ORDER FOR SUPPLIES OR SERVICES								PAGE 1 OF6			
1. CONTRACT/P SPE300-18-/		RDER/AGREEMENT NO.	2. DELIVER	Y ORDER/CALL NO.		3. DATE OF ORDE (YYYYMMMDD) 2017 OCT		4. REQUISITION/F	PURCH RE	EQUEST NO.	5. PRIORITY
6. ISSUED BY DLA TROOP SUF DIRECTORATE C 700 ROBBINS A PHILADELPHIA F USA Local Admin: Micl Email: MICHELLE	OF SUBSIST VENUE PA 19111-50 helle Moore	096 PSPRPBD Tel: 215-737-3659	L	SPE300	DLA DIRE 700 PHIL USA	MINISTERED BY (If of TROOP SUPPORT ECTORATE OF SUBSIST ROBBINS AVENUE ADELPHIA PA 19111-50 Julity: PAS: None	ENCE	6) CODE SI	PE300		8. DELIVERY FOB X DESTINATION OTHER (See Schedule if other)
9. CONTRACTO		@DLA.MIL	CODE 1	1FUU7		ACILITY		10. DELIVER TO		IT BY (Date)	11. X IF BUSINESS IS
CO NAME INC AND 460	CA-COL/ C. DBA C 00 E LAKI	A BOTTLING COMPA COCA-COLA E BLVD AM AL 35217-4032	L					12. DISCOUNT TE Net 30 days	ERMS		SMALL SMALL DISAD- VANTAGED WOMEN-OWNED
USA								13. MAIL INVOID Submit Invoice			
14. SHIP TO SEE SCHE	DULE, D	DO NOT SHIP TO ADE		N THIS PAGE	DE BS P	AYMENT WILL BE MA EF FIN AND ACCC SM O BOX 182317 OLUMBUS OH 43 SA	DUNTING	SVC	_4701		MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.
16. DELIVE	ERY/ X	This delivery order/ca	II is issued on a	another Government	agency	y or in accordance wi	th and sub	ject to terms and co	nditions o	f above numbe	ered contract.
TYPE OF	14 O E	Reference your							furnish the	e following on t	erms specified herein.
		ACCEPTANCE. THE C BEEN OR IS NOW MO									REVIOUSLY HAVE
—	OF CONTI	RACTOR supplier must sign Accepta		GNATURE			TYPED	NAME AND TITLE			DATE SIGNED (YYYYMMMDD)
18. ITEM NO.		19. SCH	EDULE OF SU	PPLIES/SERVICES				. QUANTITY ED/ ACCEPTED*	21JJNIT	22. UNIT PRICE	23. AMOUNT
See Schedule						0.000					
* If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.							\$150000.00				
27a. QUANTITY	IN COLU	MN 20 HAS BEEN						IG/ORDERING OFF		I	
INSPECTED         RECEIVED         ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:           b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE         c. DATE (YYYYMMMDD)         d. PRINTED NAME AND TITED						ED NAME AND TITLE	OF AUTHO	DRIZED GOVER	RNMENT REPRESENTATIVE		
e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE				2	28. SHIP. NO.	29. D.O.	VOUCHER NO.	30	D. INITIALS		
f. TELEPHONE NUMBER g. E-MAIL ADDRESS				-	PARTIAL FINAL	32. PAID	BY	33	3. AMOUNT VE	ERIFIED CORRECT FOR	
				3	1. PAYMENT			34	4. CHECK NUN	<b>MBER</b>	
a. DATE (YYYYMMMDD)	-	DUNT IS CORRECT AND ATURE AND TITLE OF CERTI		₹ PAYMENT.	_	COMPLETE PARTIAL FINAL			35	5. BILL OF LAI	DING NO.
37. RECEIVED AT	38. REC	38. RECEIVED BY (Print)     39. DATE RECEIVED (YYYYMMMDD)     40. TOTAL CON- TAINERS     41. S/R ACCOUNT NUMBER     42. S/R VOUCHER NO.						ER NO.			

CONTINUATION SHEET	REFERENCI	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-18-A-9300					
		SECTION B					
SUPPLIES/SERVICES:							
ITEM NO. SUPPLIES/SERVICES		UNIT UNIT PRICE	AMOUNT				
0001 GM5022361 Market Fresh Div	100.000	EA \$ 100.00000	\$ 0.00	_			
PRICING TERMS: Firm Fixed I	Price						
BASE PERIOD							
SUPPLIES/SERVICES:							
CLIN Price 0001 \$ 100.00	Delivery (in days) 000						
OPTION 01							
SUPPLIES/SERVICES:							
CLIN Price	Delivery (in days) 000						
QTY VARIANCE: PLUS 0% MINUS	S 0%						
INSPECTION POINT: DESTINAT:	ION						
ACCEPTANCE POINT: DESTINAT	ION						
FOB: DESTINATION DELIVERY	DATE:						
GOVT USE	External	External External	Customer RDD/				

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

#### **SECTION I - CONTRACT CLAUSES**

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

(a) Definitions. As used in this clause—

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

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

"Covered defense information" means unclassified information that-

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) Controlled technical information.

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

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

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

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

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

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

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

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

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

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

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

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

(End of clause)

**CONTINUED ON NEXT PAGE** 

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

(a) Definitions. As used in this clause-

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

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

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

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

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

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

"Covered defense information" means unclassified information that-

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) Controlled technical information.

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

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

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

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

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

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

<ul> <li>(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— <ul> <li>(1) Injelement information systems security protections on all covered contractor information systems including, at a minimum— <ul> <li>(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</li> <li>(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified at paragraph (b)(11)) of this clause— <ul> <li>(I) 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 requirements in specified at paragraph (b)(11)) of this clause— <ul> <li>(I) 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 requirements in National Institute of Standards and Technology (N) ST Special Publication (SP) 800-171. Whereforing Controlled Unclassified information in Nonfederal Information Systems and Organizations."</li> <li>(I) The contract award; or</li> <li>(B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and chieve equavalent protection accepted in writing by an authorized representative of the DDC (2) and</li> </ul> </li> <li>(2) Apply other information systems security measures when the Contractor shall notify the DDC (2) view enalt at eacting alternative but equality effective security realisements 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 enviro</li></ul></li></ul></li></ul></li></ul>		SPE300-18-A-9300	
<ul> <li>covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—         <ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—</li></ul></li></ul>			
<ul> <li>adequate security, the Contractor shall— <ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum— <ul> <li>(i) For covered contractor information systems that are part of an Information Technology</li> <li>(ii) For covered contractor information systems that are part of an Information Technology</li> <li>(iii) For covered contractor information systems that are part of an Information system</li> <li>(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and</li> <li>(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 requirements pecified at paragraph (b)(10) of this clause—</li> <li>(iii) For covered contractor information systems and Organizations,"</li> <li>(iii) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. That is in effect at the time the solicitation is insued or as authorized by the Contractor gottler, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd. diocis@mail.mi, within 30 days of contract award, of any security requirements specified by VIST SP 800-171 not implemented at the time of contract award; or</li> <li>(ii) Alternative but equaly effective security measures used to compensale for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representave of the DoD CIO; and</li> <li>(2) Apply other 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.</li> </ul> </li> <li>(c) Cyb</li></ul></li></ul>			
<ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—         <ul> <li>(i) For covered contractor information systems that are part of an Information Technology (IT) service or system optated on behalf of the Government—                 <ul></ul></li></ul></li></ul>			
<ul> <li>(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—         <ul> <li>(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</li> <li>(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified selsewhere in this contract; or</li> <li>(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—</li></ul></li></ul>	(1)	mplement information systems security protections on all covered contractor in	nformation systems
<ul> <li>(IT) service or system operated on behalf of the Government—         <ul> <li>(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</li> <li>(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</li> <li>(I) 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)(7)(1) of this clause—</li></ul></li></ul>			n Information Technology
<ul> <li>specified in the clause 252.238-7010, Cloud Computing Services, of this contract; and         <ul> <li>(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</li> <li>(i) 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 (0)(1)(i) of this clause—</li></ul></li></ul>			
<ul> <li>contract; and         <ul> <li>(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</li> <li>(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(1)) of this clause—</li></ul></li></ul>			
<ul> <li>(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</li> <li>(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)(11)(i) of this clause— <ul> <li>(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 dibesia@mail.mil, within 30 days of contract award, or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(i) Conduct a review for evidence of compromise of covered contractor shall—         <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific dat, and user accounts. This review shall also information, or that affects se acide as operationally critical support, the Contractor shall—         <ul> <li>(i) Otoduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review</li></ul></li></ul></li></ul></li></ul>		•	g Services, of this
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)(0) 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 Contract shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems 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 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, seveil as offormation created		,	n cloud computing) shall
<ul> <li>(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— <ul> <li>(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. that is in effect at the time the solicitation is issued or as authorized by the Contractor governments in 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 Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security 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.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(i) When the Contract discovers a cyber incident that affects a covered contractor information systems or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract report for vidue as operationally critical support, the Contractor shall—</li> <li>(i) Councut a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems are apt of the cyber incident.</li> <li>(2) Cyber incident report the requirement of bediens a information systems on the Contractor shall perior bapt</li></ul></li></ul>			
<ul> <li>operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—         <ul> <li>(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 bissued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(C) <i>Cyber incident reporting requirement.</i> <ul> <li>(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 information system or the covered defense information residing therein, or that affects a sovered contractor 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 for the contract</li></ul></li></ul></li></ul>			
<ul> <li>(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 osci.dicbsia@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</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information system security measures when the Contractor easonably determines that information system security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 edesignated as operationally critical support, the Contractor Shall— (i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system system system system system system system system security measures when the Contractor's ability to perform the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised computers, servers, specific data, and user accounts. This review shall al</li></ul>			
<ul> <li>(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.mli, 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</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(1) When the Contract 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—</li> <li>(i) Conduct a review for evidence of compromised covered defense information, including, but not limited to, identifying compromised contractor information, including, but not limited to, identifying compromised 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, created by or fo</li></ul>			
<ul> <li>Information in Nonfederal Information Systems and Örganizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(11) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 compromised convered defense information, including, but not limited to, identifying compromised conversed 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 incident to DOD at thtp://dibnet.dod.mil.</li> <li>(2) Cyber incident</li></ul>			
<ul> <li>http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as a suthorized by the Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(1) When the Contract discovers a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall— <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor report. The covered defense information system or to identify compromised covered defense information system or to identify compromised covered defense information system (i) Rapidly report cyber incident report; and (ii) Rapidly report cyber incident store) as a information system or the covered defense information system or the 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 is ability to provide operationally critical support; and</li> <li>(ii) Cayber incident report. The cyber incident to the poth</li></ul></li></ul>			
<ul> <li>solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 shall—         <ul> <li>(i) Conduct a review for evidence of compromise d computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor's network(s), that may have been accessed as a result of the contractor's ability to provide operationally critical support, and (ii) Rapidly compromised covered defense information systems on the Contractor's contractor's ability to provide operationally critical support, and the incident in order to identify compromised covered defense 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 systems on the Contractor's depend to yber incidents to DoD and shall include, at a minimum, the required elements</li></ul></li></ul>			
<ul> <li>practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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—         <ul> <li>(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 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 created by or for DoD and shall include, at a minimum, the required elements a thtp://dibnet.dod.mil.</li> <li>(3) Medium assurance certificate requirement. In order to report cyber incidents in DoD and thy://dibnet.dod.mil.</li> </ul> </li> </ul>			
<ul> <li>any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor 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 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</li> <li>(i) 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.</li> <li>(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 me</li></ul>		practical, but not later than December 31, 2017. The C	Contractor shall notify the
time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. (c) <i>Cyber incident reporting requirement.</i> (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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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 incide			
<ul> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) <i>Cyber incident reporting requirement</i>.</li> <li>(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— <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor's onetwork(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information give the incident in order to identify compromised covered defense information asystem(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 <ul> <li>(i) Cyber incident report. The cyber incidents to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(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.</li> <li>(3) Medium assurance certificate require</li></ul></li></ul>			71 not implemented at the
the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. (c) <i>Cyber incident reporting requirement</i> . (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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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			used to compensate for
<ul> <li>accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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— <ul> <li>(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 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 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, 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</li> <li>(ii) Rapidly report cyber incident to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(2) Cyber incident report. The cyber incident shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.</li> <li>(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcont</li></ul>			
<ul> <li>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.</li> <li>(c) <i>Cyber incident reporting requirement.</i> <ul> <li>(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— <ul> <li>(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, contractor's ability to provide operationally critical support; and</li> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(2) <i>Cyber incident report.</i> The cyber incident the trated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.</li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul></li></ul>			
<ul> <li>be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) <i>Cyber incident reporting requirement.</i> <ul> <li>(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— <ul> <li>(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, envice operationally critical support; and</li> <li>(ii) Rapidly report 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.</li> </ul> </li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul></li></ul>			
<ul> <li>vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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— <ul> <li>(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</li> <li>(ii) Rapidly report cyber incident to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(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.</li> <li>(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</li> </ul>			
<ul> <li>(c) Cyber incident reporting requirement.</li> <li>(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—         <ul> <li>(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</li> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>			issessed fisk of
<ul> <li>(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—         <ul> <li>(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, correct or identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and             <ul> <li>(ii) Rapidly report 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.</li> <li>(2) <i>Cyber incident report.</i> 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.</li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul> </li> </ul></li></ul>			
<ul> <li>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—         <ul> <li>(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</li></ul></li></ul>			tor information system or
<ul> <li>(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         <ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>	the	covered defense information residing therein, or that affects the contractor's a	bility to perform the
<ul> <li>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</li></ul>	requ		
<ul> <li>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</li></ul>			
<ul> <li>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         <ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>			
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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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			
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			
<ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul>			fect the Contractor's ability
<ul> <li>(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.</li> <li>(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</li> </ul>			
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	(2) (		
(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	(2) ( shal	Linclude, at a minimum, the required elements at http://dibnet.dod.mil	Greated by OFIDE DOD allo
or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information			this clause, the Contractor
	or subcontractor shall	have or acquire a DoD-approved medium assurance certificate to report cybe	r incidents. For information

(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.

(I) 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)

#### **CAUTION NOTICE**

#### BLANKET PURCHASE AGREEMENT NUMBER: SPE30018A9300

#### ITEM: CANNED AND BOTTLED SODA PRODUCTS

- 1. The supplier is required to indicate acceptance of this Blanket Purchase Agreement (BPA) and return one copy as indicated on Page <u>9</u> of this BPA at paragraph 13.
- 2. The supplier is also required to complete the applicable representation/certifications at clauses 252.209-7991, 52.212-3, and 252.225-7000 (see pages <u>10 26</u> of this BPA); and 52.215-6 Place of Performance (page 44 of this BPA).
- 3. Supplier's attention is directed to Page <u>6.</u> It is imperative that the requested information in this paragraph be provided when completing this BPA document. In particular, the Government requires the FAX NUMBER FOR ORDER RECEIPT to ensure prompt delivery to military customers. Additionally, POINT(S) OF CONTACT FOR ORDERING and POINT(S) OF CONTACT FOR INVOICING AND PAYMENT will need to be completed.

#### **CAUTION - CONTRACTOR CODE OF BUSINESS ETHICS (FEB 2012)**

FAR Part 3.1002(a) requires all government contractors to conduct themselves with the highest degree of integrity and honesty. Contractors should have a written code of business ethics and conduct within thirty days of award. To promote compliance with such code of business ethics and conduct, contractors should have an employee business ethics and compliance training program that facilitates timely discovery and disclosure of improper conduct in connection with government contracts and ensures corrective measures are promptly instituted and carried out. A contractor may be suspended and/or debarred for knowing failure by a principal to timely disclose to the government, in connection with the award, performance, or closeout of a government contract performed by the contractor or a subcontract awarded there under, credible evidence of a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in title 18 of the United States Code or a violation of the False Claims Act. (31 U.S.C. 3729-3733)

If this solicitation or contract includes FAR clause 52.203-13 - CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT; the contractor shall comply with the terms of the clause and have a written code of business ethics and conduct; exercise due diligence to prevent and detect criminal conduct; promote ethical conduct and a commitment to compliance with the law within their organization; and timely report any violations of federal criminal law involving fraud, conflict of interest, bribery or gratuity violations found in title 18 of the United States Code or any violations of the False Claims Act. (31 U.S.C. 3729-3733). When FAR 52.203-13 is included in the contract, contractors must provide a copy of its written code of business ethics and conduct to the contracting officer upon request by the contracting officer.

#### Rapid Gate Requirement and/or Other Security Programs

Many bases currently require enrollment in Rapid Gate and/or other security programs and will not allow entry without 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. We currently estimate that Rapid Gate enrollment will cost about \$250 per company and \$200 per enrolled employee for 1 year of access to multiple locations, 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.

#### <u>Contents</u>

#### **Schedule of Supplies**

-	Caution Notice	. 2
	Rapid Gate	
-	Item Description	. 6

#### **Blanket Purchase Agreement (BPA) Terms and Conditions**

1.	Description of Agreement	
2.	Extent of Obligation	
3.	Pricing	
4.	Purchase Limitation	
5.	Individuals Authorized To Place Orders	
6.	Deliveries7	
7.	Delivery Tickets	
8.	Marking Requirements	
9.	Invoices	
	Delivery Locations	
11.	Acceptance	
12.	Additional Ordering Procedures/Requirements	
13.	Additional Responsibilities of the Supplier	
14.	Right to Award Other Contract and Orders	
15.	North America Industry Classification System (NAICS) Code and	
	Small Business Size Standard   9	
Non-Co	mpete Provision	
Food D	efense / Force Protection	)

#### **Provisions and Clauses**

252.209-7991: Representation by Corporations Regarding an							
Inpaid Delinquent Tax Liability or a Felony Conviction under any							
Federal Law	10						
52.212-3: Offeror Representations and Certifications –							
Commercial Items (Nov-2015)							
252.225-7000: Buy American Act –							
Balance of Payments Program Certificate (Nov 2014)							
52.212-4: Contract Terms and Conditions Commercial Items (May 2015) -							
FAR (by reference)							
Addendum to 52.212-4 – Contract Terms and Conditions – Commercial Items	28-30						

~Continue Contents Next Page~

#### <u>Contents</u>

52.212-5: Contract Terms and Conditions Required to Implement	
Statutes or Executive Orders Commercial Items (Jan 2016)	30-42
52.233-9001: Disputes: Agreement to Use Alternative Dispute Resolution (NOV 2011) – DLAD	42-43
<b>52.252-2:</b> Clauses Incorporated by Reference (Feb 1998)	42-43
<b>52.252-1:</b> Solicitation Provisions Incorporated by Reference (Feb 1998)	43
<b>52.215-6: Place of Performance (Oct 1997)</b>	44

ORDER FOR SUPPLIES OR SERVICES								PAGE 1 OF6			
1. CONTRACT/P SPE300-18-/		RDER/AGREEMENT NO.	2. DELIVER	Y ORDER/CALL NO.		3. DATE OF ORDE (YYYYMMMDD) 2017 OCT		4. REQUISITION/F	PURCH RE	EQUEST NO.	5. PRIORITY
6. ISSUED BY DLA TROOP SUF DIRECTORATE C 700 ROBBINS A PHILADELPHIA F USA Local Admin: Micl Email: MICHELLE	OF SUBSIST VENUE PA 19111-50 helle Moore	096 PSPRPBD Tel: 215-737-3659	L	SPE300	DLA DIRE 700 PHIL USA	MINISTERED BY (If of TROOP SUPPORT ECTORATE OF SUBSIST ROBBINS AVENUE ADELPHIA PA 19111-50 Julity: PAS: None	ENCE	6) CODE SI	PE300		8. DELIVERY FOB X DESTINATION OTHER (See Schedule if other)
9. CONTRACTO		@DLA.MIL	CODE 1	1FUU7		ACILITY		10. DELIVER TO		IT BY (Date)	11. X IF BUSINESS IS
CO NAME INC AND 460	CA-COL/ C. DBA C 00 E LAKI	A BOTTLING COMPA COCA-COLA E BLVD AM AL 35217-4032	L					12. DISCOUNT TE Net 30 days	ERMS		SMALL SMALL DISAD- VANTAGED WOMEN-OWNED
USA								13. MAIL INVOID Submit Invoice			
14. SHIP TO SEE SCHE	DULE, D	DO NOT SHIP TO ADE		N THIS PAGE	DE BS P	AYMENT WILL BE MA EF FIN AND ACCC SM O BOX 182317 OLUMBUS OH 43 SA	DUNTING	SVC	_4701		MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.
16. DELIVE	ERY/ X	This delivery order/ca	II is issued on a	another Government	agency	y or in accordance wi	th and sub	ject to terms and co	nditions o	f above numbe	ered contract.
TYPE OF	14 O E	Reference your							furnish the	e following on t	erms specified herein.
		ACCEPTANCE. THE C BEEN OR IS NOW MO									REVIOUSLY HAVE
—	OF CONTI	RACTOR supplier must sign Accepta		GNATURE			TYPED	NAME AND TITLE			DATE SIGNED (YYYYMMMDD)
18. ITEM NO.		19. SCH	EDULE OF SU	PPLIES/SERVICES				. QUANTITY ED/ ACCEPTED*	21JJNIT	22. UNIT PRICE	23. AMOUNT
See Schedule						0.000					
* If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.							\$150000.00				
27a. QUANTITY	IN COLU	MN 20 HAS BEEN						IG/ORDERING OFF		I	
INSPECTED         RECEIVED         ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED:           b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE         c. DATE (YYYYMMMDD)         d. PRINTED NAME AND TITED						ED NAME AND TITLE	OF AUTHO	DRIZED GOVER	RNMENT REPRESENTATIVE		
e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE				2	28. SHIP. NO.	29. D.O.	VOUCHER NO.	30	D. INITIALS		
f. TELEPHONE NUMBER g. E-MAIL ADDRESS				+	PARTIAL FINAL	32. PAID	BY	33	3. AMOUNT VE	ERIFIED CORRECT FOR	
				3	1. PAYMENT			34	4. CHECK NUN	<b>MBER</b>	
a. DATE (YYYYMMMDD)	-	DUNT IS CORRECT AND ATURE AND TITLE OF CERTI		₹ PAYMENT.	_	COMPLETE PARTIAL FINAL			35	5. BILL OF LAI	DING NO.
37. RECEIVED AT	38. REC	38. RECEIVED BY (Print)     39. DATE RECEIVED (YYYYMMMDD)     40. TOTAL CON- TAINERS     41. S/R ACCOUNT NUMBER     42. S/R VOUCHER NO.						ER NO.			

CONTINUATION SHEET	REFERENCI	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE300-18-A-9300					
		SECTION B					
SUPPLIES/SERVICES:							
ITEM NO. SUPPLIES/SERVICES		UNIT UNIT PRICE	AMOUNT				
0001 GM5022361 Market Fresh Div	100.000	EA \$ 100.00000	\$ 0.00	_			
PRICING TERMS: Firm Fixed I	Price						
BASE PERIOD							
SUPPLIES/SERVICES:							
CLIN Price 0001 \$ 100.00	Delivery (in days) 000						
OPTION 01							
SUPPLIES/SERVICES:							
CLIN Price	Delivery (in days) 000						
QTY VARIANCE: PLUS 0% MINUS	S 0%						
INSPECTION POINT: DESTINAT:	ION						
ACCEPTANCE POINT: DESTINAT	ION						
FOB: DESTINATION DELIVERY	DATE:						
GOVT USE	External	External External	Customer RDD/				

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

#### **SECTION I - CONTRACT CLAUSES**

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

(a) Definitions. As used in this clause—

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

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

"Covered defense information" means unclassified information that-

(1) Is—

(i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(2) Falls in any of the following categories:

(i) Controlled technical information.

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

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

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

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

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

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

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

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

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

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

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

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

(End of clause)

**CONTINUED ON NEXT PAGE** 

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

(a) Definitions. As used in this clause-

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

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

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

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

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

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

"Covered defense information" means unclassified information that-

(i) Is—

(A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and

(ii) Falls in any of the following categories:

(A) Controlled technical information.

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

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

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

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

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

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

<ul> <li>(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— <ol> <li>(1) Injelement information systems security protections on all covered contractor information systems including, at a minimum— </li> <li>(A) Endu computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and </li> <li>(B) Any other such IT service or system (i.e., other than Cloud Computing) shall be subject to the security requirements specified at paragraph (b)(11)) of this clause— </li> <li>(I) 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 requirements in specified at paragraph (b)(11)) of this clause— </li> <li>(I) 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 requirements in National Institute of Standards and Technology (N) Stopeal Publication (SP) 800-171, "Proteing Controlled Unclassified information in Nonfederal Information Systems and Organizations," </li> <li>(I) The security requirements in Nationizad N, NIST SP 800-171, that is in effect at the time the solicitation is subject and security requirement and expressentive of the DoD ClO, via email at cost clause appressive shall be DoC ClO; and </li> <li>(2) Apply other information systems security measures when the Contractor shall notify the DoD ClO, via email at cost clause acounty in a subsider of solicitation system or the inability to satisfy a particular requirement and achieve equivalent protection includent information system security measures when the Contractor shall—</li> <li>(2) Apply other information systems security measures wh</li></ol></li></ul>		SPE300-18-A-9300	
<ul> <li>covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—         <ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—</li></ul></li></ul>			
<ul> <li>adequate security, the Contractor shall— <ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum— <ul> <li>(i) For covered contractor information systems that are part of an Information Technology</li> <li>(ii) For covered contractor information systems that are part of an Information Technology</li> <li>(iii) For covered contractor information systems that are part of an Information system</li> <li>(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and</li> <li>(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 requirements pecified at paragraph (b)(10) of this clause—</li> <li>(iii) For covered contractor information systems and Organizations,"</li> <li>(iii) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. That is in effect at the time the solicitation is insued or as authorized by the Contractor gottler, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd. diocis@mail.mi, within 30 days of contract award, of any security requirements specified by VIST SP 800-171 not implemented at the time of contract award; or</li> <li>(ii) Alternative but equaly effective security measures used to compensale for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representave of the DoD CIO; and</li> <li>(2) Apply other 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.</li> </ul> </li> <li>(c) Cyb</li></ul></li></ul>			
<ul> <li>(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—         <ul> <li>(i) For covered contractor information systems that are part of an Information Technology (IT) service or system optated on behalf of the Government—                 <ul></ul></li></ul></li></ul>			
<ul> <li>(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—         <ul> <li>(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</li> <li>(B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified selsewhere in this contract; or</li> <li>(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—</li></ul></li></ul>	(1)	mplement information systems security protections on all covered contractor in	nformation systems
<ul> <li>(IT) service or system operated on behalf of the Government—         <ul> <li>(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</li> <li>(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</li> <li>(I) 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)(7)(1) of this clause—</li></ul></li></ul>			n Information Technology
<ul> <li>specified in the clause 252.238-7010, Cloud Computing Services, of this contract; and         <ul> <li>(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</li> <li>(i) 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 (0)(1)(i) of this clause—</li></ul></li></ul>			
<ul> <li>contract; and         <ul> <li>(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</li> <li>(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(1)) of this clause—</li></ul></li></ul>			
<ul> <li>(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</li> <li>(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)(11)(i) of this clause— <ul> <li>(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 dibesia@mail.mil, within 30 days of contract award, or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(i) Conduct a review for evidence of compromise of covered contractor shall—         <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific dat, and user accounts. This review shall also information, or that affects se acide as operationally critical support, the Contractor shall—         <ul> <li>(i) Otoduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review</li></ul></li></ul></li></ul></li></ul>		•	g Services, of this
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)(0) 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 Contract shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems 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 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, seveil as offormation created			n cloud computing) shall
<ul> <li>(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— <ul> <li>(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. that is in effect at the time the solicitation is issued or as authorized by the Contractor governments in 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 Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security 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.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(i) When the Contract discovers a cyber incident that affects a covered contractor information systems or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract report for vidue as operationally critical support, the Contractor shall—</li> <li>(i) Could ca review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems are apprent of the cyber incident.</li> <li>(2) Cyber incident report the requirement of the contractor shall by order or subort information systems on</li></ul></li></ul>			
<ul> <li>operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—         <ul> <li>(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 bissued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(C) <i>Cyber incident reporting requirement.</i> <ul> <li>(1) When the Contractor determs information residing therein, or that affects a covered contractor information system or the 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's ability to perform the requirements of the contractor's network(s), that may have been accessed as a result of the incident in order to identify report cyber incident so bot on system or th</li></ul></li></ul></li></ul>			
<ul> <li>(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 osci.dicbsia@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</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information system security measures when the Contractor easonably determines that information system security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 edesignated as operationally critical support, the Contractor Shall— (i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system system system system (i) 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 computers, servers, specific data, and user accounts. This review shall also in</li></ul>			
<ul> <li>(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.mli, 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</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(1) When the Contract 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—</li> <li>(i) Conduct a review for evidence of compromised covered defense information, including, but not limited to, identifying compromised contractor information, including, but not limited to, identifying compromised 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, created by or fo</li></ul>			
<ul> <li>Information in Nonfederal Information Systems and Örganizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(11) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 compromised convered defense information, including, but not limited to, identifying compromised conversed 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 incident to DOD at thtp://dibnet.dod.mil.</li> <li>(2) Cyber incident</li></ul>			
<ul> <li>http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as a suthorized by the Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(1) When the Contract discovers a cyber incident that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor shall— <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor report. The covered defense information system or to identify compromised covered defense information system or to identify compromised covered defense information system (i) Rapidly report cyber incident report; and the centractor's ability to perform the requirements of the contract that are designated as operationally critical support, the Contractor information system(i) that were part of the cyber incident, as well as other information, including, but not limited to identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor is ability to provide operationally criti</li></ul></li></ul>			
<ul> <li>solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 shall—         <ul> <li>(i) Conduct a review for evidence of compromise d computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor's network(s), that may have been accessed as a result of the contractor's ability to provide operationally critical support, and (ii) Rapidly compromised covered defense information systems on the Contractor's contractor's ability to provide operationally critical support, and the incident in order to identify compromised covered defense 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 systems on the Contractor's depend to yber incidents to DoD and shall include, at a minimum, the required elements</li></ul></li></ul>			
<ul> <li>practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures when the Contractor easonably determines that information systems security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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—         <ul> <li>(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 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 created by or for DoD and shall include, at a minimum, the required elements a thtp://dibnet.dod.mil.</li> <li>(3) Medium assurance certificate requirement. In order to report cyber incidents in DoD and thy://dibnet.dod.mil.</li> </ul> </li> </ul>			
<ul> <li>any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or</li> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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 information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor 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 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</li> <li>(i) 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.</li> <li>(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 me</li></ul>		practical, but not later than December 31, 2017. The C	Contractor shall notify the
time of contract award; or (B) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. (c) <i>Cyber incident reporting requirement.</i> (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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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 incide			
<ul> <li>(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</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) <i>Cyber incident reporting requirement</i>.</li> <li>(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— <ul> <li>(i) Conduct a review for evidence of compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information systems on the Contractor's onetwork(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information give the incident in order to identify compromised covered defense information asystem(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 <ul> <li>(i) Cyber incident report. The cyber incidents to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(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.</li> <li>(3) Medium assurance certificate require</li></ul></li></ul>			71 not implemented at the
the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO; and (2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. (c) <i>Cyber incident reporting requirement</i> . (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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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			used to compensate for
<ul> <li>accepted in writing by an authorized representative of the DoD CIO; and</li> <li>(2) Apply other information systems security measures when the Contractor easonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) <i>Cyber incident reporting requirement.</i> <ul> <li>(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— <ul> <li>(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 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 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, 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</li> <li>(ii) Rapidly report 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.</li> </ul> </li> </ul></li></ul>			
<ul> <li>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.</li> <li>(c) <i>Cyber incident reporting requirement.</i> <ul> <li>(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— <ul> <li>(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, contractor's ability to provide operationally critical support; and</li> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(2) <i>Cyber incident report.</i> The cyber incident the trated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.</li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul></li></ul>			
<ul> <li>be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.</li> <li>(c) <i>Cyber incident reporting requirement.</i> <ul> <li>(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— <ul> <li>(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, envice operationally critical support; and</li> <li>(ii) Rapidly report 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.</li> </ul> </li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul></li></ul>			
<ul> <li>vulnerability.</li> <li>(c) Cyber incident reporting requirement.</li> <li>(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— <ul> <li>(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</li> <li>(ii) Rapidly report cyber incident to DoD at http://dibnet.dod.mil.</li> </ul> </li> <li>(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.</li> <li>(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</li> </ul>			
<ul> <li>(c) Cyber incident reporting requirement.</li> <li>(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—         <ul> <li>(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</li> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>			issessed fisk of
<ul> <li>(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—         <ul> <li>(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, correct or identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and             <ul> <li>(ii) Rapidly report 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.</li> <li>(2) <i>Cyber incident report.</i> 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.</li> <li>(3) <i>Medium assurance certificate requirement.</i> 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</li> </ul> </li> </ul></li></ul>			
<ul> <li>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—         <ul> <li>(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</li></ul></li></ul>			tor information system or
<ul> <li>(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         <ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>	the	covered defense information residing therein, or that affects the contractor's a	bility to perform the
<ul> <li>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</li></ul>	requ		
<ul> <li>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</li></ul>			
<ul> <li>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         <ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul> </li> </ul>			
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) <i>Cyber incident report.</i> 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) <i>Medium assurance certificate requirement.</i> 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			
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			
<ul> <li>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</li> <li>(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.</li> <li>(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</li> </ul>			fect the Contractor's ability
<ul> <li>(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.</li> <li>(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</li> </ul>			
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	(2) (		
(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	(2) ( shal	Linclude, at a minimum, the required elements at http://dibnet.dod.mil	Greated by OFIDE DOD allo
or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information			this clause, the Contractor
	or subcontractor shall	have or acquire a DoD-approved medium assurance certificate to report cybe	r incidents. For information

(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.

(I) 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)

### **Schedule of Supplies**

**Item Description**: Beverage, Carbonated and/or Non-Carbonated, Various Flavors including Coke Classic, Diet Coke, and Sprite, 12 ounce cans, 24 per case. Case price is

- Beverage, Carbonated and/or Non-Carbonated, Various Flavors including Coke Classic, Diet Coke, and Sprite, 20 ounce bottle, 24 per case. Case price is

Invoicing and Payment: Dorian Teasley 600 Beacon Parkway West Suite 601 Birmingham, AL 35209 Phone – 205-238-3325 Fax – 205-238-3308

Vendor Contact Information for Orders: Customer Solutions Center 600 Beacon Parkway West Birmingham, AL 35209 Fax – 205-808-7120 Chandler Crane – direct – 205-943-6748, ext 26748 Jennifer McPeters – direct – 205-943-6701, ext 26701 Kelsie Boylan, NRS Director – Military, 504-915-5040 Lauren Sapp, NRS Analyst – Military, 912-602-0976

# <u>A DELIVERY TICKET</u> WILL ACCOMPANY EACH DELIVERY ORDER CITING ORDER NUMBER, UNIT PRICE, BE ITEMIZED, EXTENDED AND TOTALED.

PRICES CITED ON DELIVERY TICKET FOR STORES SITES WILL BE PRICES AT THE TIME OF ORDER AND NOT THE PRICES AT TIME OF DELIVERY.

#### **DELIVERIES AND PERFORMANCE:**

ALL DELIVERIES EXCLUDE NATIONAL LEGAL HOLIDAYS UNLESS OTHERWISE INDICATED BY ORDERING ACTIVITY.

#### **INSPECTION:**

CONTRACTOR'S DELIVERY VEHICLES WILL STOP AND REPORT TO THE INSPECTION POINTS AS DESIGNATED FOR INSPECTION OF PRODUCTS BEFORE PROCEEDING TO ANY OTHER DESIGNATED DELIVERY POINT.

#### **Blanket Purchase Agreement (BPA) Terms and Conditions**

#### 1. Description of Agreement

- a. The supplier shall furnish items as set forth in this BPA Document if and when requested by the contracting officer or the authorized representative of the contracting officer during the period commencing on the effective date of this agreement as indicated in **Block 3** of the **DD Form 1155** and ending **FIVE years** from the effective date unless advance written notice of cancellation is received from either party prior to the expiration date.
- b. The supplier shall only provide the products as indicated in this agreement or its modifications. The product description and/or specifications are provided on page **6** Schedule of Supplies.
- c. All items delivered shall be produced, processed and prepared in accordance with the highest commercial standard practices, and shall conform to those products the contractor offers for resale in retail outlets, and shall be produced in an approved production facility.

#### 2. Extent of Obligation

The government is obligated only to the extent of authorized purchases actually made under this agreement.

#### 3. Pricing

- a. The supplier warrants that prices set forth in each call are as low as, or lower than; those charged his most favored customer for comparable quantities under similar terms and conditions, in addition to any discounts for prompt payments.
- b. Prices shall be firm fixed for a twelve-month period.
- c. The supplier is responsible for notifying the Contracting Officer, in writing, 60 days prior to the end of the twelve-month period of any requested price changes. If the supplier does not contact the Contracting Officer with a price change request, the previous year's prices will remain in effect.
- d. All prices are FOB Destination.

#### 4. Purchase Limitation

See paragraph 5 below.

#### 5. Individuals Authorized to Place Orders

- a. The individuals authorized to place orders against this BPA and the dollar limitation per order are as follows:
  - (1) The designated Food Service Ordering Officer(s) at the dining facilities listed in paragraph 10 below. They are limited to <u>\$3000.00</u> per order.
  - (2) The DLA Troop Support Soda Team Contracting Officer(s) and/or Soda Team Contract Specialist(s). They have no restriction per order.
- b. The supplier may only accept orders from individuals identified as being authorized to place orders under this BPA.
- c. All orders must be placed through STORES or other authorized Government purchasing system.

#### 6. Deliveries

- a. All deliveries shall be made as indicated by the BPA order.
- b. Only those products specifically listed in this BPA are authorized for delivery. Delivery of unauthorized products shall be at the risk of and the sole responsibility of the supplier and may result in non-payment as well as cancellation of this agreement.
- c. Partial shipments may not be accepted.
- d. Dining facilities shall return or exchange plastic shipping containers and pallets at the time of delivery.

#### 7. Delivery Tickets

- a. All shipments under this agreement shall be accompanied by delivery tickets or sales slips which shall contain the following minimum information:
  - (1) Name of Supplier.
  - (2) 13 Position STORES/ SAP Number. (i.e. SPE300-17-D-XXXX)
  - (3) Four Position Call Number (i.e. 131A)-Last position may be an Alpha or a Numeric figure.
  - (4) Date of Purchase.
  - (5) Itemized List of Supplies Furnished.
  - (6) Quantity, unit price, and extension of each item, less applicable discounts (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided that the invoice is itemized to show this information).
  - (7) Date of Delivery or Shipment.
- b. The customer shall sign a copy of the delivery ticket to signify acceptance of the product. Failure by the vendor to provide a delivery ticket at time of delivery may result in nonpayment.

#### 8. Marking Requirements

Standard commercial markings for individual packages will be used to clearly mark and identify the nature of contents and the expiration date. All markings shall be clear, legible, non-fading and durable.

#### 9. Invoices

Invoicing shall be done via the DLA Troop Support Web Invoicing Tool. Manual invoices will not be processed.

#### **10. Delivery Locations**

- a. All locations on Keesler Air Force Base, Mississippi including but not limited to:
- BLDG 6960, 611 PARADE LN (FT9056)
- BLDG 7409, 800 FALCON ST (FT9054)
- KEESLER NUTRITIONAL FLIGHT MEDICINE, 301 FISHER ST STE 101 (FM3010) Delivery days and times shall be agreed upon by the vendor and the customer. Once agreed upon, a change in the delivery days and times MUST be agreed upon by the vendor and the customer.
- b. Delivery lead time: 48 hours or more from vendor receipt of order via Electronic Business System (EBS).

### 11. Acceptance

Government acceptance of product shall be at the customer's delivery location.

### 12. Additional Ordering Procedures/Requirements

- a. Ordering under this BPA shall be accomplished through the STORES/SAP system only. An electronically transmitted order will be sent via a facsimile from the customer to the supplier. An order/call number will be furnished to the supplier via electronically transmitted facsimile STORES Purchase Orders. The supplier is required to insert the order/call number on the delivery ticket/invoice
- b. Ordering activities shall place orders at least three working days prior to required delivery date.
- c. Authorized personnel shall not order products other than those listed in this BPA.
- d. Individual orders in excess of \$3,000 will be placed by DLA Troop Support authorized personnel.
- e. Bottler will not accept orders placed via telephone or email.

### 13. Additional Responsibilities of the Supplier

- a. The supplier's/suppliers' authorized official shall indicate acceptance of this BPA by providing the information required at Block 16 on Page 1 of this agreement.
- b. One copy of the completed BPA shall be returned to the Contract Specialist: (Emailed copies are acceptable and all copies of the BPA must be sent to <u>Michelle.J.Moore@dla.mil</u>).

Mailed copies can be sent to the following address: DLA Troop Support Directorate of Subsistence 700 Robbins Avenue Philadelphia, PA 19111-5092

- c. The supplier is also required to complete the applicable representation/certifications at clauses unless already on file in the System for Award Management: 252.209-7991 Representation by Corporations Regarding an Unpaid Delinquent Tax Liability or a Felony Conviction under any Federal Law—Fiscal Year 2016 Appropriations (DEVIATION 2015-00005) (DEC 2014); 52.212-3 entitled Offeror Representations and Certifications-Commercial Items; 252.225-7000 entitled Buy American Act Balance of Payments Program Certificate; and 52.215-6 Place of Performance (Oct 1997).
- d. The supplier is responsible for notifying the Contracting Officer, in writing, 60 days prior to the end of the twelve-month period of any price changes. If the supplier does not contact the Contracting Officer with price changes, the previous year prices will remain in effect.

#### 14. Right to Award other Contracts and Orders

The Government reserves the right to award orders to other suppliers for like products during the same performance period as this Blanket Purchase Agreement.

#### 15. North American Industry Classification System (NAICS) Code and Small Business Size Standard

The NAICS code and small business size standard for this acquisition are 312111 and 500, respectively.

#### **Non-Compete Provision**

The offeror warrants that it will not actively promote, encourage, or market any of the customers on this acquisition away from a resultant DLA Troop Support contract and onto a contract of any other Government agency or commercial entity. This prohibition applies both on a pre-award and post-award basis.

#### **Food Defense / Force Protection**

DLA Troop Support Subsistence Directorate provides world-wide subsistence logistics support during peace time as well as during regional conflicts, contingency operations, national emergencies, and natural disasters. At any time, the United States Government, its personnel, resources and interests may be the target of enemy aggression to include espionage, sabotage, or terrorism. This increased risk requires DLA Troop Support to take steps to ensure measures are taken to prevent the deliberate tampering and contamination of subsistence items. The offeror must ensure that products and/or packaging have not been tampered with or contaminated throughout the growing, storage, and delivery process. Contract awardee will ensure to complete security of all conveyances to any military installations. The offeror must immediately inform DLA Troop Support Subsistence of any attempt or suspected attempt by any party or parties, known or unknown, to tamper with or contaminate subsistence supplies. As the holder of a contract with the Department of Defense, the awardees should be aware of the vital role they play in supporting our customers. It is incumbent upon the awardees to take all necessary actions to secure product delivered to all military customers, as well as any applicable commercial destinations.

#### **Provisions and Clauses**

#### **Deviation 2016-00002**

Class Deviation-Prohibition Against Using Fiscal Year 2016 Funds to Contract with Corporations that have an Unpaid Delinquent Tax Liability or Felony Conviction under Federal Law

# DFARS 252.209-7991 Representation by Corporations Regarding an Unpaid Delinquent Tax Liability or a Felony Conviction under any Federal Law—Fiscal Year 2016 Appropriations.

#### REPRESENTATION BY CORPORATIONS REGARDING AN UNPAID DELINQUENT TAX LIABILITY OR A FELONY CONVICTION UNDER ANY FEDERAL LAW—FISCAL YEAR 2016 APPROPRIATIONS (DEVIATION 2016-00002) (OCT 2015)

(a) In accordance with section 101(a) of the Continuing Appropriations Act, 2016 (Pub. L. 114-53) and any subsequent FY 2016 appropriations act that extends to FY 2016 funds the same restrictions as are contained in sections 744 and 745 of division E, title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), none of the funds made available by this or any other Act may be used to enter into a contract with any corporation that—

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that—

(1) It **is [] is not [] a corporation** that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability,

(2) It **is [] is not [] a corporation** that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

#### **52.212-3 Offeror Representations and Certifications -- Commercial Items** (Jan 2017)

The offeror shall complete only paragraphs (b) of this provision if the Offeror has completed the annual representations and certification electronically via the System for Award Management (SAM) Web site located at http://www.sam.gov/portal. If the Offeror has not completed the annual representations and certifications electronically, the Offeror shall complete only paragraphs (c) through (u) of this provision.

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

"Administrative merits determination" means certain notices or findings of labor law violations issued by an enforcement agency following an investigation. An administrative merits determination may be final or be subject to appeal or further review. To determine whether a particular notice or finding is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.

"Arbitral award or decision" means an arbitrator or arbitral panel determination that a labor law violation occurred, or that enjoined or restrained a violation of labor law. It includes an award or decision that is not final or is subject to being confirmed, modified, or vacated by a court, and includes an award or decision resulting from private or confidential proceedings. To determine whether a particular award or decision is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.

"Civil judgment" means--

(1) In paragraph (h) of this provision: A judgment or finding of a civil offense by any court of competent jurisdiction.

(2) In paragraph (s) of this provision: Any judgment or order entered by any Federal or State court in which the court determined that a labor law violation occurred, or enjoined or restrained a violation of labor law. It includes a judgment or order that is not final or is subject to appeal. To determine whether a particular judgment or order is covered by this definition, it is necessary to consult section II.B. in the DOL Guidance.

"DOL Guidance" means the Department of Labor (DOL) Guidance entitled: "Guidance for Executive Order 13673, 'Fair Pay and Safe Workplaces' ". The DOL Guidance, dated August 25, 2016, can be obtained from www.dol.gov/fairpayandsafeworkplaces.

"Economically disadvantaged women-owned small business (EDWOSB) concern" means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127. It automatically qualifies as a women-owned small business eligible under the WOSB Program.

"Enforcement agency" means any agency granted authority to enforce the Federal labor laws. It includes the enforcement components of DOL (Wage and Hour Division, Office of Federal Contract Compliance Programs, and Occupational Safety and Health Administration), the Equal Employment Opportunity Commission, the Occupational Safety and Health Review Commission, and the National Labor Relations Board. It also means a State agency designated to administer an OSHA-approved State Plan, but only to the extent that the State agency is acting in its capacity as administrator of such plan. It does not include other Federal agencies which, in their capacity as contracting agencies, conduct investigations of potential labor law violations. The enforcement agencies associated with each labor law under E.O. 13673 are--

(1) Department of Labor Wage and Hour Division (WHD) for--

(i) The Fair Labor Standards Act;

(ii) The Migrant and Seasonal Agricultural Worker Protection Act;

(iii) 40 U.S.C. chapter 31, subchapter IV, formerly known as the Davis-Bacon Act;

(v) 41 U.S.C. chapter 67, formerly known as the Service Contract Act;

(vi) The Family and Medical Leave Act; and

(vii) E.O. 13658 of February 12, 2014 (Establishing a Minimum Wage for Contractors);

(2) Department of Labor Occupational Safety and Health Administration (OSHA) for--

(i) The Occupational Safety and Health Act of 1970; and

(ii) OSHA-approved State Plans;

(4) Department of Labor Office of Federal Contract Compliance Programs (OFCCP) for--

(i) Section 503 of the Rehabilitation Act of 1973;

(ii) The Vietnam Era Veterans' Readjustment Assistance Act of 1972 and the Vietnam Era Veterans' Readjustment Assistance Act of 1974; and

(iii) E.O. 11246 of September 24, 1965 (Equal Employment Opportunity);

(5) National Labor Relations Board (NLRB) for the National Labor Relations Act; and

(6) Equal Employment Opportunity Commission (EEOC) for--

(i) Title VII of the Civil Rights Act of 1964;

(ii) The Americans with Disabilities Act of 1990;

(iii) The Age Discrimination in Employment Act of 1967; and

(iv) Section 6(d) of the Fair Labor Standards Act (Equal Pay Act).

"Forced or indentured child labor" means all work or service—

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

"Highest-level owner" means the entity that owns or controls an immediate owner of the offeror, or that owns or controls one or more entities that control an immediate owner of the offeror. No entity owns or exercises control of the highest level owner.

"Immediate owner" means an entity, other than the offeror, that has direct control of the offeror. Indicators of control include, but are not limited to, one or more of the following: Ownership or interlocking management, identity of interests among family members, shared facilities and equipment, and the common use of employees.

"Inverted domestic corporation," means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

"Labor compliance agreement" means an agreement entered into between a contractor or subcontractor and an enforcement agency to address appropriate remedial measures, compliance assistance, steps to resolve issues to increase compliance with the labor laws, or other related matters.

"Labor laws" means the following labor laws and E.O.s:

- (1) The Fair Labor Standards Act.
- (2) The Occupational Safety and Health Act (OSHA) of 1970.
- (3) The Migrant and Seasonal Agricultural Worker Protection Act.
- (4) The National Labor Relations Act.
- (5) 40 U.S.C. chapter 31, subchapter IV, formerly known as the Davis-Bacon Act.
- (6) 41 U.S.C. chapter 67, formerly known as the Service Contract Act.
- (7) E.O. 11246 of September 24, 1965 (Equal Employment Opportunity).
- (8) Section 503 of the Rehabilitation Act of 1973.

(9) The Vietnam Era Veterans' Readjustment Assistance Act of 1972 and the Vietnam Era Veterans' Readjustment Assistance Act of 1974.

- (10) The Family and Medical Leave Act.
- (11) Title VII of the Civil Rights Act of 1964.
- (12) The Americans with Disabilities Act of 1990.
- (13) The Age Discrimination in Employment Act of 1967.
- (14) E.O. 13658 of February 12, 2014 (Establishing a Minimum Wage for Contractors).

(15) Equivalent State laws as defined in the DOL Guidance. (The only equivalent State laws implemented in the FAR are OSHA-approved State Plans, which can be found at

www.osha.gov/dcsp/osp/approved\_state\_plans.html).

"Labor law decision" means an administrative merits determination, arbitral award or decision, or civil judgment, which resulted from a violation of one or more of the laws listed in the definition of "labor laws".

"Manufactured end product" means any end product in product and service codes (PSCs) 1000-9999, except— (1) PSC 5510, Lumber and Related Basic Wood Materials;

- (2) Product or Service Group (PSG) 87, Agricultural Supplies;
- (3) PSG 88, Live Animals;
- (4) PSG 89, Subsistence;
- (5) PSC 9410, Crude Grades of Plant Materials;
- (6) PSC 9430, Miscellaneous Crude Animal Products, Inedible;
- (7) PSC 9440, Miscellaneous Crude Agricultural and Forestry Products;
- (8) PSC 9610, Ores;
- (9) PSC 9620, Minerals, Natural and Synthetic; and
- (10) PSC 9630, Additive Metal Materials.

"Place of manufacture" means the place where an end product is assembled out of components, or otherwise made or processed from raw materials into the finished product that is to be provided to the Government. If a product is disassembled and reassembled, the place of reassembly is not the place of manufacture.

"Predecessor" means an entity that is replaced by a successor and includes any predecessors of the predecessor. "Restricted business operations" means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudar;

(2) Are conducted pursuant to specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology-

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

"Service-disabled veteran-owned small business concern"-

(1) Means a small business concern—

(i) Not less than 51 percent of which is owned by one or more service-disabled veterans or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more service-disabled veterans; and

(ii) The management and daily business operations of which are controlled by one or more service-disabled veterans or, in the case of a service-disabled veteran with permanent and severe disability, the spouse or permanent caregiver of such veteran.

(2) Service-disabled veteran means a veteran, as defined in 38 U.S.C. 101(2), with a disability that is service-connected, as defined in 38 U.S.C. 101(16).

"Small business concern" means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR Part 121 and size standards in this solicitation.

"Small disadvantaged business concern, consistent with 13 CFR 124.1002," means a small business concern under the size standard applicable to the acquisition, that--

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by--

(i) One or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States; and

(ii) Each individual claiming economic disadvantage has a net worth not exceeding 750,000 after taking into account the applicable exclusions set forth at 13 CFR 124.104(c)(2); and

(2) The management and daily business operations of which are controlled (as defined at 13.CFR 124.106) by individuals, who meet the criteria in paragraphs (1)(i) and (ii) of this definition.

"Subsidiary" means an entity in which more than 50 percent of the entity is owned—

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

"Successor" means an entity that has replaced a predecessor by acquiring the assets and carrying out the affairs of the predecessor under a new name (often through acquisition or merger). The term "successor" does not include new offices/divisions of the same company or a company that only changes its name. The extent of the responsibility of the successor for the liabilities of the predecessor may vary, depending on State law and specific circumstances.

"Veteran-owned small business concern" means a small business concern-

(1) Not less than 51 percent of which is owned by one or more veterans(as defined at 38 U.S.C. 101(2)) or, in the case of any publicly owned business, not less than 51 percent of the stock of which is owned by one or more veterans; and

(2) The management and daily business operations of which are controlled by one or more veterans.

"Women-owned business concern" means a concern which is at least 51 percent owned by one or more women; or in the case of any publicly owned business, at least 51 percent of the its stock is owned by one or more women; and whose management and daily business operations are controlled by one or more women.

"Women-owned small business concern" means a small business concern --

(1) That is at least 51 percent owned by one or more women or, in the case of any publicly owned business, at least 51 percent of the stock of which is owned by one or more women; and

(2) Whose management and daily business operations are controlled by one or more women.

"Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127)," means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States.

Note to paragraph (a): By a court order issued on October 24, 2016, the following definitions in this paragraph (a) are enjoined indefinitely as of the date of the order: "Administrative merits determination", "Arbitral award or decision", paragraph (2) of "Civil judgment", "DOL Guidance", "Enforcement agency", "Labor compliance agreement", "Labor laws", and "Labor law decision". The enjoined definitions will become effective immediately if the court terminates the injunction. At that time, DoD, GSA, and NASA will publish a document in the Federal Register advising the public of the termination of the injunction.

(b)

(1) Annual Representations and Certifications. Any changes provided by the offeror in paragraph (b)(2) of this provision do not automatically change the representations and certifications posted on the SAMwebsite.

(2) The offeror has completed the annual representations and certifications electronically via the SAM website accessed through https://www.acquisition.gov. After reviewing the SAM database information, the offeror verifies by submission of this offer that the representation and certifications currently posted electronically at FAR 52.212-3, Offeror Representations and Certifications—Commercial Items, have been entered or updated in the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201), except for paragraphs \_\_\_\_\_\_. [Offeror to identify the applicable paragraphs at (c) through (u) of this provision that the offeror has completed for the purposes of this solicitation only, if any. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer. Any changes provided by the offeror are applicable to this solicitation only, and do not result in an update to the representations and certifications offer and are solicitations and certifications posted electronically on SAM.]

(c) Offerors must complete the following representations when the resulting contract is to be performed in the United States or its outlying areas. Check all that apply.

(1) Small business concern. The offeror represents as part of its offer that it [\_] is, [\_] is not a small business concern.

(2) Veteran-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents as part of its offer that it [\_] is, [\_] is not a veteran-owned small business concern.

(3) Service-disabled veteran-owned small business concern. [Complete only if the offeror represented itself as a veteran-owned small business concern in paragraph (c)(2) of this provision.] The offeror represents as part of its offer that it [\_] is, [\_] is not a service-disabled veteran-owned small business concern.

(4) Small disadvantaged business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [\_] is, [\_] is not, a small disadvantaged business concern as defined in 13 CFR 124.1002.

(5) Women-owned small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it  $[\_]$  is,  $[\_]$  is not a women-owned small business concern.

Note: Complete paragraphs (c)(8) and (c)(9) only if this solicitation is expected to exceed the simplified acquisition threshold.

(6) WOSB concern eligible under the WOSB Program. [Complete only if the offeror represented itself as a women-owned small business concern in paragraph (c)(5) of this provision.] The offeror represents that—

(i) It [\_] is, [\_] is not a WOSB concern eligible under the WOSB Program, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It [\_] is, [\_] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(6)(i) of this provision is accurate for each WOSB concern eligible under the WOSB Program participating in the joint venture. [The offeror shall enter the name or names of the WOSB concern eligible under the WOSB Program and other small businesses that are participating in the joint venture:

\_\_\_\_\_.] Each WOSB concern eligible under the WOSB Program participating in the joint venture shall submit a separate signed copy of the WOSB representation.

(7) Economically disadvantaged women-owned small business (EDWOSB) concern. [Complete only if the offeror represented itself as a WOSB concern eligible under the WOSB Program in (c)(6) of this provision.] The offeror represents that—

(i) It [\_] is, [\_] is not an EDWOSB concern, has provided all the required documents to the WOSB Repository, and no change in circumstances or adverse decisions have been issued that affects its eligibility; and

(ii) It [\_] is, [\_] is not a joint venture that complies with the requirements of 13 CFR part 127, and the representation in paragraph (c)(7)(i) of this provision is accurate for each EDWOSB concern participating in the joint venture. [The offeror shall enter the name or names of the EDWOSB concern and other small businesses that are participating in the joint venture: \_\_\_\_\_\_.] Each EDWOSB concern participating in the joint venture shall submit a separate signed copy of the EDWOSB representation.

(8) Women-owned business concern (other than small business concern). [Complete only if the offeror is a women-owned business concern and did not represent itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents that it [\_] is, a women-owned business concern.

(9) Tie bid priority for labor surplus area concerns. If this is an invitation for bid, small business offerors may identify the labor surplus areas in which costs to be incurred on account of manufacturing or production (by offeror or first-tier subcontractors) amount to more than 50 percent of the contract price:

(10) HUBZone small business concern. [Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.] The offeror represents, as part of its offer, that--

(i) It [\_] is, [\_] is not a HUBZone small business concern listed, on the date of this representation, on the List of Qualified HUBZone Small Business Concerns maintained by the Small Business Administration, and no material changes in ownership and control, principal office, or HUBZone employee percentage have occurred since it was certified in accordance with 13 CFR part 126; and

(ii) It [\_] is, [\_] is not a HUBZone joint venture that complies with the requirements of 13 CFR part 126, and the representation in paragraph (c)(10)(i) of this provision is accurate for each HUBZone small business concern participating in the HUBZone joint venture. [The offeror shall enter the names of each of the HUBZone small business concern participating in the HUBZone joint venture: \_\_\_\_\_\_.] Each HUBZone small business concern participating in the HUBZone joint venture shall submit a separate signed copy of the HUBZone representation.

(d) Representations required to implement provisions of Executive Order 11246 --

(1) Previous contracts and compliance. The offeror represents that --

(i) It [\_] has, [\_] has not, participated in a previous contract or subcontract subject to the Equal Opportunity clause of this solicitation; and

(ii) It [\_] has, [\_] has not, filed all required compliance reports.

(2) Affirmative Action Compliance. The offeror represents that --

(i) It [\_] has developed and has on file, [\_] has not developed and does not have on file, at each establishment, affirmative action programs required by rules and regulations of the Secretary of Labor (41 CFR parts 60-1 and 60-2), or

(ii) It [\_] has not previously had contracts subject to the written affirmative action programs requirement of the rules and regulations of the Secretary of Labor.

(e) Certification Regarding Payments to Influence Federal Transactions (31 U.S.C. 1352). (Applies only if the contract is expected to exceed \$150,000.) By submission of its offer, the offeror certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress on his or her behalf in connection with the award of any resultant contract. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(f) Buy American Certificate. (Applies only if the clause at Federal Acquisition Regulation (FAR) 52.225-1, Buy American – Supplies, is included in this solicitation.)

(1) The offeror certifies that each end product, except those listed in paragraph (f)(2) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product." The terms "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," and "United States" are defined in the clause of this solicitation entitled "Buy American—Supplies."

(2) Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(3) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. (g)

(1) Buy American -- Free Trade Agreements -- Israeli Trade Act Certificate. (Applies only if the clause at FAR 52.225-3, Buy American -- Free Trade Agreements -- Israeli Trade Act, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(1)(ii) or (g)(1)(iii) of this provision, is a domestic end product and that for other than COTS items, the offeror has considered components of unknown origin to have been mined, produced, or manufactured outside the United States. The terms "Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end product," "commercially available off-the-shelf (COTS) item," "component," "domestic end product," "end product," "foreign end product," "Free Trade Agreement country," "Free Trade Agreement country end product," "Israeli end product," and "United States" are defined in the clause of this solicitation entitled "Buy American--Free Trade Agreements--Israeli Trade Act."

(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Free Trade Agreement Country End Products (Other than Bahrainian, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iii) The offeror shall list those supplies that are foreign end products (other than those listed in paragraph (g)(1)(ii) or this provision) as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act." The offeror shall list as other foreign end products those end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (2) of the definition of "domestic end product." Other Foreign End Products:

LINE ITEM NO.	COUNTRY OF ORIGIN

[List as necessary]

(iv) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25.

(2) Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate I. If Alternate I to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(i) for paragraph (g)(1)(i) of the basic provision:

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act":

Canadian End Products:

Line Item No.:

[List as necessary]

(g)(1)(ii) The offeror certifies that the following supplies are Canadian end products or Israeli end products as defined in the clause of this solicitation entitled "Buy American--Free Trade Agreements--Israeli Trade Act": Canadian or Israeli End Products:

Line Item No.:	Country of Origin:

[List as necessary]

<sup>(3)</sup> Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate II. If Alternate II to the clause at FAR 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

<sup>(4)</sup> Buy American—Free Trade Agreements—Israeli Trade Act Certificate, Alternate III. If Alternate III to the clause at 52.225-3 is included in this solicitation, substitute the following paragraph (g)(1)(ii) for paragraph (g)(1)(ii) of the basic provision:

<sup>(</sup>g)(1)(ii) The offeror certifies that the following supplies are Free Trade Agreement country end products (other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian end products) or Israeli end products as defined in the clause of this solicitation entitled "Buy American—Free Trade Agreements—Israeli Trade Act": Free Trade Agreement Country End Products (Other than Bahrainian, Korean, Moroccan, Omani, Panamanian, or Peruvian End Products) or Israeli End Products:

Line Item No.:	Country of Origin:	

[List as necessary]

(5) Trade Agreements Certificate. (Applies only if the clause at FAR 52.225-5, Trade Agreements, is included in this solicitation.)

(i) The offeror certifies that each end product, except those listed in paragraph (g)(5)(ii) of this provision, is a U.S.-made or designated country end product as defined in the clause of this solicitation entitled "Trade Agreements."

(ii) The offeror shall list as other end products those end products that are not U.S.-made or designated country end products.

Other End Products

Line Item No.:	Country of Origin:

[List as necessary]

(iii) The Government will evaluate offers in accordance with the policies and procedures of FAR Part 25. For line items covered by the WTO GPA, the Government will evaluate offers of U.S.-made or designated country end products without regard to the restrictions of the Buy American statute. The Government will consider for award only offers of U.S.-made or designated country end products unless the Contracting Officer determines that there are no offers for such products or that the offers for such products are insufficient to fulfill the requirements of the solicitation.

(h) Certification Regarding Responsibility Matters (Executive Order 12689). (Applies only if the contract value is expected to exceed the simplified acquisition threshold.) The offeror certifies, to the best of its knowledge and belief, that the offeror and/or any of its principals--

(1) [\_] Are, [\_] are not presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;

(2) [\_] Have, [\_] have not, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a Federal, state or local government contract or subcontract; violation of Federal or state antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property; and

(3) [\_] Are, [\_] are not presently indicted for, or otherwise criminally or civilly charged by a Government entity with, commission of any of these offenses enumerated in paragraph (h)(2) of this clause; and

(4) [\_] Have, [\_] have not, within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds \$3,500 for which the liability remains unsatisfied.

(i) Taxes are considered delinquent if both of the following criteria apply:

(A) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if there is a pending administrative or judicial challenge. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(B) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) Examples.

(A) The taxpayer has received a statutory notice of deficiency, under I.R.C. §6212, which entitles the taxpayer to seek Tax Court review of a proposed tax deficiency. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek Tax Court review, this will not be a final tax liability until the taxpayer has exercised all judicial appear rights.

(B) The IRS has filed a notice of Federal tax lien with respect to an assessed tax liability, and the taxpayer has been issued a notice under I.R.C. §6320 entitling the taxpayer to request a hearing with the IRS Office of Appeals Contesting the lien filing, and to further appeal to the Tax Court if the IRS determines to sustain the lien filing. In the course of the hearing, the taxpayer is entitled to contest the underlying tax liability because the taxpayer has had no prior opportunity to contest the liability. This is not a delinquent tax because it is not a final tax liability. Should the taxpayer seek tax court review, this will not be a final tax liability until the taxpayer has exercised all judicial appeal rights.

(C) The taxpayer has entered into an installment agreement pursuant to I.R.C. §6159. The taxpayer is making timely payments and is in full compliance with the agreement terms. The taxpayer is not delinquent because the taxpayer is not currently required to make full payment.

(D) The taxpayer has filed for bankruptcy protection. The taxpayer is not delinquent because enforced collection action is stayed under 11 U.S.C. §362 (the Bankruptcy Code).

(i) Certification Regarding Knowledge of Child Labor for Listed End Products (Executive Order 13126). [The Contracting Officer must list in paragraph (i)(1) any end products being acquired under this solicitation that are included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, unless excluded at 22.1503(b).]

(1) Listed End Product

Listed End Product:	Listed Countries of Origin:

(2) Certification. [If the Contracting Officer has identified end products and countries of origin in paragraph (i)(1) of this provision, then the offeror must certify to either (i)(2)(i) or (i)(2)(i) by checking the appropriate block.]

[\_] (i) The offeror will not supply any end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product.

[\_] (ii) The offeror may supply an end product listed in paragraph (i)(1) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that is has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture any such end product furnished under this contract. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(j) Place of manufacture. (Does not apply unless the solicitation is predominantly for the acquisition of manufactured end products.) For statistical purposes only, the offeror shall indicate whether the place of manufacture of the end products it expects to provide in response to this solicitation is predominantly—

(1) [\_] In the United States (Check this box if the total anticipated price of offered end products manufactured in the United States exceeds the total anticipated price of offered end products manufactured outside the United States); or

(2) [\_] Outside the United States.

(k) Certificates regarding exemptions from the application of the Service Contract Labor Standards. (Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services.) [The contracting officer is to check a box to indicate if paragraph (k)(1) or (k)(2) applies.]

(1) [\_] Maintenance, calibration, or repair of certain equipment as described in FAR 22.1003-4(c)(1). The offeror [\_] does [\_] does not certify that—

(i) The items of equipment to be serviced under this contract are used regularly for other than Governmental purposes and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontract) in substantial quantities to the general public in the course of normal business operations;

(ii) The services will be furnished at prices which are, or are based on, established catalog or market prices (see FAR 22.1003-4(c)(2)(ii)) for the maintenance, calibration, or repair of such equipment; and

(iii) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract will be the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(2) [\_] Certain services as described in FAR 22.1003-4(d)(1). The offeror [\_] does [\_] does not certify that—

(i) The services under the contract are offered and sold regularly to non-Governmental customers, and are provided by the offeror (or subcontractor in the case of an exempt subcontract) to the general public in substantial quantities in the course of normal business operations;

(ii) The contract services will be furnished at prices that are, or are based on, established catalog or market prices (see FAR 22.1003-4(d)(2)(iii));

(iii) Each service employee who will perform the services under the contract will spend only a small portion of his or her time (a monthly average of less than 20 percent of the available hours on an annualized basis, or less than 20 percent of available hours during the contract period if the contract period is less than a month) servicing the Government contract; and

(iv) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract is the same as that used for these employees and equivalent employees servicing commercial customers.

(3) If paragraph (k)(1) or (k)(2) of this clause applies—

(i) If the offeror does not certify to the conditions in paragraph (k)(1) or (k)(2) and the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation, the offeror shall notify the Contracting Officer as soon as possible; and

(ii) The Contracting Officer may not make an award to the offeror if the offeror fails to execute the certification in paragraph (k)(1) or (k)(2) of this clause or to contact the Contracting Officer as required in paragraph (k)(3)(i) of this clause.

(l) Taxpayer identification number (TIN) (26 U.S.C. 6109, 31 U.S.C. 7701). (Not applicable if the offeror is required to provide this information to the SAM database to be eligible for award.)

(1) All offerors must submit the information required in paragraphs (l)(3) through (l)(5) of this provision to comply with debt collection requirements of 31 U.S.C. 7701(c) and 3325(d), reporting requirements of 26 U.S.C. 6041, 6041A, and 6050M, and implementing regulations issued by the Internal Revenue Service (IRS). (2) The TIN may be used by the government to collect and report on any delinquent amounts arising out of the offeror's relationship with the Government (31 U.S.C. 7701(c)(3)). If the resulting contract is subject to the payment reporting requirements described in FAR 4.904, the TIN provided hereunder may be matched with IRS records to verify the accuracy of the offeror's TIN.

(3) Taxpayer Identification Number (TIN).

[\_] TIN:\_

[\_] TIN has been applied for.

[\_] TIN is not required because:

[\_] Offeror is a nonresident alien, foreign corporation, or foreign partnership that does not have income effectively connected with the conduct of a trade or business in the United States and does not have an office or place of business or a fiscal paying agent in the United States;

[\_] Offeror is an agency or instrumentality of a foreign government;

[\_] Offeror is an agency or instrumentality of the Federal Government;

(4) Type of organization.

[\_] Sole proprietorship;

[\_] Partnership;

[\_] Corporate entity (not tax-exempt);

[\_] Corporate entity (tax-exempt);

[\_] Government entity (Federal, State, or local);

[\_] Foreign government;

[\_] International organization per 26 CFR 1.6049-4;

[\_] Other \_\_\_\_\_.

(5) Common parent.

[\_] Offeror is not owned or controlled by a common parent:

[\_] Name and TIN of common parent:

Name \_\_\_\_\_

TIN \_\_\_\_\_

(m) Restricted business operations in Sudan. By submission of its offer, the offeror certifies that the offeror does not conduct any restricted business operations in Sudan.

(n) Prohibition on Contracting with Inverted Domestic Corporations-

(1) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(2) Representation. The offeror represents that-

(i) It [] is, [] is not an inverted domestic corporation; and

(ii) It [] is, [] is not a subsidiary of an inverted domestic corporation.

(o) Prohibition on contracting with entities engaging in certain activities or transactions relating to Iran.

(1) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(2) Representation and Certification. Unless a waiver is granted or an exception applies as provided in paragraph (o)(3) of this provision, by submission of its offer, the offeror—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Iran Sanctions Act; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds \$3,500 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50(U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at http://www.treasury.gov/ofac/downloads/t11sdn.pdf).

(3) The representation and certification requirements of paragraph (o)(2) of this provision do not apply if—

(i) This solicitation includes a trade agreements certification (e.g., 52.212-3(g) or a comparable agency provision); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products.

(p) Ownership or Control of Offeror. (Applies in all solicitations when there is a requirement to be registered in SAM or a requirement to have a unique entity identifier in the solicitation.

(1) The Offeror represents that it [] has or [] does not have an immediate owner. If the Offeror has more than one immediate owner (such as a joint venture), then the Offeror shall respond to paragraph (2) and if applicable, paragraph (3) of this provision for each participant in the joint venture.

(2) If the Offeror indicates "has" in paragraph (p)(1) of this provision, enter the following information:

Immediate owner CAGE code:\_\_\_\_

Immediate owner legal name:

(Do not use a "doing business as" name)

Is the immediate owner owned or controlled by another entity:

[] Yes or [] No.

(3) If the Offeror indicates "yes" in paragraph (p)(2) of this provision, indicating that the immediate owner is owned or controlled by another entity, then enter the following information:

Highest level owner CAGE code:\_\_

Highest level owner legal name:\_\_\_\_

(Do not use a "doing business as" name)

(q) Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law.

(1) As required by section 744 and 745 of Division E of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts, the Government will not enter into a contract with any corporation that—

(i) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless and agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(ii) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(2) The Offeror represents that--

(i) It is [] is not [] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(ii) It is [] is not [] a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(r) Predecessor of Offeror. (Applies in all solicitations that include the provision at 52.204-16, Commercial and Government Entity Code Reporting.)

(1) The Offeror represents that it [] is or [] is not a successor to a predecessor that held a Federal contract or grant within the last three years.

(2) If the Offeror has indicated "is" in paragraph (r)(1) of this provision, enter the following information for all predecessors that held a Federal contract or grant within the last three years (if more than one predecessor, list in reverse chronological order):

Predecessor CAGE code \_\_\_\_\_(or mark "Unknown).

legal name:

(Do not use a "doing business as" name).

Predecessor

(s) Representation regarding compliance with labor laws (Executive Order 13673). If the offeror is a joint venture that is not itself a separate legal entity, each concern participating in the joint venture shall separately comply with the requirements of this provision.

(1)(i) For solicitations issued on or after October 25, 2016 through April 24, 2017: The Offeror [] does [] does not anticipate submitting an offer with an estimated contract value of greater than \$50 million.

(ii) For solicitations issued after April 24, 2017: The Offeror [] does [] does not anticipate submitting an offer with an estimated contract value of greater than \$500,000.

(2) If the Offeror checked ``does" in paragraph (s)(1)(i) or (ii) of this provision, the Offeror represents to the best of the Offeror's knowledge and belief [Offeror to check appropriate block]:

[](i) There has been no administrative merits determination, arbitral award or decision, or civil judgment for any labor law violation(s) rendered against the offeror (see definitions in paragraph (a) of this section) during the period beginning on October 25, 2015 to the date of the offer, or for three years preceding the date of the offer, whichever period is shorter; or

[](ii) There has been an administrative merits determination, arbitral award or decision, or civil judgment for any labor law violation(s) rendered against the Offeror during the period beginning on October 25, 2015 to the date of the offer, or for three years preceding the date of the offer, whichever period is shorter.

(3)(i) If the box at paragraph (s)(2)(ii) of this provision is checked and the Contracting Officer has initiated a responsibility determination and has requested additional information, the Offeror shall provide--

(A) The following information for each disclosed labor law decision in the System for Award Management (SAM) at www.sam.gov, unless the information is already current, accurate, and complete in SAM. This information will be publicly available in the Federal Awardee Performance and Integrity Information System (FAPIIS):

(1) The labor law violated.

(2) The case number, inspection number, charge number, docket number, or other unique identification number.

(3) The date rendered.

(4) The name of the court, arbitrator(s), agency, board, or commission that rendered the determination or decision;

(B) The administrative merits determination, arbitral award or decision, or civil judgment document, to the Contracting Officer, if the Contracting Officer requires it;

(C) In SAM, such additional information as the Offeror deems necessary to demonstrate its responsibility, including mitigating factors and remedial measures such as offeror actions taken to address the violations, labor compliance agreements, and other steps taken to achieve compliance with labor laws. Offerors may provide explanatory text and upload documents. This information will not be made public unless the contractor determines that it wants the information to be made public; and

(D) The information in paragraphs (s)(3)(i)(A) and (s)(3)(i)(C) of this provision to the Contracting Officer, if the Offeror meets an exception to SAM registration (see FAR 4.1102(a)).

(ii)(A) The Contracting Officer will consider all information provided under (s)(3)(i) of this provision as part of making a responsibility determination.

(B) A representation that any labor law decision(s) were rendered against the Offeror will not necessarily result in withholding of an award under this solicitation. Failure of the Offeror to furnish a representation or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(C) The representation in paragraph (s)(2) of this provision is a material representation of fact upon which reliance was placed when making award. If it is later determined that the Offeror knowingly rendered an erroneous representation, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation in accordance with the procedures set forth in FAR 12.403.

(4) The Offeror shall provide immediate written notice to the Contracting Officer if at any time prior to contract award the Offeror learns that its representation at paragraph (s)(2) of this provision is no longer accurate.

(5) The representation in paragraph (s)(2) of this provision will be public information in the Federal Awardee Performance and Integrity Information System (FAPIIS).

Note to paragraph (s): By a court order issued on October 24, 2016, this paragraph (s) is enjoined indefinitely as of the date of the order. The enjoined paragraph will become effective immediately if the court terminates the injunction. At that time, DoD, GSA, and NASA will publish a document in the Federal Register advising the public of the termination of the injunction.

(t) Public Disclosure of Greenhouse Gas Emissions and Reduction Goals. Applies in all solicitations that require offerors to register in SAM (52.212-1(k)).

(1) This representation shall be completed if the Offeror received \$7.5 million or more in contract awards in the prior Federal fiscal year. The representation is optional if the Offeror received less than \$7.5 million in Federal contract awards in the prior Federal fiscal year.

(2) Representation. [Offeror to check applicable block(s) in paragraph (t)(2)(i) and (ii)].

(i) The Offeror (itself or through its immediate owner or highest-level owner) [] does, [] does not publicly disclose greenhouse gas emissions, i.e., makes available on a publicly accessible Web site the results of a

greenhouse gas inventory, performed in accordance with an accounting standard with publicly available and consistently applied criteria, such as the Greenhouse Gas Protocol Corporate Standard.

(ii) The Offeror (itself or through its immediate owner or highest-level owner) [] does, [] does not publicly disclose a quantitative greenhouse gas emissions reduction goal, i.e., make available on a publicly accessible Web site a target to reduce absolute emissions or emissions intensity by a specific quantity or percentage.

(iii) A publicly accessible Web site includes the Offeror's own Web site or a recognized, third-party greenhouse gas emissions reporting program.

(3) If the Offeror checked ``does'' in paragraphs (t)(2)(i) or (t)(2)(ii) of this provision, respectively, the Offeror shall provide the publicly accessible Web site(s) where greenhouse gas emissions and/or reduction goals are reported:\_\_\_\_\_.

(u)

(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions), Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with an entity that requires employees or subcontractors of such entity seeking to report waste, fraud, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(2) The prohibition in paragraph (u)(1) of this provision does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(3) Representation. By submission of its offer, the Offeror represents that it will not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

#### Addendum to 52.212-3(f):

#### **252.225-7000 -** BUY AMERICAN ACT—BALANCE OF PAYMENTS PROGRAM CERTIFICATE -BASIC (NOV 2014)

(a) *Definitions*. "Commercially available off-the-shelf (COTS) item," "component," "domestic end product," "foreign end product," "qualifying country," "qualifying country end product," and "United States," as used in this provision, have the meanings given in the Buy American and Balance of Payments Program-Basic clause of this solicitation.

(b) Evaluation. The Government—

(1) Will evaluate offers in accordance with the policies and procedures of Part 225 of the Defense Federal Acquisition Regulation Supplement; and (2) Will evaluate offers of qualifying country end products without regard to the restrictions of the Buy American statute or the Balance of Payments Program.

(c) Certifications and identification of country of origin.

(1) For all line items subject to the Buy American and Balance of Payments Program-Basic clause of this solicitation, the offeror certifies that—

(i) Each end product, except those listed in paragraphs (c)(2) or (3) of this provision, is a domestic end product; and

(ii) For end products other than COTS items, components of unknown origin are considered to have been mined, produced, or manufactured outside the United States or a qualifying country.

(2) The offeror certifies that the following end products are qualifying country end products:

Line Item Number	Country of Origin	

(3) The following end products are other foreign end products, including end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (ii) of the definition of "domestic end product":

Line Item Number	Country of Origin (If known)

#### (End of Provision)

*Alternate I.* As prescribed in <u>225.1101</u>(1)(ii), use the following provision, which adds "South Caucasus/Central and South Asian (SC/CASA) state" and "South Caucasus/Central and South Asian (SC/CASA) state end product" in paragraph (a), and replaces "qualifying country end products" in paragraphs (b)(2) and (c)(2) with "qualifying country end products or SC/CASA state end products":

BUY AMERICAN—BALANCE OF PAYMENTS PROGRAM CERTIFICATE—ALTERNATE I (NOV 2014)

(a) *Definitions*. "Commercially available off-the-shelf (COTS) item," "component," "domestic end product," "foreign end product," "qualifying country," "qualifying
country end product," "South Caucasus/Central and South Asian (SC/CASA) state," "South Caucasus/Central and South Asian (SC/CASA) state end product," and "United States," as used in this provision, have the meanings given in the Buy American and Balance of Payments Program—Alternate I clause of this solicitation.

(b) Evaluation. The Government—

(1) Will evaluate offers in accordance with the policies and procedures of part 225 of the Defense Federal Acquisition Regulation Supplement; and

(2) Will evaluate offers of qualifying country end products or SC/CASA state end products without regard to the restrictions of the Buy American statute or the Balance of Payments Program.

(c) Certifications and identification of country of origin.

(1) For all line items subject to the Buy American and Balance of Payments Program—Alternate I clause of this solicitation, the offeror certifies that—

(i) Each end product, except those listed in paragraphs (c)(2) or (3) of this provision, is a domestic end product; and

(ii) For end products other than COTS items, components of unknown origin are considered to have been mined, produced, or manufactured outside the United States or a qualifying country.

(2) The offeror certifies that the following end products are qualifying country end products or SC/CASA state end products:

Line Item Number	Country of Origin	

(3) The following end products are other foreign end products, including end products manufactured in the United States that do not qualify as domestic end products, i.e., an end product that is not a COTS item and does not meet the component test in paragraph (ii) of the definition of "domestic end product":

Line Item Number	Country of Origin (If known)

(End of Provision)

**52.212-4 Contract Terms and Conditions -- Commercial Items (May 2015)** is incorporated by reference. Its full text may be accessed electronically at <u>https://www.acquisition.gov/far/index.html</u>.

## Addendum to 52.212-4 – Contract Terms and Conditions – Commercial Items

The following paragraph(s) of 52.212-4 are amended as indicated below:

- Paragraph (a), <u>Inspection/Acceptance</u>, is revised to add the following: "Inspection and acceptance of products will be performed at destination. The authorized receiving official for each customer is responsible for signing for and accepting products when they are delivered. The final disposition decision rests with the food service officer and/or the authorized receiving official.
- 2. Paragraph (c), <u>Changes</u>, is deleted in its entirety and replaced with the following:
  - (c) Changes.
    - (1) In addition to bilateral modifications, the Contracting Officer, at his/her discretion, may unilaterally invoke any of the contingency options set forth in this contract.
    - (2) The Contracting Officer may at anytime, by unilateral written order, make changes within the general scope of this contract in any one or more of the following:
      - (i) Method of shipment or packing;
      - (ii) Place, manner, or time of delivery.
    - (3) If such change causes an increase or decrease in the cost of, or time required for, performance for any part of the work under this contract, the Contracting Officer shall make equitable adjustment in the contract price, the delivery schedule, or both, and shall modify the contract.
    - (4) The Contractor must assert its right to an adjustment under this clause within thirty (30) days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.
    - (5) Failure to agree to any adjustment shall be a dispute under the Disputes Clause. However, nothing in this clause shall excuse the Contractor from proceeding with the contract.
- 3. Paragraph (m), <u>Termination for Cause</u>.

Delete paragraph (m) in its entirety and substitute the following:

- (m)Termination for Cause. The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government upon request, with adequate assurances of future performance. In the event of termination for cause, the Government shall not be liable to the Contractor for any amount for supplies or services not accepted, and the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If this contract is terminated in whole or in part for cause, and the supplies or services covered by the contract so terminated are repurchased by the Government, the Government will incur administrative costs in such repurchases. The Contractor and the Government expressly agree that, in addition to any excess costs of repurchase, or any other damages resulting from such default, the Contractor shall pay, and the Government shall accept, the sum of \$1155.00 as payment in full for the administrative costs of such repurchase. This assessment of damages for administrative costs shall apply for any termination for cause following which the Government repurchases the terminated supplies or services together with any incidental or consequential damages incurred because of the termination. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.
- 4. Paragraph (o) <u>Warranty</u>, is revised to add the following:

- (o) The supplies furnished under the resultant contract shall be covered by the most favorable commercial warranties the contractor gives to any customer for such supplies and the rights and remedies provided therein are in addition to and do not limit any rights afforded to the Government in accordance with FAR Clause 52.212-4(o) "Warranty."
- 5. Paragraph (r) <u>Compliance with laws unique to Government contracts</u>, is revised to include the following:
  - (r) The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. 3701, et seq., Contract Work Hours and Safety Standards Act; 41 U.S.C. 51-58, Anti-Kickback Act of 1986; 41 U.S.C. 265 and 10 U.S.C. 2409 relating to whistleblower protections; Section 1553 of the American Recovery and Reinvestment Act of 2009 relating to whistleblower protections for contracts funded under that Act; 49 U.S.C. 40118, Fly American; and 41 U.S.C. 423 relating to procurement integrity.
- 6. Paragraph (t), <u>System for Award Management.</u> Add the following paragraph:
  - (a) Definitions.

"System for Award Management (SAM) Database" means the primary Government repository for contractor information required for the conduct of business with the Government.

"Commercial and Government Entity (CAGE) Code" means-

(1) A code assigned by the Defense Logistics Information Service (DLIS) to identify a commercial or Government entity; or

(2) A code assigned by a member of the North Atlantic Treaty Organization that DLIS records and maintains in the CAGE master file. This type of code is known as an "NCAGE code".

"<u>Data Universal Number System (DUNS) Number</u>" means the 9-digit number assigned by Dun and Bradstreet, Inc. (D&B) to identify unique business entities.

"<u>Data Universal Numbering System +4 (DUNS+4) Number</u>" means the DUNS number assigned by D&B plus a 4-character suffix that may be assigned by a business concern. (D&B has no affiliation with this 4-character suffix.) This 4-character suffix may be assigned at the discretion of the business concern to establish additional SAM records for identifying alternative Electronic Funds Transfer (EFT) accounts (see Subpart 32.11 of the Federal Acquisition Regulation) for the same parent concern.

"Registered in the System for Award Management database" means that-

(1) The Contractor has entered all mandatory information, including the DUNS number or the DUNS+4 number, and Contractor and Government Entity (CAGE) code into the SAM database; (2) The contractor has completed the Core Data, Assertions, Representations and Certifications, and Points of Contact sections of the registration in the SAM database;

(3) The Government has validated all mandatory data fields to include validation of the Taxpayer Identification Number (TIN) with the Internal Revenue Service. The Contractor will be required to provide consent for TIN validation to the Government as part of the SAM registration process; and

(4) The Government has marked the record "Active".

#### 52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders --Commercial Items.

As prescribed in 12.301(b)(4), insert the following clause:

## Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Jan 2017)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(2) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(3) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

 $\underline{X}$  (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

X (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

(4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Oct 2015) (Pub. L. 109-282) (31 U.S.C. 6101 note).

\_\_\_\_(5) [Reserved]

(6) 52.204-14, Service Contract Reporting Requirements (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).

\_\_\_\_ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Jan 2014) (Pub. L. 111-117, section 743 of Div. C).

(8) 52.209-6, Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

(9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

\_\_\_\_(10) [Reserved]

\_\_\_\_ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

(ii) Alternate I (Nov 2011) of 52.219-3.

\_X\_\_ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

(ii) Alternate I (Jan 2011) of 52.219-4.

\_\_\_\_(13) [Reserved]

(14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

- (ii) Alternate I (Nov 2011).
- (iii) Alternate II (Nov 2011).
- (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).
- (ii) Alternate I (Oct 1995) of 52.219-7.
- (iii) Alternate II (Mar 2004) of 52.219-7.
- (16) 52.219-8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)).
- \_\_\_\_ (17) (i) 52.219-9, Small Business Subcontracting Plan (Jan 17) (15 U.S.C. 637 (d)(4)).
- (ii) Alternate I (Oct 2001) of 52.219-9.
- (iii) Alternate II (Oct 2001) of 52.219-9.
- (iv) Alternate III (Oct 2015) of 52.219-9.
- (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

(19) 52.219-14, Limitations on Subcontracting (Nov 2011) (15 U.S.C. 637(a)(14)).

\_\_\_\_ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).

(22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).

(23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).

(24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).

\_X\_ (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

\_X\_ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2016) (E.O. 13126).

\_X\_(27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

\_X\_ (28) 52.222-26, Equal Opportunity (Apr 2015) (E.O. 11246).

\_X\_(29) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

\_X\_(30) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

\_X\_ (31) 52.222-37, Employment Reports on Veterans (Oct 2015) (38 U.S.C. 4212).

(32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

\_\_\_\_ (33) (i) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).

(34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

\_\_\_\_ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

\_\_\_\_ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

\_\_\_\_ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (JUN 2016) (E.O. 13693).

\_\_\_\_ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (JUN 2016) (E.O. 13693).

\_\_\_\_ (38) (i) 52.223-13, Acquisition of EPEAT  $\ensuremath{\mathbb{B}}$  -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514

(ii) Alternate I (Oct 2015) of 52.223-13.

(39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

\_\_\_\_ (ii) Alternate I (Jun 2014) of 52.223-14.

(40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

\_\_\_\_ (41) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

(ii) Alternate I (Jun 2014) of 52.223-16.

\_\_X\_ (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).

(43) 52.223-20, Aerosols (JUN 2016) (E.O. 13693)

\_\_\_\_ (44) 52.223-21, Foams (JUN 2016) (E.O. 13693)

(45) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).

(46) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

(ii) Alternate I (May 2014) of 52.225-3.

\_\_\_\_ (iii) Alternate II (May 2014) of 52.225-3.

(iv) Alternate III (May 2014) of 52.225-3.

\_\_\_\_\_(47) 52.225-5, Trade Agreements (Nov 2013) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

(48) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

(49) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

\_\_\_\_ (50) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

\_\_\_\_ (51) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

\_\_\_\_ (52) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).

\_\_\_\_ (53) 52.232-30, Installment Payments for Commercial Items (Oct 1995) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

\_X\_ (54) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Jul 2013) (31 U.S.C. 3332).

\_\_\_\_ (55) 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

(56) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

(57) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

\_\_\_\_ (58) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

(ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

(1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)

(2) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67.).

\_\_\_\_ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (May 2014) (29 U.S.C.206 and 41 U.S.C. chapter 67).

\_\_\_\_ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

\_\_\_\_ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

(8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).

(9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

(10) 52.237-11, Accepting and Dispensing of \$1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

#### (e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(iv) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(v) 52.222-26, Equal Opportunity (Apr 2015) (E.O. 11246).

(vi) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(vii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(viii) 52.222-37, Employment Reports on Veterans (Oct 2015) (38 U.S.C. 4212).

(ix) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(x) 52.222-41, Service Contract Labor Standards (May 2014), (41 U.S.C. chapter 67).

(xi) \_\_\_\_ (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xiii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xiv) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xv) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).

(xvi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xvii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xviii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

*Alternate I (Feb 2000).* As prescribed in  $\underline{12.301}(b)(4)(i)$ , delete paragraph (d) from the basic clause, redesignate paragraph (e) as paragraph (d), and revise the reference to "paragraphs (a), (b), (c), or (d) of this clause" in the redesignated paragraph (d) to read "paragraphs (a), (b), and (c) of this clause".

Alternate II (Dec 2015). As prescribed in  $\underline{12.301}(b)(4)(ii)$ , substitute the following paragraphs (d)(1) and (e)(1) for paragraphs (d)(1) and (e)(1) of the basic clause as follows:

# (d)

(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to—

(i) Examine any of the Contractor's or any subcontractors' records that pertain to, and involve transactions relating to, this contract; and

(ii) Interview any officer or employee regarding such transactions.

## (e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), and (c), of this clause, the Contractor is not required to flow down any FAR clause in a subcontract for commercial items, other than—

(i) *Paragraph* (*d*) of this clause. This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (d)(1)(ii) does not flow down; and

(ii) *Those clauses listed in this paragraph* (e)(1). Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(A) 52.203–13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(B) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5).

(C) 52.219–8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(D) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(E) 52.222–26, Equal Opportunity (Apr 2015) (E.O. 11246).

(F) 52.222–35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(G) 52.222–36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(H) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(I) 52.222–41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

(J) \_\_\_\_ (1) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(2) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(K) 52.222–51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(L) 52.222–53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

(M) 52.222–54, Employment Eligibility Verification (Oct 2015) (Executive Order 12989).

(N) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E. O. 13658).

(O) 52.226–6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226–6.

(P) 52.247–64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247–64.

[Class Deviation- 2013-O0019, Commercial Item Omnibus Clauses for Acquisitions Using the Standard Procurement System. This clause deviation is effective on Sep 25, 2013, and remains in effect for five years, or until otherwise rescinded.

#### FAR 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (DEVIATION 2013-00019) (Jun 2016)

(a) *Comptroller General Examination of Record*. The Contractor shall comply with the provisions of this paragraph (a) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the

other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(b)

(1) Notwithstanding the requirements of any other clause in this contract, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (b)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).

(ii) 52.219-8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$650,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) 52.222-17, Non-displacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(iv) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(v) 52.222-26, Equal Opportunity (Apr 2015) (E.O. 11246).

(vi) 52.222-35, Equal Opportunity for Veterans (Jul 2014) (38 U.S.C. 4212).

(vii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(viii) 52.222-37, Employment Reports on Veterans (Jul 2014) (38 U.S.C. 4212).

(ix) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(x) 52.222-41, Service Contract Labor Standards (May 2014), (41 U.S.C. chapter 67).

(xi) (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xiii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xiv) 52.222-54, Employment Eligibility Verification (Aug 2013).

(xv) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2014) (E.O. 13658).

(xvi) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Jul 2013) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xvii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xviii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

#### (End of Clause)

*Alternate I* (2013-00019) (*Jul 2014*). As prescribed in 12.301(b)(4), delete paragraph (a) from the basic clause, redesignate paragraph (b)(1) as paragraph (a), and redesignate paragraphs (b)(1)(i) through (b)(1)(xiv) as paragraphs (a)(1) through (a)(14) and redesignate paragraph (b)(2) as paragraph (b).

*Alternate II (2013-00019) (Apr2015).* As prescribed in 12.301(b)(4)(ii), substitute the following paragraphs (a)(1) and (b)(1) for paragraphs (a)(1) and (b)(1) of the basic clause as follows:

(a)

(1) The Comptroller General of the United States, an appropriate Inspector General appointed under section 3 or 8G of the Inspector General Act of 1978 (5 U.S.C. App.), or an authorized representative of either of the foregoing officials shall have access to and right to—

(i) Examine any of the Contractor's or any subcontractors' records that pertain to, and involve transactions relating to, this contract; and

(ii) Interview any officer or employee regarding such transactions.

#### (b)

(1) Notwithstanding the requirement of any other clause in this contract, the Contractor is not required to flow down any FAR clause in a subcontract for commercial items, other than—

(i) *Paragraph* (*a*) of this clause. This paragraph flows down to all subcontracts, except the authority of the Inspector General under paragraph (a)(1)(ii) does not flow down; and

(ii) *Those clauses listed in this paragraph* (b)(1). Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(A) 52.203–13, Contractor Code of Business Ethics and Conduct (Apr 2010) (41 U.S.C. 3509).

(B) 52.203-15, Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5).

(C) 52.219–8, Utilization of Small Business Concerns (Oct 2014) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$650,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(D) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(E) 52.222–26, Equal Opportunity (Mar 2007) (E.O. 11246).

(F) 52.222–35, Equal Opportunity for Veterans (Jul 2010) (38 U.S.C. 4212).

(G) 52.222–36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(H) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(I) 52.222–41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67).

(J) \_\_\_\_ (1) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(2) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(K) 52.222–51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(L) 52.222–53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

(M) 52.222–54, Employment Eligibility Verification (Aug 2013).

(N) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2014) (E. O. 13658).

(O) 52.226–6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226–6.

(P) 52.247–64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx. 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247–64.

# 52.233-9001 DISPUTES: AGREEMENT TO USE ALTERNATIVE DISPUTE RESOLUTION (NOV 2011) – DLAD

(a) The parties agree to negotiate with each other to try to resolve any disputes that may arise. If unassisted negotiations are unsuccessful, the parties will use alternative dispute resolution (ADR) techniques to try to resolve the dispute. Litigation will only be considered as a last resort when ADR is unsuccessful or has been documented by the party rejecting ADR to be inappropriate for resolving the dispute.

(b) Before either party determines ADR inappropriate, that party must discuss the use of ADR with the other party. The documentation rejecting ADR must be signed by an official authorized to bind the Contractor (see Federal Acquisition Regulation (FAR) clause 52.233-1), or, for the Agency, by the Contracting Officer, and approved at a level above the Contracting Officer after consultation with the ADR Specialist and with legal. Contractor personnel are also encouraged to include the ADR Specialist in their discussions with the Contracting Officer before determining ADR to be inappropriate.

(c) The offeror should check here to opt out of this clause:

[] Alternate wording may be negotiated with the Contracting Officer.

#### FAR 52.252-2 Clauses Incorporated By Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): http://farsite.hill.af.mil/ *OR* www.acquisition.gov

The following additional clauses are incorporated by <u>REFERENCE</u>:

CLAUSE Number	Title
52.204-7	Systems for Award Management
52.247-34	F.O.B. Destination

#### FAR 52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): <a href="http://www.dla.mil/j-3/j-336/icps.htm">http://www.dla.mil/j-3/j-336/icps.htm</a>

OR http://www.dla.mil/j-3/j-336/logisticspolicy/procurementlinks2.htm.

<b>Provision Number</b>	Title
	Protecting the Government's Interests When Subcontracting with
FAR 52.209-6	Contractors Debarred, Suspended or Proposed for Debarment
FAR 52.212-2	Evaluation of Commercial Items
FAR 52.225-25	Prohibition on Engaging in Sanctioned Activities Relating to
	Iran—Certification
FAR 52.232-17	Interest

#### The following additional provisions are incorporated by <u>REFERENCE:</u>

FAR 52.242-13	Bankruptcy
FAR 52.242-15	Stop-Work Order
DFARS 252.204-7003	Control of Government Personnel Work Product
DFARS 252.204-7004	Alternate A, System for Award Management
	Subcontracting with Firms that are Owned or Controlled by the
DFARS 252.209-7004	Government of a Terrorist Country
DFARS 252.225-7002	Qualifying Countries as Subcontractors
DLAD 52.233-9000	Agency Protests

#### 52.215-6 - Place of Performance (Oct 1997)

(a) The offeror or respondent, in the performance of any contract resulting from this solicitation, intends, does not intend [*check applicable block*] to use one or more plants or facilities located at a different address from the address of the offeror or respondent as indicated in this proposal or response to request for information.

(b) If the offeror or respondent checks "intends" in paragraph (a) of this provision, it shall insert in the following spaces the required information:

Place of Performance(Street Address, City, State, County, Zip Code)	Name and Address of Owner and Operator of the Plant or Facility if Other Than Offeror or Respondent