to the Contracting Officer a written recommendation within [Contracting Officer shall insert period of time] as to the corrective action required to remedy the breach. After the notice of breach, but not later than [Contracting Officer shall insert period within which the warranty remedies should be exercised] after receipt of the Contractor's recommendation for corrective action, the Contracting Officer may, in writing, direct correction or replacement as in paragraph (c)(1) of this clause, and the Contractor shall, notwithstanding any disagreement regarding the existence of a breach of warranty, comply with this direction. If it is later determined that the Contractor did not breach the warranty in paragraph (b)(1) of this clause, the contract price will be equitably adjusted.
(4) If supplies are corrected or replaced, the period for notification of a breach of the Contractor's warranty in paragraph (c)(3) of this clause shall be [Contracting Officer shall insert period within which the Contractor must be notified of a breach as to corrected or replaced supplies] from the furnishing or return by the Contractor to the Government of the corrected or replaced supplies or parts thereof, or, if correction or replacement is effected by the Contractor at a Government or other activity, for [Contracting Officer shall insert period within which the Contractor must be notified of a breach of warranty as to corrected or replaced supplies] thereafter.
(5) The rights and remedies of the Government provided in this clause are in addition to and do not limit any rights afforded to the Government by any other clause of the contract.
(End of clause)

252.247-7023 TRANSPORATION OF SUPPLIES BY SEA (APR 2014) DFARS

52.253-1 COMPUTER GENERATED FORMS (JAN 1991) FAR

SECTION J - LIST OF ATTACHMENTS

List of Attachments

File Name	Description
ATTACH_	SPE3S1-18-D-Z112 Bilateral Sigantures.pdf