

AWARD/CONTRACT J	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE 1 OF 09 PAGES
	2. CONTRACT (Proc. Inst. Ident.) NO. SPE3S1-16-D-Z107	3. EFFECTIVE DATE 2015 DEC 04	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 1000018087

5. ISSUED BY DLA TROOP SUPPORT SUBSISTENCE SUPPLY CHAIN 700 ROBBINS AVENUE PHILADELPHIA PA 19111-5098 USA Local Admin: Stephen Granato PSPTRCA Tel: 216-737-3839 Fax: 216-737-3184 Email: STEPHEN.GRANATO@DLA.MIL	CODE SPE3S1	6. ADMINISTERED BY (If other than Item 5) DCMA DAYTON BUILDING 30 AREA A 1726 VAN PATTON DR WRIGHT PATTERSON AFB OH 45433-5302 USA Criticalty: PAS: None	CODE S3605A
--	-------------	--	-------------

7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, State and ZIP Code) AMERICAL GROUP, LLC DBA AMERI QUAL FOODS 18200 HIGHWAY 41 N EVANSVILLE IN 47726-8588 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
---	--

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

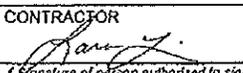
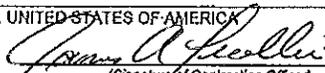
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304(c) <input type="checkbox"/> 41 U.S.C. 253(c)	14. ACCOUNTING AND APPROPRIATION DATA
---	---------------------------------------

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	See Schedule	3.000			
16G. TOTAL AMOUNT OF CONTRACT					\$1,600,000.00

(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					

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

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) Lana Lis Director of Government Sales	20A. NAME OF CONTRACTING OFFICER James Lecollier PSPTRC1
19B. NAME OF CONTRACTOR BY  (Signature of person authorized to sign)	19C. DATE SIGNED 12/4/2015
20B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)	20C. DATE SIGNED 2015 DEC 04

B-1. ITEMS TO BE SUPPLIED

WATER, DRINKING, EMERGENCY,
 NSN: 8960-01-587-6603
 Item description:
 4 oz flex pouch pg, w/centered spout
 CID A-A 20332
 Type I, size a, class 1, design c

WATER, DRINKING, EMERGENCY,
 NSN: 8960-01-485-9695
 Item description:
 4 oz flex pouch pg, w/side spout
 CID A-A 20332
 Type I, size a, class 1, design b

WATER, DRINKING, EMERGENCY,
 NSN: 8960-01-124-4543
 Item description:
 4 oz flex pouch pg, w/o spout
 CID A-A 20332
 Type I, size a, class 1, design a

This procurement is for an Indefinite Quantity Contract (IQC) with a minimum and maximum order quantity. The term of the contract will be three 12 month tier periods. The ordering period shall commence on the award date of the contract and shall continue for one calendar year thereafter (tier 1), followed by 2 subsequent tiers. Deliveries might fall outside of the effective period for any given tier.

B-2. QUANTITY REQUIREMENTS FOR EACH TIER:

<u>ITEM/NSN</u>	<u>Minimum Qty.</u>	<u>Maximum Qty.</u>
WATER, DRINKING, EMERGENCY, FLEXIBLE POUCH NSN: 8960-01-587-6603	75,000	225,000
WATER, DRINKING, EMERGENCY, FLEXIBLE POUCH NSN: 8960-01-485-9695	50,000	150,000
WATER, DRINKING, EMERGENCY, FLEXIBLE POUCH NSN: 8960-01-124-4543	175,000	525,000

Delivery will be FOB DESTINATION for all three NSNs.

There are currently 5 locations where this product will be shipped – DoDAAC in ():

- Tracy, California DDJC - (W62G2T)
- Susquehanna, Pennsylvania DDSP - (W25G1U)
- Warner Robins AFB, GA DDWG - (SW3119)
- Tinker AFB, OK DDOO - (SW3211)
- Hill, Utah DDHU – (SW3210)

1. WATER, DRINKING, EMERGENCY,
NSN: 8960-01-587-6603 (Center Spout)
Tier 1 unit price \$.57
Tier 2 unit price \$.58
Tier 3 unit price \$.59
2. WATER, DRINKING, EMERGENCY,
NSN: 8960-01-485-9695 (Side Spout)
Tier 1 unit price \$.58
Tier 2 unit price \$.59
Tier 3 unit price \$.60
3. WATER, DRINKING, EMERGENCY,
NSN: 8960-01-124-4543 (No Spout)
Tier 1 unit price \$.55
Tier 2 unit price \$.56
Tier 3 unit price \$.57

The inspection point for this contract is at Origin. The inspection will be performed by the cognizant USDA-AMS office.

The Acceptance point for this contract is at Origin.

This award consummates the contract which consists of the following documents:

Solicitation SPE3S1-14-R-0004, Amendment 0001, your original offer dated September 11, 2015 and this award/contract.

The following clause replaces FAR 52.216-18 in the solicitation:

DFARS 252.216-7006 ORDERING (MAY 2011)

A. Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the contract schedule. Such orders may be issued from 11/30/2015 through 11/29/2018.

B. All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

C. (1) If issued electronically, the order is considered "issued" when a copy has been posted to the Electronic Document Access system, and notice has been sent to the Contractor.

(2) If mailed or transmitted by facsimile, a delivery order or task order is considered "issued" when the Government deposits the order in the mail or transmits by facsimile. Mailing includes transmittal by U.S. mail or private delivery services.

(3) Orders may be issued orally only if authorized in the schedule.

The following clauses are also incorporated into this contract:

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls

(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) If the Offeror proposes to deviate from any of 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, the Offeror shall submit to the Contracting Officer, for consideration by the DoD CIO, a written explanation of—

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

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

(d) An authorized representative of the DoD CIO will approve or disapprove offeror requests to deviate from NIST SP 800-171 requirements in writing prior to contract award. Any approved deviation from NIST SP 800-171 shall be incorporated into the resulting contract.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

(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 an actual or potentially adverse effect on an information system and/or the information residing therein.

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

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

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

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

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

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this 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; or

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

(2) Apply other information systems security measures when the Contractor reasonably 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>.

(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://lase.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 the substance of this clause, including this paragraph (m), in all subcontracts, including subcontracts for commercial items; and

(2) 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 next higher-tier subcontractor) as soon as practicable.