	SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30				1. REQUISITION NUMBER 1000048929				PAGE		
2. CONTRACT N	10.	3. AWARD/EFFECTIVE DATE	4. ORDER NUM	BER	5, SOLICIT		NUM	BER		6, SOLIC	ITATION ISSUE
SPE300-17-D	-V251	2016 NOV 06			SPE300	-16-R-00	147				)16 AUG 22
7. FOR SOLI INFORMATIC		a. NAME	- <b></b>		b. TELEPH calls)	ONE NU	MBE	ER (No collec	ct	8. OFFEI LOCA	R DUE DATE/ L TIME
9. ISSUED BY		CODE	SPE300	10, THIS ACQUISITION	vis 🕟		STF	RICTED OR		ET ASIDE	:%
700 ROBBINS A' PHILADELPHIA USA	OF SUBSISTENCE VENUE PA 19111-5096 via Reitano PAA1216 Tr	al: 215-737-0750		SMALL BUSINES HUBZONE SMAI BUSINESS SERVICE-DIS, VETERAN-OW SMALL BUSIN		⊥ (wos	ib)e Leu Osb	JSINESS PF	ider Rögf Nai	THE WON	
11. DELIVERY FO TION UNLESS		12. DISCOUNT TERMS		SMALL BUSIN				RATING		<u> </u>	
MARKED	ILCON IS	Not 10	dev e		RDER UND		14.1	METHOD OI	F SOI	ICITATION	4
SEE SCHED	DULE	Net 10 (	заує	DPAS (15	5 CFR 700)			RFQ		IFB	RFP
15, DELIVER TO		CODE		16. ADMINISTERE	) BY					CODE	SPE300
SEE SCHED	ULE			SEĘ BLOCK 9 Criticality PAS: None	9						
17a, CONTRACT	OR/ CODE 3MC	CW6 FACILITY CODE	:	18a. PAYMENT WIL	L BE MADE	BY				CODE	SL4701
ALTA DENA 17637 E VAL CITY OF IND USA IELEPHONE NO.	USTRY CA 91744- 6269646401 K IF REMITTANCE	LLC	UCH ADDRESS IN	DEF FIN AND / BSM P O BOX 1823 COLUMBUS O USA 18b. SUBMIT INVOI BELOW IS CHI	17 H 43218-23	DORESS		own in blo Dendum	OCK 1	8a UNLES:	3 BLOCK
19. ITEM NO,	*	20. SCHEDULE OF SUPPLIE	0/0CD1////CE0	<b>!</b>	21, QUANTITY	22. UNIT	T	23. UNIT PRIC	_	 A	24, MOUNT
								, ,			-
	See Schedu	le									
	See Schedu	le									•
25. ACCOUNTING	See Schedu	-						AWARD AM	IOUN	T (For Gov	t. Use Only)
27a, 90LICIT/	3 AND APPROPRIA	-				\$15 ADDENE	i7,75		1E		t. Use Only) OT ATTACHED, OT ATTACHED,
27a, SOLICITA 27b, CONTRA 28. CONTRA	3 AND APPROPRIA ATION INCORPORATE CT/PURCHASE ORDE ACTOR IS REQUIR	TION DATA S BY REFERENCE FAR 52.212- R INCORPORATES BY REFER ED TO SIGN THIS DOCUM	ENCE FAR 52,212-4, I	FAR 52,212-5 IS ATTACI		\$15 ADDENE	57,75 DA	61,78	RE RE	ARE N	OT ATTACHED.
27a, SOLICITA 27b, CONTRA 28. CONTRA COPIES TO DELIVER ALL	ATION INCORPORATE CT/PURCHASE ORDE ACTOR IS REQUIR DISSUING OFFICE.	TION DATA S BY REFERENCE FAR 52.212- R INCORPORATES BY REFER	ENCE FAR 52,212-4, I ENT AND RETURN O FURNISH AND IED ABOVE AND	FAR 52,212-5 IS ATTACI	HED, ADDEN AWARD OI 2016-Oc	ADDENE ADDENE DA F CONTE	7,75 A RAC <sup>-</sup> YOU	II.78	RE RE 200-16-R 20N SC		OT ATTACHED, OT ATTACHED,
27a, SOLICITA 27b, CONTRA 27b, CONTRA 28. CONTRA COPIES TO DELIVER ALL ADDITIONAL 3	ATION INCORPORATE CT/PURCHASE ORDE ACTOR IS REQUIR DISSUING OFFICE.	TION DATA S BY REFERENCE FAR 52.212 R INCORPORATES BY REFER ED TO SIGN THIS DOCUM CONTRACTOR AGREES T I OR DTHERWISE IDENTIF TO THE TERMS AND CON	ENCE FAR 52,212-4, I ENT AND RETURN O FURNISH AND IED ABOVE AND	FAR 52,212-5 IS ATTACI	HED, ADDEN AWARD OI 2016-Oc DING ANY A N IS ACCEP	ADDENIE ADDENIE IDA F CONTI Ita-20 DDITTON TED AS	7,75 A A A A A A C A A C A A C A A C A C A	IT: REF, SPEA JR OFFER ( R CHANGE TEMS: ALL	RE RE DOL 16-R DN SC S WH ITEM:	ARE N ARE N 0047 DLICITATIO NCH ARE S S	OT ATTACHED, OT ATTACHED, OFFE ON (BLOCK 5), SET FORTH ,
27a, SOLICIT 27b, CONTRA 27b, CONTRA 28, CONTRA COPIES TO DELIVER ALL ADDITIONAL : 30a, SIGNATURE	ATION INCORPORATE CT/PURCHASE ORDE ACTOR IS REQUIR DISSUING OFFICE. ITEMS SET FORTH SHEETS SUBJECT	TION DATA S BY REFERENCE FAR 52.212- R INCORPORATES BY REFERI ED TO SIGN THIS DOCUMI CONTRACTOR AGREES T I OR DTHERWISE IDENTIF TO THE TERMS AND CON	ENCE FAR 52,212-4, I ENT AND RETURN O FURNISH AND IED ABOVE AND	FAR 52,2125 IS ATTACK N_1 ON ANY ED 31a. UNITED STATI 31b, NAME OF CON	HED, ADDEN 2016-00 DING ANY A N IS ACCEP ES OF AME MA	\$16 ADDENLIDA F CONTINA A20 DDITION TED AS RICA (S)		IT: REF. SPEA DR OFFER ( R CHANGE TEMS: ALL   ATURE OF ( TYPP OF Print)	RE RE DN SC S WH ITEM CONT	ARE N ARE N OG47 DLICITATIO IICH ARE S S RACTING	OT ATTACHED, OT ATTACHED, OFFE ON (BLOCK 5), SET FORTH ,

C.,

19. ITEM NO.		20 SCHEDULE OF SUF	). PLIES/SERVICES			21, QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
				·					
			. ·						
					-				
329. QUANTITY IN			ED, AND CONFORMS 1	го тне	E CONTR	ACT, EXCEPT	AS NOTE	D:	
32b. SIGNATURE REPRESENT		ORIZED GOVERNMENT	32c. DATE	;	32d. PRI REF	NTED NAME A RESENTATIV	ND TITLE E	OF AUTHORIZED G	OVERNMENT
32e. MAILING AD	32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE								
33. SHIP NUMBE	R	34. VOUCHER NUMBER	35. AMOUNT VERIFIE CORRECT FOR	D	36. PAY	MENT			37. CHECK NUMBER
PARTIAL 38. S/R ACCOUN	FINAL	39. S/R VOUCHER NUMBER				OMPLETE		NAL FINAL	
		UNT IS CORRECT AND PROF E OF CERTIFYING OFFICER				D BY (Print)			
						DAT (Location)			
				42c. E	DATE REC	C'D (YY/MM/DE	9 4:	2d, TOTAL CONTAIN	ERS

STANDARD FORM 1449 (REV, 2/2012) BACK

ELOCE 25 23 GURARITED MITTINH: 539,437,95 2305 MARIMUM DOLLAR VALUE: 5354,379.45 ELOCE 26 TOTAL AWARD AMOUNT FOR A THREE-YEAR PERIOD IS \$157,751.78 THE CONTRACT PERIOD OF PERFORMANCE IS FROM NOVEMBER 6, 2016 TO NOVEMBER 2, 2019. Tior 1: Nov. 6, 2016 - Nov. 2, 2013 Tier 2: Nov. 4, 2018 - Nov. 2, 2013	CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-17-D-V251	PAGE 3 OF 6 PAGES
258 GUARANTERE HINNUM: 539,4379,45 ISON MAXIMUM DOLLAR VALUE: 5394,379,45 ILCOK 26 TOTAL AWARD AMOUNT FOR A THREE-YEAR PERIOD IS \$157,751.78 THE CONTRACT PERIOD OF PERFORMANCE IS FROM NOVEMBER 6, 2016 TO NOVEMBER 2, 2019. Tier 1: Nov. 6, 2016 - Nov. 2, 2019 Tier 2: Nov. 4, 2018 - Nov. 2, 2019			
25% GUARANTERED HIRIMUME: \$39,437.95 250% MAXIMUM DOLLAR VALUE: \$394,379.45 BLOCK 26 TOTAL AWARG AMOUNT FOR A THREE-YEAR PERIOD IS \$157,751.70 THE CONTRACT PERIOD OF TERFORMANCE IS FROM NOVEMBER 6, 2016 TO NOVEMBER 2, 2019. Tier 1: Nov. 6, 2016 - Nov. 2, 2019 Tier 2: Nov. 4, 2018 - Nov. 2, 2019			
TOTAL AWARD AMOUNT FOR A THREE-YEAR PERIOD IS \$157,751.78 THE CONTRACT PERIOD OF PERFORMANCE IS FROM NOVEMBER 6, 2016 TO NOVEMBER 2, 2019. Tier 1: Nov. 6, 2016 - Nov. 2, 2018 Tier 2: Nov. 4, 2018 - Nov. 2, 2019	25% GUARANTEED MINIMUM: \$3	9,437.95 \$394,379:45	
Tier 1: Nov. 6, 2016 - Nov. 3, 2018 Tier 2: Nov. 4, 2019 - Nov. 2, 2019		HREE-YEAR PERIOD IS \$157,751.78	
	Tier 1: Nov. 6, 2016 - Nov	. 3, 2018	
	1161 2: NOV. 4, 2013 - HOV	. 21 2013	
	v		
$\cdot$			
· · ·			

CONTINUED ON NEXT PAGE

<text><section-header><section-header><section-header><section-header><section-header><text><text><text><text><text><text><text><text><text><text><text><text><text></text></text></text></text></text></text></text></text></text></text></text></text></text></section-header></section-header></section-header></section-header></section-header></text>	CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED:	PAGE 4 OF 6 PAGES
<section-header><section-header><text><text><text><text><text><text><text><text><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></text></text></text></text></text></text></text></text></section-header></section-header>		SPE300-17-D-V251	
<section-header><section-header><text><text><text><text><text><text><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></list-item></text></text></text></text></text></text></section-header></section-header>			<u>I</u>
<section-header><section-header><text><text><text><text><text><text><text><list-item><list-item><list-item><list-item><list-item><list-item><list-item><table-row></table-row></list-item></list-item></list-item></list-item></list-item></list-item></list-item></text></text></text></text></text></text></text></section-header></section-header>			
<ul> <li>(a) Definitions. As used in this clause—         *****************************</li></ul>	Part 12 Clauses		
<ul> <li>"Adaquate security" means protective measures that are commensurate with the consequences and probability of loss, misus, or unauthorized access to, or modification of information.</li> <li>"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized media may have occurred.</li> <li>"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information tax is trade security, commercially and escription, facility locations, personally identifiable information, as well as trade security, commercially and escription, facility locations, personally identifiable information as a trade security, commercially and information, or other commercially sensitive information that is not customarily shared outside of the company.</li> <li>"Contractor information system" means an information with milliary or space application that is subject to controls on the access, use, reproduction, modification, performance, display, represent by or for, the Contractor.</li> <li>"Controlled technical information system" means an information with milliary or space application that is subject to controls on the access, use, reproduction, modification, performance, display, represent that is outperformance of the contractor and that processes, stores, or transmis covored defines information.</li> <li>"Covored contractor information system" means an information.</li> <li>"Covored contractor information system" means an information.</li> <li>"Covored contractor information, sequentized, and 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</li> <li>(1) For (A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract, and</li> <li>(1) Collecte</li></ul>		NG COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPOR	TING (DEC 2015)
<ul> <li>"Adaquate security" means protective measures that are commensurate with the consequences and probability of loss, misus, or unauthorized access to, or modification of information.</li> <li>"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized media may have occurred.</li> <li>"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information tax is trade security, commercially and escription, facility locations, personally identifiable information, as well as trade security, commercially and escription, facility locations, personally identifiable information as a trade security, commercially and information, or other commercially sensitive information that is not customarily shared outside of the company.</li> <li>"Contractor information system" means an information with milliary or space application that is subject to controls on the access, use, reproduction, modification, performance, display, represent by or for, the Contractor.</li> <li>"Controlled technical information system" means an information with milliary or space application that is subject to controls on the access, use, reproduction, modification, performance, display, represent that is outperformance of the contractor and that processes, stores, or transmis covored defines information.</li> <li>"Covored contractor information system" means an information.</li> <li>"Covored contractor information system" means an information.</li> <li>"Covored contractor information, sequentized, and 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</li> <li>(1) For (A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract, and</li> <li>(1) Collecte</li></ul>	(a) Definition	s. As used in this clause—	
<ul> <li>which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information in unauthorized media may have occurred.</li> <li>"Contractor attributional/proprietary information, as well as trade secrets, commercial or financial information, or other commercially sensitive information, as well as trade secrets, commercial or financial information, or other commercially sensitive information system means the information and the information mays there doubtied of the company.</li> <li>"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.</li> <li>"Contractor information means technical information astements B through F using the criteria set forth in DoD Instruction Size.</li> <li>"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.</li> <li>"Covered contractor information means unclassified information that."</li> <li>"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.</li> <li>"Covered contractor information system" means an information that—         <ul> <li>(1) Is—</li> <li>(2) Cleicted, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contractor; and</li> <li>(1) Falls in any of the following categories:</li> <li>(2) Controlled technical information conceptable consequences for friendly mission accompliatment (part of Operations Security process).</li> <li>(3) Controlled technical information conceptable consequences for friendly mission accomplication shows export advinitions, and Gaverna export advinitization in cuppet relates at fact by or on the part of the</li></ul></li></ul>	"Adequate security" m misuse, or unauthoriz	eans protective measures that are commensurate with the consequences and ed access to, or modification of information.	
<ul> <li>indirectly, by the grouping of information, as well as trade secrets, commercial or financial information, around all as trade secrets, commercial or financial information, around information, around all as trade secrets, commercial or financial information, around information system. The anses an information system that is not outside of the company.</li> <li>"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 Dob Instruction Scatteria and information and the processes, stores, or transmits covered defense information.</li> <li>"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.</li> <li>"Covered defense 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.</li> <li>"Covered defense information gester defense information.</li> <li>(f) Is=</li> <li>(f) Solided in the contract or on behalf of DoD in connection with the performance of the contract, or (B) Collected, developed, received, transmited, used, or stored by or on behalf of the contractor in support of the performance of the contract; and</li> <li>(f) Falls in any of the following categories:</li> <li>(g) Chicka information, operations security. Specific facts identified through the Operations Security process about filendly intertions, 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 Operatio</li></ul>	which unauthorized in information to unauthor	tentional or unintentional disclosure, modification, destruction, or loss of an ob prized media may have occurred.	ject, or the copying of
<ul> <li>"Contractor information system 'means an information system belonging to, or operated by or for, the Contractor.</li> <li>"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 statements. The term does not include information that is lawfully publicly available without restrictions.</li> <li>"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."</li> <li>"Covered contractor information means unclassified information that—         <ul> <li>(1) Is—</li></ul></li></ul>	indirectly, by the group locations), personally	ping of information that can be traced back to the contractor(s) (e.g., program identifiable information, as well as trade secrets, commercial or financial inform	description, facility
<ul> <li>information would meet the criteria, if disseminated, for distribution statements 8 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.</li> <li>"Covered defense 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 that—         <ul> <li>(1) Is—</li> <li>(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract, and</li> <li>(ii) Falls in any of the following categories:</li></ul></li></ul>	"Contractor Informatio "Controlled technical i	n system" means an information system belonging to, or operated by or for, the nformation" means technical information with military or space application that	is subject to controls on
<ul> <li>"Covered contractor information system" means an information system that is owned, or operated by or for, a contractor and the processes, stores, or transmits covered defense information that—         <ul> <li>(i) Is—                 <ul></ul></li></ul></li></ul>	information would meet Instruction 5230.24, D	et the criteria, if disseminated, for distribution statements B through F using the istribution Statements on Technical Documents. The term does not include in	e criteria set forth in DoD
<ul> <li>(i) Is—         <ul> <li>(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         </li> <li>(II) Falls in any of the following categories:             <ul></ul></li></ul></li></ul>	"Covered contractor in that processes, stores	formation system" means an information system that is owned, or operated b , or transmits covered defense information.	y or for, a contractor and
<ul> <li>(B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the parformance of the contract; and</li> <li>(II) Falls in any of the following categories: <ul> <li>(A) Controlled technical information.</li> <li>(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).</li> <li>(C) <i>Export control</i>. Unclassified information concerning cartain 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,</li> <li>(D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with iaw, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).</li> </ul> </li> <li>"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.</li> <li>"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.</li> <li>"Mailclous 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 is recorded, stored, or print</li></ul>	(i) Is—		
<ul> <li>(A) Controlled lechnical information.</li> <li>(B) Critical information (perations 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).</li> <li>(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 munifions list; license applications; and sensitive nuclear technology information.</li> <li>(D) Any other information marked or otherwise identified in the contract, that requires safeguarding or dissemination constols pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).</li> <li>"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.</li> <li>"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.</li> <li>"Maliclous 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, Trojah norse, or other code-based entity that infects a host, as well as spyware and some forms of advare.</li> <li>"Media" means physical devices or writing surfaces including, but is not limited to, magnetic t</li></ul>	(B) (	Collected, developed, received, transmitted, used, or stored by or on behalf of	
<ul> <li>(B) Critical information (operations security). Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitaly 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).</li> <li>(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.</li> <li>(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).</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"Melcia" means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disk</li></ul>			
<ul> <li>(C) <i>Export control</i>. 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.</li> <li>(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).</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"Operationally critical support" means supplies or services designated by the Government as critical for airlift, intermodal transportation services, or logistical support that is essential to the mobilization,</li></ul>	(B) (	Critical information (operations security). Specific facts identified through the C ess about friendly intentions, capabilities, and activities vitally needed by adve	ersaries for them to plan
<ul> <li>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.</li> <li>(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).</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"Operationally critical support" means supplies or services designated by the Government as critical for alrifit, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.</li> <li>"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.</li> <li>"Technical information" means technical data or computer soff</li></ul>	(C) /	Export control. Unclassified information concerning certain items, commodities	
<ul> <li>(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 Governmentvide policies (e.g., privacy, proprietary business information).</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.</li> <li>"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 e</li></ul>	seci regi	rrity and nonproliferation objectives. To include dual use items; items identified lations, international traffic in arms regulations and munitions list; license app	d in export administration
<ul> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"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.</li> <li>"Rapid(ly) report(ing)" means within 72 hours of discovery of any cyber incident.</li> <li>"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</li> </ul>	(D) / diss	Any other information, marked or otherwise identified in the contract, that requeemination controls pursuant to and consistent with law, regulations, and Gove	ires safeguarding or rnmentwide policies (e.g.,
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	"Cyber incident" mean potentially adverse effe	s actions taken through the use of computer networks that result in a compror act on an information system and/or the information residing therein.	
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	in a manner that maint	ains the integrity of the data.	
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	adverse impact on the Trojan horse, or other	confidentiality, integrity, or availability of an information system. This definition code-based entity that infects a host, as well as spyware and some forms of a	n includes a virus, worm, adware.
"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	disks, large-scale integ		
"Rapid(Iy) 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	"Operationally critical s intermodal transportati	on services, or logistical support that is essential to the mobilization, deploym	
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	"Rapid(ly) report(ing)"	means within 72 hours of discovery of any cyber incident.	
	252.227-7013, Rights solicitation or contract.	n Technical Data-Non Commercial Items, regardless of whether or not the cla Examples of technical information include research and engineering data, en	ause is incorporated in this gineering drawings, and
			-
		CONTINUED ON NE	

(

.

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-17-D-V251	PAGE 5 OF 6 PAGES
identifications data sets	, studies and analyses and related information, and computer software e	xecutable code and source
code.		
covered contra	ecurity. The Contractor shall provide adequate security for all covered de ctor information systems that support the performance of work under this ity, the Contractor shall	fense information on all contract. To provide
(1) lm	olement information systems security protections on all covered contract ng, at a minimum—	or information systems
	<ul> <li>(i) For covered contractor information systems that are part of (IT) service or system operated on behalf of the Government</li> </ul>	; <u> </u>
	(A) Cloud computing services shall be subject to the specified in the clause 252.239-7010, Cloud Compu- contract, and	
	contract; and (B) Any other such IT service or system (i.e., other be subject to the security requirements specified els	
	(ii) For covered contractor information systems that are not p operated on behalf of the Government and therefore are not	art of an IT service or system
	requirement specified at paragraph (b)(1)(i) of this clause— (A) The security requirements in National Institute of (A) The security requirements in National Institute of (A)	
	(NIST) Special Publication (SP) 800-171, "Protectin Information in Nonfederal Information Systems and http://dx.doi.org/10.6028/NIST.SP.800-171 that is ir	Organizations,"
	solicitation is issued or as authorized by the Contra practical, but not later than December 31, 2017. Th	cting Officer, as soon as
	DoD CIO, via email at osd.dibcsia@mail.mil, within any security requirements specified by NIST SP 80	30 days of contract award, of
	time of contract award; or (B) Alternative but equally effective security measur the inability to satisfy a particular requirement and a	
(2) Ap	accepted in writing by an authorized representative accepted in writing by an authorized representative bly other information systems security measures when the Contractor ea	of the DoD CIO; and
inform be req	ation systems security measures, in addition to those identified in paragr uired to provide adequate security in a dynamic environment based on a	aph (b)(1) of this clause, may
vulner (c) <i>Cyber incide</i>	nt reporting requirement.	
(1) Wł	en the Contractor discovers a cyber incident that affects a covered cont vered defense information residing therein, or that affects the contractor	
	ments of the contract that are designated as operationally critical suppo (i) Conduct a review for evidence of compromise of covered	rt, the Contractor shall— defense information,
	including, but not limited to, identifying compromised comput and user accounts. This review shall also include analyzing of system(s) that were part of the cyber incident, as well as oth	covered contractor information
	Contractor's network(s), that may have been accessed as a to identify compromised covered defense information, or tha	result of the incident in order
	to provide operationally critical support; and (ii) Rapidly report cyber incidents to DoD at http://dibnet.dod	
shall ir	<i>ber incident report.</i> The cyber incident report shall be treated as informatic lude, at a minimum, the required elements at http://dibnet.dod.mil.	-
or subcontractor shall ha	ertificate requirement. In order to report cyber incidents in accordance w ve or acquire a DoD-approved medium assurance certificate to report cy oved medium assurance certificate, see http://iase.disa.mil/pki/eca/Page	ber incidents. For information
(d) Malicious so	flware. The Contractor or subcontractors that discover and isolate malic cyber incident shall submit the malicious software in accordance with ins	ious software in connection
Contracting Offi (e) <i>Media prese</i>	rvation and protection. When a Contractor discovers a cyber incident ha	is occurred, the Contractor
shall preserve a clause and all re	nd protect images of all known affected information systems identified in elevant monitoring/packet capture data for at least 90 days from the sub	t paragraph (c)(1)(i) of this
(f) Access to ad	OD to request the media or decline interest. ditional information or equipment necessary for forensic analysis. Upon provide DoD with access to additional information or equipment that is	

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED	PAGE 6 OF 6 PAGES
	SPE300-17-D-V251	
	ident damage assessment activities. If DoD elects to conduct a da	
	quest that the Contractor provide all of the damage assessment in	nformation gathered in accordance with
	) of this clause.	
	guarding and use of contractor attributional/proprietary information	
	nauthorized use or release of information obtained from the contra	
	n the contractor) under this clause that includes contractor attribut tion submitted in accordance with paragraph (c). To the maximum	
	and mark attributional/proprietary information. In making an autho	
	will implement appropriate procedures to minimize the contractor	
	ed in such authorized release, seeking to include only that information	
	urpose(s) for which the information is being released.	· · · · · · · · · · · · · · · · · · ·
	elease of contractor attributional/proprietary information not create	d by or for DoD. Information that is
	n the contractor (or derived from information obtained from the cor	ntractor) under this clause that is not
	for DoD is authorized to be released outside of DoD-	
	to entities with missions that may be affected by such information	
	o entities that may be called upon to assist in the diagnosis, dete	
	To Government entities that conduct counterintelligence or law entities	
	For national security purposes, including cyber situational awarene	
	Defense Industrial Base (DIB) participants in the program at 32 C To a support services contractor ("recipient") that is directly support	
	ract that includes the clause at 252.204-7009, Limitations on the 1	
	tractor Reported Cyber incident Information.	
	elease of contractor attributional/proprietary information created by	y or for DoD. Information that is
obtained from	the contractor (or derived from information obtained from the cor	ntractor) under this clause that is
	for DoD (including the information submitted pursuant to paragra-	
	released outside of DoD for purposes and activities authorized by	
	ful Government purpose or activity, subject to all applicable statut	iory, regulatory, and policy based
	hthe Government's use and release of such information. actor shall conduct activities under this clause in accordance with	opplicable laws and regulations on the
	nonitoring, eccess, use, and disclosure of electronic communicati	
	guarding or reporting requirements. The safeguarding and cyber i	
	way abrogates the Contractor's responsibility for other safeguardir	
	ts unclassified information systems as required by other applicable	
	r appliceble U.S. Government statutory or regulatory requirements	
	acts. The Contractor shell—	
	nclude this clause, including this paragraph (m), in subcontracts, o	
	ationally critical support, or for which subcontract performance wi	
	mation system, including subcontracts for commercial items, with es; and	out alteration, except to identify the
	es, and Vhen this clause is included in a subcontract, require subcontract	ors to rapidly report cyber incidents
	ty to DoD at http://dibnet.dod.mil and the prime Contractor. This	
	ber, automatically assigned by DoD, to the prime Contractor (or n	
	racticable.	<b>,</b> , , , , , , , , , , , , , , , , , ,
	(End of clause)	
Attachments		
Attachments		
List of Attachments		
	,	
	Name	
ATTACH.Award Awa	ard SPE300-17-D-	
	1.pdf	
Unsigned		

# Schedule of Items

## **DESCRIPTION/SPECIFICATIONS:**

### Group III: Delivery to customers at Port Hueneme, California

# Class 1 Items Firm Fixed Price with EPA Adjustments (November 6, 2016 - November 2, 2019)

A CAR AND DE CARACTER A	Item Name/Pensorption	Prof-Material	Guinnteorannin Glyportunit	ene i camo	ion indes por contribuid
891001E110569	BUTTERMILK, CHL, HALF GAL	22163	-346		
8910018110586	EGGNOG, CHL, QUART	22165	126		
891001E113398	MILK; CHOC; NONFAT; CHL, 6 GAL BIB	14480	540	a the test of a state of the	
891001E114723	MILK, LOW FAT, CHL, 1% MILK FAT, GAL	21201	927	البحثي ال	
891001E110543	MILK, REDUCED FAT, CHL/2% MILK FAT, GAL	21184	80		
891001E112149	MILK, REDUCED FAT, CHL, 2% MILK FAT, 6 GAL BIB	14446	1;280		
891001E116336	MILK, SOY, SILK, PLAIN, CHL, HALF GAL	22211	818		
891001E110531	MILK, WHOLE, CHL, GAL	21185	875		

Note: Prices on this award document reflect October 2016 pricing. The subsequent monthly EPA price adjustments will be applied accordingly to this "base price." The STORES catalog will be updated to reflect EPA price adjustments for all months going forward from October 2016.

# DESCRIPTION/SPECIFICATIONS: Group III: Delivery to customers at Port Hueneme, California

# Class 2 Items Firm Fixed Price for Tier 1: November 6, 2016 - November 3, 2018

	Titl(11(@4;1132)
Stors (You) (114) - Den Hans/December	is Extinated Annual Ory net Wolfs Pilice par unit - Falal Price per Unit Frank,
891001E113402 CHEESE, COTTAGE, CHL, CREAMED, LG OR SM CURD, 5 LB CO 1450	
891001E113403 CHEESE, COTTAGE, LOW FAT, CHL, CREAMED, LG OR SM CURD, 5 LB CO 145:	2 471 471 471
891001E110598 ICREAM, HEAVY, MIN 36% MILK FAT, PINT. 430	8 206 •••••••••••••••••••••••••••••••••••
891001E118058 CREAM, MFG, CHI, HALF GAL 145-	
891001E114536 SOUR CREAM, CHL, CULTURED OR ACIDIFIED, SLB CO	84 641 641
VARIOUS YOGURT, LOW FAT, ASSORTED, CHL, 6 OZ CÓ See Belo	vi 3,306 <b>(270) (270)</b>

VGSUITUEVOIS/AV	ander			Productsconfo
Peach		 		22955
Blueberry		 		22956
Strawberry Banan	a	 	 	22957
Strawburry			 	23119

Page 2 of 7

# Page 3 of 7

# DESCRIPTION/SPECIFICATIONS: Group III: Delivery to customers at Port Hueneme, California

# Class 2 Items Firm Fixed Price for Tier 2: November 4, 2018 - November 2, 2019

	•		( ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	l6R22[Veap 4]=		18 A
Sure Aunited (199) Alternative/Deterration	la onu de se de	Estimated Ann	united the stare lands	Price per Unit	Totel Pilce per	Uniterine
891001E113402 CHEESE, COTTAGE, CHL, EREAMED, LG OR SM CURD, 518 CO	14508	(*	63			
891001E113403 CHEESE, COTTAGE, LOW FAT, CHL, CREAMED, LG OR SM CURD, 51B CO	14512		471		1	
8910018110598 CREAM, HEAVY, MIN 36% MILK FAT, PINT	45018		206		1	
891001E118058 CREAM, MFG, CHL, HALF GAL	14546	1	-46		ļ	
8910016114536 SOUR CREAM/ CHL, CULTURED ON ACIDIFIED, 5 LB CO	14518		641		N 77 - SA VI 197	
VARIOUS YOGURT, LOW FAT, ASSORTED, CHL, 6 OZ CO	See Below		3,306			وعند جراب
					· · · · · · · · · · · · · · · · · · ·	

C DETERMENT	100.55 578	1、12、54之子		A CULUTING STATE
Peach				22955
(Blitcherry			1	22956
Strawberry Banena	· · · · · · · · · · · · · · · · · · ·			22957
Strawberry		 	. 1	23119

Tier 1 (Inc. Fluid Milk)	
Tier 2	
Aggregate	\$157,751.78

Guaranteed	
Minimum:	\$39,437.95
250 % Max:	\$394,379.45

Award SPE300-17-D-V251

Page 4 of 7

WITHIN 72 HOURS OF RECEIPT OF NOTICE OF AWARD, CONTRACTOR WILL SUPPLY EACH ORDERING ACTIVITITY WITH THE CONTRACTOR'S CODING SYSTEM (PULL DATE, COLOR CODES, ETC.) THIS IS A MANDATORY REQUIREMENT.

The terms and conditions of solicitation SPE300-16-R-0047 (as amended, if amended), are hereby included in this contract.

All aspects of your offer are also incorporated herein.

#### BULK MILK CONTAINERS:

THE BULK MILK/JUICE DISPENSER CONTAINER SHALL BE A SINGLE SERVICE DISPENSER CONTAINER (MULTI-GALLON POLYETHYLENE BAG) AND SHALL BE DELIVERED IN A SINGLE SERVICE SHIPPING CONTAINER (CORRUGATED CARDBOARD BOX) OR A MULTI-SERVICE SHIPPING CONTAINER (PLASTIC/METAL HOLDER/KEEPER CASE) WHICH DOES NOT REQUIRE A TRANSFERRING OF THE SINGLE SERVICE DISPENSER CONTAINER (POLYETHYLENE BAG) TO A HOLDER/KEEPER CASE OR DISPENSER CASE AT POINT OF USE.

#### POINT(S) OF CONTACT FOR ORDERING:

#### Order Department

 Phone:
 (800) 533-2479

 Fax:
 (888) 454-7704

 Email:
 altadena orders@deanfoods.com

#### POINT(S) OF CONTACT FOR INVOICING AND PAYMENT:

Credit Department Phone: (626) 854-4237 Fax: (626) 854-4295

Ordering and Delivery Qualifications: 48-hours order lead time for all items

FOR ALL DELIVERY LOCATIONS IN THIS GROUP: INSPECTION REQUIREMENTS: CONTRACTOR'S DELIVERY VEHICLES WILL STOP AND REPORT TO THE VETERINARY INSPECTION POINT AS DESIGNATED FOR INSPECTION OF THEIR PRODUCTS BEFORE PROCEEDING TO ANY OTHER DESIGNATED DELIVERY POINT(S). (Please note: Rapid Gate is currently a requirement for access to some military bases, the contractor is responsible for obtaining all required enrollments and clearances for each of their drivers as soon as they receive notice of such a requirement)

# Page 5 of 7

# **DESCRIPTION/SPECIFICATIONS:**

# <u>Group III: Delivery to customers at Port Hueneme, CA</u> PoP: November 6, 2016 – November 2, 2019

# DELIVERY POINTS

	Ship To DoDAAC	Activity	Frequency and Time of Delivery
N63126	N69232	Naval Base Ventura County 32 <sup>nd</sup> Street, Bidg. 61 Port Hueneme, CA 93043 POC: (805) 982-3402 glennajane.guevarra@navy.mil	Two (2) deliveries per week 0800-1000
N63126	FT6043	Channel Islands Air National Guard 107 Mulcahey Drive Port Hueneme, CA 93041 POC: (805) 986-7827 nathaniel.bulatao@ang.af.mil joseph.magat@ang.af.mil	One (2) delivery, first week of the month 0800-1000
Z47720	FT9585	LAX Child Development Center 483 N. Aviation Blvd, Bidg. 281 Los Angeles, CA 90245 POC: (310) 653-6800 margarita.gutierrez@us.af.mil	One (1) delivery per week 0800-1200
Z47720	FT9584	LAX Youth Center 2400 S. Pacific Ave, Bldg. 425 San Pedro, CA 90731 POC: (310) 653-8383 esther.dulaney@us.af.mil	One (1) delivery per week 0800-1200
Z47720	1691E6	Long Beach Job Corps 1903 Santa Fe Ave, Bldg. 3 Long Beach, CA 90810 POC: (562) 491-5185 smith.brenden@jobcorps.org	One (1) delivery per week 0700-1200
Various Various	USCG Base LA/LB Galley 1001 Seaside Ave, Bldg. 20 San Pedro, CA 90731 POC: (310) 521-6151 casey.a.bettega@uscg.mil thomas.f.gaulke@uscg.mil	Two (2) deliveries per week 0600-1100	
		The following Coast Guard Cutters docking at San Pedro (1001 Seaside Ave): Z11403 USCGC Mellon Z11408 USCGC Morgenthau Z11411 USCGC Jarvis	As Needed

#### Award SPE300-17-D-V251

Various	Various	US Navy Ships docking at Port Hueneme	As Needed
		Z15248 USCGC Aspen Z15252 USCGC Hickory Z15530 USCGC George	
		Z12104 USCGC Active Z12109 USCGC Steadfast Z12116 USCGC Alert	
		Z11412 USCGC Midgett Z11702 USCGC Waesche	

#### DELIVERIES TO SHIPS:

Due to fluctuating arrival and /or departure schedules, ships may require delivery of products within a specific time frame. The Ordering Officer will advise the contractor of any special delivery requirements when placing orders, and the contractor will comply with the request. Deliveries ARE NOT required to be made outside the "time of delivery" specified unless agreed to between the contractor and customer and approved by the DLA Troop Support Contracting Officer.

FOR DELIVERIES MADE TO SHIPS, ALL ITEMS ARE REQUIRED TO BE PACKAGED IN DISPOSABLE, NON-RETURNABLE CARDBOARD BOXES SUITABLE FOR STACKING. THIS REQUIREMENT IS MANDATORY, NOT NEGOTIABLE.

Note For Ships: Deliveries shall not be left on docks or wharves and must be made available to government representatives authorized to accept deliveries.

The Inter-Service Supply Support Operations Program (ISSOP) monitors the contractor hired to continue the delivery process for the ships by transporting the stores from the brow of the ship into their storeroom. In order to accomplish this, the Contractor may have to schedule deliveries through the NAVSUP Fleet Logistics Center (FLC) when making deliveries of their product.

Signed delivery tickets (i.e., annotated and signed copies of the receipt documents) must be dropped off at the NAVSUP FLC Office or Drop Box, prior to the delivery truck departing from the base, depending on the individual requirement of each customer. Signed delivery tickets may also be faxed within 24 hours of delivery.

## **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 <u>freshness requirements</u>. 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 (ultrapasteurized) 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,

## "SELL-BY-DATE" COMPLIANCE IS REQUIRED WHEN DELIVERY IS MADE IN CALIFORNIA.