

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, &amp; 30</b>				1. REQUISITION NUMBER 1000049481	PAGE 1 OF 6	
2. CONTRACT NO. SPE300-17-D-V258	3. AWARD/EFFECTIVE DATE 2018 NOV 16	4. ORDER NUMBER	5. SOLICITATION NUMBER SPE300-16-R-0049	8. SOLICITATION ISSUE DATE 2018 SEP 16		
7. FOR SOLICITATION INFORMATION CALL:			a. NAME	b. TELEPHONE NUMBER (No collect call/s)	8. OFFER DUE DATE/ LOCAL TIME	
9. ISSUED BY  DLA TROOP SUPPORT DIRECTORATE OF SUBSISTENCE 700 ROBBINS AVENUE PHILADELPHIA PA 19111-5086 USA		CODE SPE300	10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE _____ % FOR <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> EDWOSB NAICS: 311812 <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> 8 (A) SIZE STANDARD:			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input checked="" type="checkbox"/> SEE SCHEDULE	12. DISCOUNT TERMS Net 10 days		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b. RATING	
15. DELIVER TO SEE SCHEDULE		CODE	16. ADMINISTERED BY SEE BLOCK 9 CriticBy: PAS None			
17a. CONTRACTOR/ OFFEROR MAYFIELD DAIRY FARMS, LLC DBA MAYFIELD DAIRY FARMS, LLC 1971 DELK INDUSTRIAL BLVD MARIETTA GA 30067-8903 USA TELEPHONE NO. 6782830854	CODE 0X877	FACILITY CODE	18a. PAYMENT WILL BE MADE BY DEF FIN AND ACCOUNTING SVC BSM P O BOX 182317 COLUMBUS OH 43218-2317 USA			
17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>			18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	See Schedule					
25. ACCOUNTING AND APPROPRIATION DATA				26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$101,031.36		
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA			<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED			
<input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA			<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED			
<input checked="" type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN ONE COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED			<input checked="" type="checkbox"/> 29. AWARD OF CONTRACT: REF. SPE30016R0049 OFFER DATED 2018-Nov-08 YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH, HEREIN IS ACCEPTED AS TO ITEMS: ALL ITEMS			
30a. SIGNATURE OF OFFEROR/CONTRACTOR 			31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) 			
30b. NAME AND TITLE OF SIGNER (Type or Print) Brad Anderson - SVP, South Region		30c. DATE SIGNED 11/15/16	31b. NAME OF CONTRACTING OFFICER (Type or Print) MICHELLE MOORE		31c. DATE SIGNED 2018 NOV 16	

AUTHORIZED FOR LOCAL REPRODUCTION  
PREVIOUS EDITION IS NOT USABLE

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

RECEIVED   
 INSPECTED   
 ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: \_\_\_\_\_

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32c. DATE

32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER

34. VOUCHER NUMBER

35. AMOUNT VERIFIED CORRECT FOR

36. PAYMENT

37. CHECK NUMBER

PARTIAL     FINAL

COMPLETE     PARTIAL     FINAL

38. S/R ACCOUNT NO.

39. S/R VOUCHER NUMBER

40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT

42a. RECEIVED BY (*Print*)

41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

41c. DATE

42b. RECEIVED AT (*Location*)

42c. DATE REC'D (*YY/MM/DD*)

42d. TOTAL CONTAINERS

CONTINUED ON NEXT PAGE

## Part 12 Clauses

**252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2015)  
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 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

CONTINUED ON NEXT PAGE

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](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; 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 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://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 next higher-tier subcontractor) as soon as practicable.

(End of clause)

**Group 1: Georgia – Moody AFB**

The terms and conditions of solicitation SPE300-16-R-0049 (as amended, if amended), are hereby included in this contract.

The entire contract period is 27 November 2016 to 23 November 2019

Contract Minimum Value is 25% of the estimated awarded contract value: \$25,257.84

Contract Maximum Value is 250% of the estimated awarded contract value: \$252,578.40

**Points of Contact for Ordering:**

Jocelyn Spradlin / 706.654.9180 x214 / [Jocelyn\\_spradlin@deanfoods.com](mailto:Jocelyn_spradlin@deanfoods.com) / FAX 706.654.5680

Rod Allen / 706.654.910 x252 / [rod\\_allen@deanfoods.com](mailto:rod_allen@deanfoods.com) / FAX 706.654.5680

Carlton Bates / 678.283.0954 / [carlton\\_bates@deanfoods.com](mailto:carlton_bates@deanfoods.com) / FAX 423.745.6419

**Points of Contact for Invoicing and Payment**

Pasha Versa / 800.872.5444 x2257 / [pasha\\_versa@deanfoods.com](mailto:pasha_versa@deanfoods.com) / FAX 423.333.3011

*Ordering period for routine orders shall be a minimum of 48 hours (2 days)*

**Schedule of Items:**

*Fixed Price with EPA:* For fluid milk items (line items 1 –5) the unit prices are in effect at the start of the contract ordering period, and are subject to monthly adjustments as tied to an index in accordance with the Economic Price Adjustment (EPA) clause in the solicitation. The monthly adjustments will continue through the entire 3-year contract period, as applicable.

Item	Stock Number (LSN)	Item Name/Description	Product Code	Unit Size	3 Year Contract Period		
					Estimated Annual Qty per Unit	Price per Unit	Total Price per Unit
1	891001E112203	MILK, CHOC, NONFAT, CHL, 1/2 PT CO	48111	Half Pint (HP)			
2	891001E110544	MILK, LOW FAT, CHL, 1% MILK FAT, 1 GAL CO	12311	Gallon (GAL)			
3	891001E110539	MILK, LOW FAT, CHL, 1% MILK FAT, 1/2 PT CO	51985	Half Pint (HP)			
4	891001E110546	MILK, REDUCED FAT, CHL, 2% MILK FAT, 1/2 PT CO	51983	Half Pint (HP)			
5	891001E110531	MILK, WHOLE, CHL, 1 GAL CO	12313	Gallon (GAL)			

**Schedule of Deliveries:**

**GROUP I – MOODY AFB**

Vendor is responsible for all deliveries on Moody AFB, including:

Moody AFB, GA

1.) Moody AFB 347 SVS/SVMF  
& Friday

6:00am – 11:00am - Monday, Wednesday,

GA Pines Dining Hall B

7255 Woolsey Street

Moody AFB, GA 31699-1796

(229)257-4817

Ship to DoDAAC: FT9013

2.) Moody AFB CDC B

0600 -0900 Tuesday, & Friday

Bldg 210

3103 Robins Road

Moody AFB, GA 31699-1796

POC: Ellen Seth

Ellen.seth@moody.af.mil

(229)257-3135

Ship to DoDAAC: CDC210

3.) YOUTH CENTER

0600 – 0900 Fridays

1804 PREWITTE STREET

MOODY AFB GA 31699

POC: Ellen Seth

Ellen.seth@moody.af.mil

(229)257-3135

Ship to DoDAAC: FT9567

4.) MOODY AFB

0700 – 1100 Monday, Wednesday &

Friday

FLIGHT KITCHEN

8205 APRON RD.

MOODY AFB, GA 31699

POC: Jeffrey Stuart

Jeffrey.stuart@moody.af.mil

229-257-3048

Ship to DoDAAC: FT9267

**MARINES**

1.) Albany Marine Corps

0600 – 1100 Monday, Wednesday & Friday

Child Dev. Center

Albany, GA 30080

(229)639-5765

Ship to DoDAAC: M67004



## **Additional Information:**

### **Rapid Gate**

Many bases currently require enrollment in Rapid Gate and will not allow entry without Rapid Gate clearance. During the contract implementation period, the Contractor must contact all customer locations to determine whether enrollment in Rapid Gate or another security program is required for access to each location. If Rapid Gate or other security enrollment is required, the contractor must take all necessary steps to obtain this in time for the start of performance under this contract. Failure to have Rapid Gate clearance may result in a vendor being turned away from the base and being unable to complete delivery. The contractor is responsible for the additional cost for Rapid Gate enrollment and must ensure that a Rapid Gate enrolled driver is available for all deliveries. There will be a fee for Rapid Gate enrollment that will include access to multiple locations for multiyear access, but the cost of Rapid Gate or other security enrollment may vary, so the contractor should contact Rapid Gate to determine its own costs. If more than one driver is required, Rapid Gate enrollment must be obtained for each driver. Note that enrollment can take several weeks, so an awardee that is not already enrolled must begin enrollment at the time of award notification at the latest. If difficulty or delay in enrollment in Rapid Gate is encountered during the implementation period, the contractor MUST contact Rapid Gate and/or the Security Officer at the applicable customer locations to resolve any issues with processing Rapid Gate enrollment so that the contractor will be able to deliver as required. For additional information regarding Rapid Gate, including enrollment instructions, please visit their website at <http://www.rapidgate.com>.

### **Product Quality**

- A. Acceptance of supplies awarded under this solicitation will be limited to fresh product. All products delivered under this contract must conform to the following **freshness requirements**. Fluid dairy products and other dairy products shall have sufficient remaining shelf life commensurate with good commercial practice. Each container, carton, etc. shall have visible, legible and understandable "sell-by-date" or equivalent.
1. Milk, Whipping Cream (fresh), Cream (fresh) and Half-and-Half (fresh), Ice Milk Mix, Fresh (soft serve), Milk Shake Mix, Fresh (direct draw), Buttermilk and Eggnog must be delivered with a minimum 10 days shelf life remaining.
  2. Whipping Cream (ultra-pasteurized), Half-and-Half (ultra-pasteurized) and Cream (ultra-pasteurized) must be delivered with a minimum 14 days shelf life remaining.
  3. Cottage Cheese, cultured and acidified, normal and extended shelf life must be delivered with a minimum 14 days shelf life remaining.
  4. Sour Cream must be delivered with a minimum 21 days shelf life remaining.
  5. Yogurt must be delivered with a minimum of 18 days shelf life remaining.
  6. Ice Cream must be delivered with a minimum 120 days shelf life remaining.
- B. Commercial standards should be used to maintain temperatures appropriate for the individual items.