

AWARD/CONTRACT J	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE 1	OF 16 PAGES
	2. CONTRACT (Proc. Inst. Ident.) NO. SPE3S1-17-D-Z117	3. EFFECTIVE DATE 2016 DEC 02	4. REQUISITION/PURCHASE REQUEST/PROJECT NO. 1000047680	

5. ISSUED BY DLA TROOP SUPPORT SUBSISTENCE SUPPLY CHAIN 700 ROBBINS AVENUE PHILADELPHIA PA 19111-5096 USA Local Admin: Stephen Granato PSPTRCA Tel: 215-737-3839 Fax: 215-737-3184 Email: STEPHEN.GRANATO@DLA.MIL	CODE SPE3S1	6. ADMINISTERED BY (If other than Item 5) DCMA CHICAGO 1523 WEST CENTRAL ROAD ARLINGTON HEIGHTS IL 60005-2451 USA Criticality: PAS: None	CODE S1403A
--	----------------	---	----------------

7. NAME AND ADDRESS OF CONTRACTOR (No., street, city, county, State and ZIP Code) JIANAS BROTHERS PACKAGING COMPANY 2533 SOUTHWEST BLVD KANSAS CITY MO 64108-2345 USA	8. DELIVERY <input type="checkbox"/> FOB ORIGIN <input checked="" type="checkbox"/> OTHER (See below)
	9. DISCOUNT FOR PROMPT PAYMENT Net 30 (Do not Use)
	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN ITEM

CODE 64806	FACILITY CODE	11. SHIP TO/MARK FOR SEE SCHEDULE, DO NOT SHIP TO ADDRESS ON THIS PAGE	12. PAYMENT WILL BE MADE BY DEF FIN AND ACCOUNTING SVC BSM P O BOX 182317 COLUMBUS OH 43218-2317 USA	CODE SL4701
------------	---------------	---	---	----------------

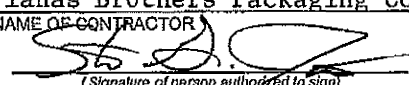
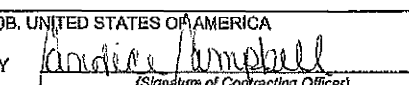
13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION: <input type="checkbox"/> 10 U.S.C. 2304(c) <input type="checkbox"/> 41 U.S.C. 253(c)	14. ACCOUNTING AND APPROPRIATION DATA
---	---------------------------------------

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	See Schedule	13335000.000			
15G. TOTAL AMOUNT OF CONTRACT					\$44,000,000.00

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES			
X	A	SOLICITATION/CONTRACT FORM	1		I	CONTRACT CLAUSES	
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	2	PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.			
	C	DESCRIPTION/SPECS./WORK STATEMENT			J	LIST OF ATTACHMENTS	
	D	PACKAGING AND MARKING		PART IV - REPRESENTATIONS AND INSTRUCTIONS			
	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	F	DELIVERIES OR PERFORMANCE			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	G	CONTRACT ADMINISTRATION DATA			M	EVALUATION FACTORS FOR AWARD	
	H	SPECIAL CONTRACT REQUIREMENTS					

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. <input checked="" type="checkbox"/> CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)	18. <input type="checkbox"/> SEALED-BID AWARD (Contractor is not required to sign this document.) Your bid on Solicitation Number _____ including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)
---	---

19A. NAME AND TITLE OF SIGNER (Type or Print) Steve G. Jianas, Vice President Jianas Brothers Packaging Company	20A. NAME OF CONTRACTING OFFICER Lardice Campbell
19B. NAME OF CONTRACTOR BY  (Signature of person authorized to sign)	19C. DATE SIGNED 12/2/2016
20B. UNITED STATES OF AMERICA BY  (Signature of Contracting Officer)	20C. DATE SIGNED 2016 DEC 02

The following documents are hereby incorporated by reference into this contract: Solicitation SPES1-16-R-0011, all solicitation amendments 0001, 0002, and 0003, and your final offer, including final proposal revisions, which is being accepted by the Government to form this contract.

Effective period of performance.

Tier 1: December 2, 2016 - December 1, 2017
Tier 2: December 2, 2017 - December 1, 2018
Tier 3: December 2, 2018 - December 1, 2019
Tier 4: December 2, 2019 - December 1, 2020
Tier 5: December 2, 2020 - December 1, 2021

Guaranteed Minimum Quantity: 13,335,000

Guaranteed Maximum Quantity (Including Surge): 81,015,768

Schedule of Items:

8960-00-170-8446	COCOA BEVERAGE POWDER, CHOCOLATE
8960-01-527-8228	COCOA BEVERAGE POWDER, CHOCOLATE HAZELNUT
8955-01-538-0702	CAPPUCCINO, FRENCH VANILLA
8955-01-538-0705	CAPPUCCINO, MOCHA
8955-01-556-0077	CAPPUCCINO, IRISH CREAM
8960-01-523-6344	BEVERAGE POWDER, ASCORBIC ACID/MALTDX, ORANGE
8960-01-523-6346	BEVERAGE POWDER, ASCORBIC ACID/MALTDX, LEMON-LIME

PDM:

COCOA BEVERAGE POWDER, CHOCOLATE - Lot# 6169
COCOA BEVERAGE POWDER, CHOCOLATE HAZELNUT - Lot# 6124
CAPPUCCINO, FRENCH VANILLA - Lot# 6187
CAPPUCCINO, MOCHA - Lot# 6186
CAPPUCCINO, IRISH CREAM - Lot# 6188
BEVERAGE POWDER, ASCORBIC ACID/MALTDX, ORANGE - Lot# 6160
BEVERAGE POWDER, ASCORBIC ACID/MALTDX, LEMON-LIME - Lot# 6166

Delivery terms: F.O.B. Destination.

The Wornick Company
4700 Creek Road
Cincinnati, OH 45242

SOPAKCO Packaging
118 South Cypress Street
Mullins, SC 29574

AmeriQual Group LLC
18200 Highway 41 North
Evansville, Indiana 47725

Pricing terms: Firm-Fixed-Price.

Inspection and acceptance point(s): Origin.

DLA Troop Support will establish Rations National Contracts (RNC) with component manufacturers, and will authorize the MRE assemblers to order directly from the national contracts in lieu of DLA providing the components as GFM. The Rations National Contracts will establish the component prices, but the assemblers, Wornick, SOPAKCO, and AmeriQual, will order and pay for the material directly. The assemblers will have full control over when to order, how much to order, and have full responsibility for the supply chain and

CONTINUED ON NEXT PAGE

inventory. See FAR 52.216-19 - Order limitations for more information.
Note: Terms and conditions of the individual component contract shall prevail in case of a conflict between the MRE assembly contract(s) and this individual component contract.

THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED BY REFERENCE:

252.211-7006 Passive Radio Frequency Identification (JUN 2016) DFARS
52.222-26 -- Equal Opportunity. (Sept 2016)
52.222-37 Employment Reports on Veterans (FEB 2016)
252.225-7002 Qualifying Country Sources as Subcontractors. (Aug 2016) DFARS
52.244-6 Subcontracts for Commercial Items (SEPT 2016)
FAR 52.223-11 Ozone-Depleting Substances (MAY 2001) **FULL TEXT
New: 52.223-11 -- Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons. JUN 2016
52.204-7 System for Award Management (Oct 2016)
52.204-13 - System for Award Management Maintenance (Oct 2016)
52.204-16 --Commercial and Government Entity Code Reporting (Jul 2016)
52.204-18 Commercial and Government Entity Code Maintenance (Jul 2016)
252.204-7015 NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION FOR LITIGATION SUPPORT (MAY 2016)
52.204-9000 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS (JUL 2015)
52.212-1 -- Instructions to Offerors -- Commercial Items (Oct 2016)
252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)
52.225-25 -- Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran-Representation and Certification (Oct 2015)
252.225-7012 PREFERENCE FOR CERTAIN DOMESTIC COMMODITIES (AUG 2016)
252.211-7006 RADIO FREQUENCY IDENTIFICATION (JUN 2016)

THE FOLLOWING CLAUSES ARE HEREBY INCORPORATED BY FULL TEXT:

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls.

As prescribed in 204.7304(a), use the following provision:

COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016)

(a) Definitions. As used in this provision-

"Controlled technical information," "covered contractor information system," "covered defense information," "cyber incident," "information system," and "technical information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology service or system operated on behalf of the Government (see 252.204-7012(b)(2)-

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see <http://dx.doi.org/10.6028/NIST.SP.800-171>) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

(2) (i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting

Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of-

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

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

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP

800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

252.204-7009 Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

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

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

(a) Definitions. As used in this clause-

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

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

"Covered defense information" means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is-

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

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

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

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

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

(b) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a 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

CONTINUED ON NEXT PAGE

other appropriate remedies by the United States; and

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

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

(End of clause)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

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

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

(a) Definitions. As used in this clause-

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

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

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

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

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

"Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at <http://www.archives.gov/cui/registry/category-list.html>, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is-

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

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

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

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

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

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

"Operationally critical support" means supplies or services designated by the Government as critical for

CONTINUED ON NEXT PAGE

airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

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

"Technical information" means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-

Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

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

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

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

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

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b) (1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b) (2) (ii) of this clause, the covered contractor information system shall be subject to the security requirements in National

Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at <http://dx.doi.org/10.6028/NIST.SP.800-171>) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii) (A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief

Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline

(<https://www.fedramp.gov/resources/documents/>) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

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

(c) Cyber incident reporting requirement.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(m) Subcontracts. The Contractor shall--

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract

performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to--

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

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

(End of clause)

252.211-7006 Passive Radio Frequency Identification.

As prescribed in 211.275-3, use the following clause:

PASSIVE RADIO FREQUENCY IDENTIFICATION (JUN 2016)

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

"Advance shipment notice" means an electronic notification used to list the contents of a shipment of goods as well as additional information relating to the shipment, such as passive radio frequency identification (RFID) or item unique identification (IUID) information, order information, product description, physical characteristics, type of packaging, marking, carrier information, and configuration of goods within the transportation equipment.

"Bulk commodities" means the following commodities, when shipped in rail tank cars, tanker trucks, trailers, other bulk wheeled conveyances, or pipelines:

(1) Sand.

(2) Gravel.

(3) Bulk liquids (water, chemicals, or petroleum products).

(4) Ready-mix concrete or similar construction materials.

(5) Coal or combustibles such as firewood.

(6) Agricultural products such as seeds, grains, or animal feed.

"Case" means either a MIL-STD-129 defined exterior container within a palletized unit load or a MIL-STD-129 defined individual shipping container.

"Electronic Product Code" (EPC) means an identification scheme for universally identifying physical objects via RFID tags and other means. The standardized EPC data consists of an EPC (or EPC identifier) that uniquely identifies an individual object, as well as an optional filter value when judged to be necessary to enable effective and efficient reading of the EPC tags. In addition to this standardized data, certain classes of EPC tags will allow user-defined data. The EPC Tag Data Standards will define the length and position of this data, without defining its content.

"EPCglobal@" means a subscriber-driven organization comprised of industry leaders and organizations focused

on creating global standards for the adoption of passive RFID technology.

"Exterior container" means a MIL-STD-129 defined container, bundle, or assembly that is sufficient by reason of material, design, and construction to protect unit packs and intermediate containers and their contents during shipment and storage. It can be a unit pack or a container with a combination of unit packs or intermediate containers. An exterior container may or may not be used as a shipping container.

"Palletized unit load" means a MIL-STD-129 defined quantity of items, packed or unpacked, arranged on a pallet in a specified manner and secured, strapped, or fastened on the pallet so that the whole palletized load is handled as a single unit. A palletized or skidded load is not considered to be a shipping container. A loaded 463L System pallet is not considered to be a palletized unit load. Refer to the Defense Transportation Regulation, DoD 4500.9-R, Part II, Chapter 203, for marking of 463L System pallets.

"Passive RFID tag" means a tag that reflects energy from the reader/interrogator or that receives and temporarily stores a small amount of energy from the reader/interrogator signal in order to generate the tag response. The only acceptable tags are EPC Class 1 passive RFID tags that meet the EPCglobal™ Class 1 Generation 2 standard.

"Radio frequency identification (RFID)" means an automatic identification and data capture technology comprising one or more reader/interrogators and one or more radio frequency transponders in which data transfer is achieved by means of suitably modulated inductive or radiating electromagnetic carriers.

"Shipping container" means a MIL-STD-129 defined exterior container that meets carrier regulations and is of sufficient strength, by reason of material, design, and construction, to be shipped safely without further packing (e.g., wooden boxes or crates, fiber and metal drums, and corrugated and solid fiberboard boxes).

(b) (1) Except as provided in paragraph (b) (2) of this clause, the Contractor shall affix passive RFID tags, at the case- and palletized-unit-load packaging levels, for shipments of items that-

(i) Are in any of the following classes of supply, as defined in DoD 4140.1-R, DoD Supply Chain Materiel Management Regulation, APL 1.11:

(A) Subclass of Class I - Packaged operational rations.

(B) Class II - Clothing, individual equipment, tentage, organizational tool kits, hand tools, and administrative and housekeeping supplies and equipment.

(C) Class IIIP - Packaged petroleum, lubricants, oils, preservatives, chemicals, and additives.

(D) Class IV - Construction and barrier materials.

(E) Class VI - Personal demand items (non-military sales items).

(F) Subclass of Class VIII - Medical materials (excluding pharmaceuticals, biologicals, and reagents - suppliers should limit the mixing of excluded and non-excluded materials).

(G) Class IX - Repair parts and components including kits, assemblies and subassemblies, repairable and consumable items required for maintenance support of all equipment, excluding medical-peculiar repair parts; and

(ii) Are being shipped to one of the locations listed at http://www.acq.osd.mil/log/sci/RFID_ship-to-locations.html or to-

(A) A location outside the contiguous United States when the shipment has been assigned Transportation Priority 1, or to-

(B) The following location(s) deemed necessary by the requiring activity:

Contract Line, Subline, or Exhibit Line Item Number Location Name City State DoDAAC

(2) The following are excluded from the requirements of paragraph (b) (1) of this clause:

(i) Shipments of bulk commodities.

(ii) Shipments to locations other than Defense Distribution Depots when the contract includes the clause at FAR 52.213-1, Fast Payment Procedures.

(c) The Contractor shall-

(1) Ensure that the data encoded on each passive RFID tag are globally unique (i.e., the tag ID is never repeated across two or more RFID tags and conforms to the requirements in paragraph (d) of this clause;

(2) Use passive tags that are readable; and

(3) Ensure that the passive tag is affixed at the appropriate location on the specific level of packaging, in accordance with MIL-STD-129 (Section 4.9.2) tag placement specifications.

(d) Data syntax and standards. The Contractor shall encode an approved RFID tag using the instructions

provided in the EPC™ Tag Data Standards in effect at the time of contract award. The EPC™ Tag Data Standards are available at <http://www.epcglobalinc.org/standards/>.

(1) If the Contractor is an EPCglobal™ subscriber and possesses a unique EPC™ company prefix, the Contractor may use any of the identifiers and encoding instructions described in the most recent EPC™ Tag Data Standards document to encode tags.

(2) If the Contractor chooses to employ the DoD identifier, the Contractor shall use its previously assigned Commercial and Government Entity (CAGE) code and shall encode the tags in accordance with the tag identifier details located in the DoD Suppliers' Passive RFID Information Guide at <http://www.acq.osd.mil/log/sci/ait.html>. If the Contractor uses a third-party packaging house to encode its tags, the CAGE code of the third-party packaging house is acceptable.

(3) Regardless of the selected encoding scheme, the Contractor with which the Department holds the contract is responsible for ensuring that the tag ID encoded on each passive RFID tag is globally unique, per the requirements in paragraph (c) (1).

(e) Advance shipment notice. The Contractor shall use Wide Area WorkFlow (WAWF), as required by DFARS 252.232-7003, Electronic Submission of Payment Requests, to electronically submit advance shipment notice(s) with the RFID tag ID(s) (specified in paragraph (d) of this clause) in advance of the shipment in accordance with the procedures at <https://wawf.eb.mil/>.

252.225-7001 Buy American and Balance of Payments Program.

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

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

(a) Definitions. As used in this clause#

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

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

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

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

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

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

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

"Domestic end product" means-

(i) An unmanufactured end product that has been mined or produced in the United States; or

(ii) An end product manufactured in the United States if-

(A) The cost of its qualifying country components and its components that are mined, produced, or manufactured in the United States exceeds 50 percent of the cost of all its components. The cost of components includes transportation costs to the place of incorporation into the end product and U.S. duty (whether or not a duty-free entry certificate is issued). Scrap generated, collected, and prepared for processing in the United States is considered domestic. A component is considered to have been mined, produced, or manufactured in the United States (regardless of its source in fact) if the end product in which it is incorporated is manufactured in the United States and the component is of a class or kind for which the Government has determined that-

(1) Sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States; or

(2) It is inconsistent with the public interest to apply the restrictions of the Buy American statute; or

(B) The end product is a COTS item.

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

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

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

Austria
Belgium
Canada
Czech Republic
Denmark
Egypt
Finland
France
Germany
Greece
Israel
Italy
Japan
Luxembourg
Netherlands
Norway
Poland
Portugal
Slovenia
Spain
Sweden
Switzerland
Turkey

United Kingdom of Great Britain and Northern Ireland.

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

"Qualifying country end product" means—

- (i) An unmanufactured end product mined or produced in a qualifying country; or
- (ii) An end product manufactured in a qualifying country if —
 - (A) The cost of the following types of components exceeds 50 percent of the cost of all its components:
 - (1) Components mined, produced, or manufactured in a qualifying country.
 - (2) Components mined, produced, or manufactured in the United States.
 - (3) Components of foreign origin of a class or kind for which the Government has determined that sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States; or
 - (B) The end product is a COTS item.

"United States" means the 50 States, the District of Columbia, and outlying areas.

(b) This clause implements 41 U.S.C chapter 83, Buy American. In accordance with 41 U.S.C. 1907, the component test of the Buy American statute is waived for an end product that is a COTS item (see section 12.505(a)(1) of the Federal Acquisition Regulation). Unless otherwise specified, this clause applies to all line items in the contract.

(c) The Contractor shall deliver only domestic end products unless, in its offer, it specified delivery of other end products in the Buy American Balance of Payments Program Certificate provision of the solicitation. If the Contractor certified in its offer that it will deliver a qualifying country end product, the Contractor shall deliver a qualifying country end product or, at the Contractor's option, a domestic end product.

(d) The contract price does not include duty for end products or components for which the Contractor will claim duty-free entry.

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

(a) *Definitions.* As used in this provision—

"Controlled technical information," "covered contractor information system," and "covered defense information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.

(b) The security requirements required by contract clause 252.204-7012, Covered Defense Information and Cyber Incident Reporting, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.

(c) For covered contractor information systems that are not part of an information technology (IT) service or system operated on behalf of the Government (see 252.204-7012(b)(1)(ii))—

(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see <http://dx.doi.org/10.6028/NIST.SP.800-171>), not later than December 31, 2017.

(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—

- (A) Why a particular security requirement is not applicable; or
- (B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.

(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

(End of provision)

252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (DEC 2015) 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).

CONTINUED ON NEXT PAGE

"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)

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

(a) *Definitions.* As used in this clause—

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

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

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

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

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

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

"Covered defense information" means unclassified information that—

(i) Is—

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

(ii) Falls in any of the following categories:

(A) *Controlled technical information.*

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

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

CONTINUED ON NEXT PAGE

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.

(b) *Adequate security.* The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall—

(1) Implement information systems security protections on all covered contractor information systems including, at a minimum—

(i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government—

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

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

(ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause—

(A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," <http://dx.doi.org/10.6028/NIST.SP.800-171> that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD CIO, via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

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

(2) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

(c) *Cyber incident reporting requirement.*

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

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data,

CONTINUED ON NEXT PAGE

and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

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

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

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

(d) *Malicious software.* The Contractor or subcontractors that discover and isolate malicious software in connection with a reported cyber incident shall submit the malicious software in accordance with instructions provided by the Contracting Officer.

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

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

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

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

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

- (1) To entities with missions that may be affected by such information;
- (2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
- (3) To Government entities that conduct counterintelligence or law enforcement investigations;
- (4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
- (5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

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

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

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

(m) *Subcontracts.* The Contractor shall—

- (1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve a covered contractor information system, including subcontracts for commercial items, without alteration, except to identify the parties; and
- (2) When this clause is included in a subcontract, require subcontractors to rapidly report cyber incidents directly to DoD at <http://dibnet.dod.mil> and the prime Contractor. This includes providing the incident report

number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.

(End of clause)

SECTION J - LIST OF ATTACHMENTS**List of Attachments**

Description	File Name
ATTACH.Awarded Pricing Attachment	Jianas' awarded pricing sheet - MRE37 Beverages.pdf

JIANAS BROTHERS PACKAGING COMPANY

FINAL PRICING SPREADSHEET - JIANAS AWARD

LINE ITEM	NSN	ITEM NAME	Tier 1	Tier 2	Tier 3	Tier 4	Tier 5
0001	8960-00-170-8446	COCOA BEVERAGE POWDER,CHOCOLATE	\$ 0.2388	\$ 0.2413	\$ 0.2437	\$ 0.2463	\$ 0.2480
0002	8960-01-527-8228	COCOA BEVERAGE POWDER,CHOCOLATE HAZELNUT	\$ 0.2388	\$ 0.2413	\$ 0.2437	\$ 0.2463	\$ 0.2480
0003	8955-01-538-0702	CAPPUCCINO, FRENCH VANILLA	\$ 0.2231	\$ 0.2254	\$ 0.2277	\$ 0.2299	\$ 0.2322
0004	8955-01-538-0705	CAPPUCCINO, MOCHA	\$ 0.2268	\$ 0.2291	\$ 0.2314	\$ 0.2337	\$ 0.2360
0005	8955-01-556-0077	CAPPUCCINO, IRISH CREAM	\$ 0.2231	\$ 0.2254	\$ 0.2277	\$ 0.2299	\$ 0.2322
0006	8960-01-523-6344	BEVERAGE POWDER, ASCORBIC ACID/MALTDX, ORANGE	\$ 0.1035	\$ 0.1046	\$ 0.1056	\$ 0.1067	\$ 0.1078
0007	8960-01-523-6346	BEVERAGE POWDER, ASCORBIC ACID/MALTDX, LEMON-LIME	\$ 0.1005	\$ 0.1016	\$ 0.1026	\$ 0.1036	\$ 0.1047