

<b>AWARD/CONTRACT J</b>		1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		RATING		PAGE 1 OF 15 PAGES	
2. CONTRACT (Proc. Inst. Ident.) NO. SPE3S1-17-D-Z125		3. EFFECTIVE DATE 2017 APR 07		4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 1000052192			
5. ISSUED BY DLA TROOP SUPPORT SUBSISTENCE SUPPLY CHAIN 700 ROBBINS AVENUE PHILADELPHIA PA 19111-5096 USA Local Admin: Stephen Chenoweth PEPCDDB Tel: 215-737-7438 Email: stephen.chenoweth@dla.mil		CODE SPE3S1		6. ADMINISTERED BY (If other than Item 5) DCMA ATLANTA 2300 LAKE PARK DRIVE SMYRNA GA 30080-0000 USA Criticality: PAS: None		CODE S1103A	
7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, State and ZIP Code)  ADAM CLINGERMAN DBA ABC VENTURES ABC VENTURES 2411 OLD CROW CANYON RD # 105 SAN RAMON CA 94583-1240 USA				8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)			
				9. DISCOUNT FOR PROMPT PAYMENT  Net 30 (Do not Use)			
				10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN  ITEM 12			
CODE 1VR02		FACILITY CODE					
11. SHIP TO/MARK FOR  SEE SCHEDULE, DO NOT SHIP TO ADDRESS ON THIS PAGE		CODE		12. PAYMENT WILL BE MADE BY DEF FIN AND ACCOUNTING SVC BSM P O BOX 182317 COLUMBUS OH 43218-2317 USA		CODE SL4701	
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:  <input type="checkbox"/> 10 U.S.C. 2304(c) <input type="checkbox"/> 41 U.S.C. 253(c)				14. ACCOUNTING AND APPROPRIATION DATA			
15A. ITEM NO.	15B. SUPPLIES/SERVICES		15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT	
	See Schedule		18937500.000				
<b>15G. TOTAL AMOUNT OF CONTRACT</b>						\$3,123,953.70	
<b>16. TABLE OF CONTENTS</b>							
(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM	1		I	CONTRACT CLAUSES	
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
	C	DESCRIPTION/SPECS./WORK STATEMENT			J	LIST OF ATTACHMENTS	
	D	PACKAGING AND MARKING		PART IV - REPRESENTATIONS AND INSTRUCTIONS			
	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	F	DELIVERIES OR PERFORMANCE			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD	
	H	SPECIAL CONTRACT REQUIREMENTS					
<b>CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE</b>							
17. <input checked="" type="checkbox"/> 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. <input type="checkbox"/> 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 James Lecollier JAMES.LECOLLIER@DLA.MIL PSPTRC1			
19B. NAME OF CONTRACTOR  BY _____ (Signature of person authorized to sign)		19C. DATE SIGNED		20B. UNITED STATES OF AMERICA  BY (Signature of Contracting Officer)		20C. DATE SIGNED 2017 APR 07	

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

Effective period of performance.

Tier 1: April 7, 2017 - April 6, 2018  
Tier 2: April 7, 2018 - April 6, 2019  
Tier 3: April 7, 2019 - April 6, 2020  
Tier 4: April 7, 2020 - April 6, 2021  
Tier 5: April 7, 2021 - April 6, 2022

Estimated quantity: 7,575,000  
Guaranteed Minimum Quantity: 6,312,500

Schedule of Items:  
8950-01-527-8387 - Fat Free Mayonnaise

Pricing terms: Firm-Fixed-Price:  
Fat Free Mayonnaise

Tier 1 Unit Pricing  
Fat Free Mayonnaise      \$0.1324

Tier 2 Unit Pricing  
Fat Free Mayonnaise      \$0.1344

Tier 3 Unit Pricing  
Fat Free Mayonnaise      \$0.1364

Tier 4 Unit Pricing  
Fat Free Mayonnaise      \$0.1385

Tier 5 Unit Pricing  
Fat Free Mayonnaise      \$0.1405

PDM:  
Fat Free Mayonnaise Lot No 7013

Delivery terms: F.O.B. Destination.  
The Wornick Company  
4700 Creek Road  
Cincinnati, OH 45242

SOPAKCO Packaging  
118 South Cypress Street  
Mullins, SC 29574

AmeriQual Group LLC  
18200 Highway 41 North  
Evansville, Indiana 47725

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 3 OF 15 PAGES
--------------------	--	--------------------

Inspection: Origin and acceptance: Destination

Inspection Office:  
USDA, AMS, Dairy Programs, DGB  
2150 Western Court, Suite 100  
Lisle, IL 60532  
(630) 297-4740 Voice

DLA Troop Support will establish Rations National Contracts (RNC) with component manufacturers, and will authorize the MRE assemblers to order directly from the national contracts in lieu of DLA providing the components as GFM. The Rations National Contracts will establish the component prices, but the assemblers, Wornick, SOPAKCO, and AmeriQual, will order and pay for the material directly. The assemblers will have full control over when to order, how much to order, and have full responsibility for the supply chain and inventory. See FAR 52.216-19 - Order limitations for more information.  
Note: Terms and conditions of the individual component contract shall prevail in case of a conflict between the MRE assembly contract(s) and this individual component contract.

THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED BY REFERENCE:  
252.211-7006 Passive Radio Frequency Identification (JUN 2016) DFARS  
52.222-26 -- Equal Opportunity. (Sept 2016)  
252.225-7002 Qualifying Country Sources as Subcontractors. (Aug 2016) DFARS  
52.244-6 Subcontracts for Commercial Items (SEPT 2016)  
52.204-7 System for Award Management (Oct 2016)  
52.204-13 - System for Award Management Maintenance (Oct 2016)  
252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)  
252.225-7012 PREFERENCE FOR CERTAIN DOMESTIC COMMODITIES (AUG 2016)  
252.211-7006 RADIO FREQUENCY IDENTIFICATION (JUN 2016)

THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED BY FULL TEXT:  
52.223-11 -- Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons.

As prescribed in 23.804(a), insert the following clause:  
Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016)  
(a) Definitions. 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 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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 4 OF 15 PAGES
<p>(2) Class II , including, but not limited to hydrochlorofluorocarbons.</p> <p>(b) The Contractor shall label products which 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:</p> <p>Warning</p> <p>Contains (or manufactured with, if applicable) *_____, a substance(s) which harm(s) public health and environment by destroying ozone in the upper atmosphere.</p> <p>* The Contractor shall insert the name of the substance(s).</p> <p>(c) Reporting. For equipment and appliances that normally each contain 50 or more pounds of hydrofluorocarbons or refrigerant blends containing hydrofluorocarbons, the Contractor shall-</p> <p>(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-</p> <p>(i) Type of hydrofluorocarbon (e.g., HFC-134a, HFC-125, R-410A, R-404A, etc.);</p> <p>(ii) Contract number; and</p> <p>(iii) Equipment/appliance;</p> <p>(2) Report that information to the Contracting Officer for FY16 and to <a href="http://www.sam.gov">www.sam.gov</a>, for FY17 and after00</p> <p>(i) Annually by November 30 of each year during contract performance; and</p> <p>(ii) At the end of contract performance.</p> <p>(d) The Contractor shall refer to EPA's SNAP program (available at <a href="http://www.epa.gov/snap">http://www.epa.gov/snap</a> ) to identify alternatives. The SNAP list of alternatives is found at 40 CFR part 82, subpart G, with supplemental tables available at <a href="http://www.epa.gov/snap">http://www.epa.gov/snap</a> .</p> <p>(End of Clause)</p> <p>252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.</p> <p>As prescribed in 204.7304(a), use the following provision:</p> <p>COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)</p> <p>(a) Definitions. As used in this provision-</p> <p>"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.</p> <p>(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.</p> <p>(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)-</p>		
CONTINUED ON NEXT PAGE		

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 5 OF 15 PAGES
--------------------	--	--------------------

(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—

(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.

As prescribed in 204.7304(b), use the following clause:

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

(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 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.

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

"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.

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) 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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 6 OF 15 PAGES
--------------------	--	--------------------

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.
- (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.  
As prescribed in 204.7304(c), use the following clause:

**SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)**

- (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.

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 7 OF 15 PAGES
--------------------	--	--------------------

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

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

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

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

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

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

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

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

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

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

(2) For covered contractor information systems that are not part of an IT service 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" (available via the internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at [osd.dibcsia@mail.mil](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

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 8 OF 15 PAGES
--------------------	--	--------------------

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

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

(c) Cyber incident reporting requirement.

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

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

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

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

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

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

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

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

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

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



CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 9 OF 15 PAGES
--------------------	--	--------------------

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

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

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

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

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

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

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

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

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

(m) Subcontracts. The Contractor shall—

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

(2) Require subcontractors to—

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

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

(End of clause)

252.225-7001 Buy American and Balance of Payments Program.

Basic. As prescribed in 225.1101(2)(i) and (2)(ii), use the following clause:

BUY AMERICAN AND BALANCE OF PAYMENTS PROGRAM-BASIC (AUG 2016)

(a) Definitions. As used in this clause#

"Commercially available off-the-shelf (COTS) item"—

(i) Means any item of supply (including construction material) that is—

(A) A commercial item (as defined in paragraph (1) of the definition of "commercial item" in section 2.101 of the Federal Acquisition Regulation);

(B) Sold in substantial quantities in the commercial marketplace; and

(C) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(ii) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 10 OF 15 PAGES
--------------------	--	---------------------

"Component" means an article, material, or supply incorporated directly into an end product.

"Domestic end product" means—

- (i) An unmanufactured end product that has been mined or produced in the United States; or
- (ii) An end product manufactured in the United States if—
  - (A) The cost of its qualifying country components and its components that are mined, produced, or manufactured in the United States exceeds 50 percent of the cost of all its components. The cost of components includes transportation costs to the place of incorporation into the end product and U.S. duty (whether or not a duty-free entry certificate is issued). Scrap generated, collected, and prepared for processing in the United States is considered domestic. A component is considered to have been mined, produced, or manufactured in the United States (regardless of its source in fact) if the end product in which it is incorporated is manufactured in the United States and the component is of a class or kind for which the Government has determined that—
    - (1) Sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States; or
    - (2) It is inconsistent with the public interest to apply the restrictions of the Buy American statute; or
  - (B) The end product is a COTS item.

"End product" means those articles, materials, and supplies to be acquired under this contract for public use.

"Foreign end product" means an end product other than a domestic end product.

"Qualifying country" means a country with a reciprocal defense procurement memorandum of understanding or international agreement with the United States in which both countries agree to remove barriers to purchases of supplies produced in the other country or services performed by sources of the other country, and the memorandum or agreement complies, where applicable, with the requirements of section 36 of the Arms Export Control Act (22 U.S.C. 2776) and with 10 U.S.C. 2457. Accordingly, the following are qualifying countries:

- Australia
- Austria
- Belgium
- Canada
- Czech Republic
- Denmark
- Egypt
- Finland
- France
- Germany
- Greece
- Israel
- Italy
- Japan
- Luxembourg
- Netherlands
- Norway
- Poland
- Portugal
- Slovenia
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom of Great Britain and Northern Ireland.

"Qualifying country component" means a component mined, produced, or manufactured in a qualifying country.

"Qualifying country end product" means—

- (i) An unmanufactured end product mined or produced in a qualifying country; or
- (ii) An end product manufactured in a qualifying country if —
  - (A) The cost of the following types of components exceeds 50 percent of the cost of all its components:
    - (1) Components mined, produced, or manufactured in a qualifying country.

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-Z125	PAGE 11 OF 15 PAGES
<p>(2) Components mined, produced, or manufactured in the United States.</p> <p>(3) Components of foreign origin of a class or kind for which the Government has determined that sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States; or</p> <p>(B) The end product is a COTS item.</p> <p>"United States" means the 50 States, the District of Columbia, and outlying areas.</p> <p>(b) This clause implements 41 U.S.C chapter 83, Buy American. In accordance with 41 U.S.C. 1907, the component test of the Buy American statute is waived for an end product that is a COTS item (see section 12.505(a)(1) of the Federal Acquisition Regulation). Unless otherwise specified, this clause applies to all line items in the contract.</p> <p>(c) The Contractor shall deliver only domestic end products unless, in its offer, it specified delivery of other end products in the Buy American#Balance of Payments Program Certificate provision of the solicitation. If the Contractor certified in its offer that it will deliver a qualifying country end product, the Contractor shall deliver a qualifying country end product or, at the Contractor's option, a domestic end product.</p> <p>(d) The contract price does not include duty for end products or components for which the Contractor will claim duty-free entry.</p> <p><b>CONTINUED ON NEXT PAGE</b></p>		

SECTION B

SUPPLIES/SERVICES: 8950-01-527-8387

ITEM DESCRIPTION:

1 oz flex pg, CID A-A-20140, style c, type I, (for MEAL, READY-TO-EAT)  
RP001: DLA PACKAGING REQUIREMENTS FOR PROCUREMENT

RA001: THIS DOCUMENT INCORPORATES TECHNICAL AND/OR QUALITY REQUIREMENTS (IDENTIFIED BY AN 'R' OR AN 'I' NUMBER) SET FORTH IN FULL TEXT IN THE DLA MASTER LIST OF TECHNICAL AND QUALITY REQUIREMENTS FOUND ON THE WEB AT: <http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx>. FOR SIMPLIFIED ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE SOLICITATION ISSUE DATE OR THE AWARD DATE CONTROLS. FOR LARGE ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE RFP ISSUE DATE APPLIES UNLESS A SOLICITATION AMENDMENT INCORPORATES A FOLLOW-ON REVISION, IN WHICH CASE THE AMENDMENT DATE CONTROLS.

RQ011: REMOVAL OF GOVERNMENT IDENTIFICATION FROM NON-ACCEPTED SUPPLIES

IAW BASIC CID A-A-20140D  
REVISION NR D DTD 06/25/2008  
PART PIECE NUMBER:

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	8950-01-527-8387 MAYONNAISE	18,937,500.000	OZ	\$ 0.13240	\$ 2,507,325.00

PRICING TERMS: Firm Fixed Price

SUPPLIES/SERVICES: 8950-01-527-8387

CLIN	Price	Delivery (in days)
0001	\$ 132.40	0

QTY VARIANCE: PLUS 0% MINUS 0%

INSPECTION POINT: DESTINATION

ACCEPTANCE POINT: DESTINATION

FOB: DESTINATION DELIVERY DATE:

PREP FOR DELIVERY:

SHALL BE PACKAGED IN ACCORDANCE WITH ASTM D 3951.

Markings Paragraph  
When ASTM D3951, Commercial Packaging is specified, the following apply:

SECTION B

SUPPLY/SERVICE: 8950-01-527-8387 CONT'D

- ,,All Section "D" Packaging and Marking Clauses take precedence over ASTM D3951.
- ,,In addition to requirements in MIL-STD-129, when Commercial Packaging is used, the Method of Preservation for all MIL-STD-129 marking and labeling shall be "CP" Commercial Pack.
- ,,The Unit of Issue (U/I) and Quantity per Unit Pack (QUP) as specified in the contract take precedence over QUP in ASTM D3951.

GOVT USE

ITEM	PR	External		External	External	Customer RDD/ Need Ship Date
		PRLI	PR	PRLI	Material	
0001	1000052192	0001	N/A	N/A	N/A	N/A

\*\*\*\*\*

**SECTION I - CONTRACT CLAUSES**

**252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (DEC 2015) DFARS**

- (a) *Definitions.* As used in this provision—  
 “Controlled technical information,” “covered contractor information system,” and “covered defense 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, Covered Defense Information and Cyber Incident Reporting, 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 (IT) service or system operated on behalf of the Government (see 252.204-7012(b)(1)(ii))—  
 (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>), 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 is 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—  
     (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)

**SECTION J - LIST OF ATTACHMENTS**

**PRICING SHEET**

TIER	ITEM NSN	ITEM DESCRIPTION	UNIT PRICE
1	8950-01-527-8387	Fat Free Mayonnaise	\$ 0.1324
TIER	ITEM NSN	ITEM DESCRIPTION	UNIT PRICE
2	8950-01-527-8387	Fat Free Mayonnaise	\$ 0.1344
TIER	ITEM NSN	ITEM DESCRIPTION	UNIT PRICE
3	8950-01-527-8387	Fat Free Mayonnaise	\$ 0.1364
TIER	ITEM NSN	ITEM DESCRIPTION	UNIT PRICE
4	8950-01-527-8387	Fat Free Mayonnaise	\$ 0.1385
TIER	ITEM NSN	ITEM DESCRIPTION	UNIT PRICE
5	8950-01-527-8387	Fat Free Mayonnaise	\$ 0.1405

**List of Attachments**

Description	File Name
-------------	-----------

ATTACH.	SIGNED AWARD, SPE3S117DZ125.pdf
---------	------------------------------------