

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF 14

1. CONTRACT/PURCH ORDER/AGREEMENT NO. SPE4A7-17-P-2872	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMDD) 2016 DEC 07	4. REQUISITION/PURCH REQUEST NO. 0066424596	5. PRIORITY DO-A1
--	-----------------------------------	---	---	-----------------------------

6. ISSUED BY DLA AVIATION ASC SUPPLIER OPER AE AND AF DIV 8000 JEFFERSON DAVIS HWY RICHMOND VA 23297 USA Local Admin: Steven Powell DSP0018 Tel: DSN-695-6228 Email: Steven.Powell@dia.mil	CODE	SPE4A7	7. ADMINISTERED BY (If other than 6) DLA AVIATION ASC SUPPLIER OPER AE AND AF DIV 8000 JEFFERSON DAVIS HWY RICHMOND VA 23297 USA Criticality: C PAS: None	CODE	SPE4A7	8. DELIVERY FOB DESTINATION <input type="checkbox"/> OTHER (See Schedule if other)
--	------	--------	--	------	--------	--

9. CONTRACTOR NAME AND ADDRESS HYDRO-AIRE, INC. 3000 WINONA AVE BURBANK CA 91504-2540 USA	CODE	81982	FACILITY	10. DELIVER TO FOB POINT BY (Date) (YYYYMMDD) 165 DAYS ADO	11. X IF BUSINESS IS <input type="checkbox"/> SMALL <input type="checkbox"/> SMALL DISADVANTAGED <input type="checkbox"/> WOMEN-OWNED
				12. DISCOUNT TERMS Net 30 days	
				13. MAIL INVOICES TO THE ADDRESS IN BLOCK See Block 15	

14. SHIP TO SEE SCHEDULE, DO NOT SHIP TO ADDRESSES ON THIS PAGE	CODE		15. PAYMENT WILL BE MADE BY DEF FIN AND ACCOUNTING SVC BSM P O BOX 182317 COLUMBUS OH 43218-2317 USA	CODE	SL4701	MARK ALL PACKAGES AND PAPERS WITH IDENTIFICATION NUMBERS IN BLOCKS 1 AND 2.
---	------	--	--	------	--------	--

16. TYPE OF ORDER	DELIVERY/ CALL		This delivery order/call is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract.			
	PURCHASE	<input checked="" type="checkbox"/>	Reference your Offer/Quote dated 2016 NOV 22 furnish the following on terms specified herein.			
ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.						

NAME OF CONTRACTOR	SIGNATURE	TYPED NAME AND TITLE	DATE SIGNED (YYYYMMDD)
If this box is marked, supplier must sign Acceptance and return the following number of copies:			

17. ACCOUNTING AND APPROPRIATION DATA/LOCAL USE

BX: 97X4930 5CBX 001 2620 S33189 \$528.00

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21.UNIT	22. UNIT PRICE	23. AMOUNT
	Award sent EDI, Do not duplicate shipment	48.000			

* 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.	24. UNITED STATES OF AMERICA Daniel Sink Daniel.Sink@dia.mil BY: PARFE25	 CONTRACTING/ORDERING OFFICER	25. TOTAL	26. DIFFERENCES
--	--	--	------------------	------------------------

27a. QUANTITY IN COLUMN 20 HAS BEEN

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

b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE		c. DATE (YYYYMMDD)	d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE			
e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		28. SHIP. NO.	29. D.O. VOUCHER NO.	30. INITIALS		
f. TELEPHONE NUMBER		g. E-MAIL ADDRESS		31. PAYMENT		
		PARTIAL		32. PAID BY		
		FINAL		33. AMOUNT VERIFIED CORRECT FOR		
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.		COMPLETE		34. CHECK NUMBER		
a. DATE (YYYYMMDD)	b. SIGNATURE AND TITLE OF CERTIFYING OFFICER		PARTIAL		35. BILL OF LADING NO.	
		FINAL				
37. RECEIVED AT	38. RECEIVED BY (Print)	39. DATE RECEIVED (YYYYMMDD)	40. TOTAL CONTAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.	

The following DLA Aviation Notices are incorporated by reference. The full-text of the notices can be found at: <http://www.dla.mil/Aviation/Business/IndustryResources/DLAResourcesforSuppliers/DAANs.aspx>

DAAN-11-01 Notification of Rejection of Award with Technical Data
(September 2016)

DAAN-13-02 Notification of Rejection of Unilateral Award
(September 2016)

First Destination Transportation (FDT) TAC - S8AF
Second Destination Transportation (SDT) TAC - S9NA

FOB: Origin
INSPECTION/ACCEPTANCE: Destination

YOU ARE ENCOURAGED AND AUTHORIZED TO MAKE EARLY DELIVERIES ON THIS REQUIREMENT AT NO ADDITIONAL COST TO THE GOVERNMENT.

CONTINUED ON NEXT PAGE

SECTION B

SUPPLIES/SERVICES: 2915-00-605-9903
MFR. CAGE: 81982 P/N: 60-12523

ITEM DESCRIPTION:

HOLDER, BEARING
RP001: DLA PACKAGING REQUIREMENTS FOR PROCUREMENT

RA001: THIS DOCUMENT INCORPORATES TECHNICAL AND/OR QUALITY REQUIREMENTS (IDENTIFIED BY AN 'R' OR AN 'I' NUMBER) SET FORTH IN FULL TEXT IN THE DLA MASTER LIST OF TECHNICAL AND QUALITY REQUIREMENTS FOUND ON THE WEB AT: <http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx>. FOR SIMPLIFIED ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE SOLICITATION ISSUE DATE OR THE AWARD DATE CONTROLS. FOR LARGE ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE RFP ISSUE DATE APPLIES UNLESS A SOLICITATION AMENDMENT INCORPORATES A FOLLOW-ON REVISION, IN WHICH CASE THE AMENDMENT DATE CONTROLS.

RQ001: HIGHER LEVEL CONTRACT QUALITY REQUIREMENTS (MANUFACTURERS AND NON-MANUFACTURERS)

RQ002: CONFIGURATION CHANGE MANAGEMENT - ENGINEERING CHANGE PROPOSAL REQUEST FOR VARIANCE (DEVIATION OR WAIVER)

RQ011: REMOVAL OF GOVERNMENT IDENTIFICATION FROM NON-ACCEPTED SUPPLIES

CRANE CO, HYDRO-AIRE DIV

SAMPLING:

THE SAMPLING METHOD SHALL BE IN ACCORDANCE WITH MIL-STD-1916 OR ASQ H1331, TABLE 1 OR A COMPARABLE ZERO BASED SAMPLING PLAN UNLESS OTHERWISE SPECIFIED BY THE CONTRACT. IF THE APPLICABLE DRAWING, SPECIFICATION, STANDARD, OR QUALITY ASSURANCE PROVISION (QAP) SPECIFIES CRITICAL, MAJOR AND/OR MINOR ATTRIBUTES, THEY SHALL BE ASSIGNED VERIFICATION LEVELS OF VII, IV AND II OR AQLS OF 0.1, 1.0 AND 4.0 RESPECTIVELY. UNSPECIFIED ATTRIBUTES SHALL BE CONSIDERED AS MAJOR UNLESS SAMPLING PLANS ARE SPECIFIED IN APPLICABLE DOCUMENTS. FOR MIL-STD-1916, THE MANUFACTURER MAY USE THE ATTRIBUTE OR VARIABLE INSPECTION METHOD AT THEIR OPTION OR PER THE CONTRACT. MIL-STD-105/ASQ Z1.4 MAY BE USED TO SET SAMPLE LOT SIZE, BUT ACCEPTANCE WOULD BE ZERO NON-CONFORMANCES IN THE SAMPLE LOT UNLESS OTHERWISE SPECIFIED IN THE CONTRACT.

DSCR DOES NOT CURRENTLY HAVE AN APPROVED

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 2915-00-605-9903 MFR. CAGE: 81982 P/N: 60-12523 CONT'D

TECHNICAL DATA PACKAGE AVAILABLE FOR THIS NSN.
DATA IS PROPRIETARY OR INSUFFICIENT FOR
COMPETITIVE PROCUREMENT.

SAMPLING:

CRITICAL APPLICATION ITEM

HYDRO-AIRE, INC. 81982 P/N 60-12523

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	2915-00-605-9903 CAGE/PN: 81982 60-12523 HOLDER, BEARING	48.000	EA		

PRICING TERMS: Firm Fixed Price

QTY VARIANCE: PLUS 0% MINUS 0%

INSPECTION POINT: DESTINATION

ACCEPTANCE POINT: DESTINATION

FOB: ORIGIN DELIVERY DATE: 2017 MAY 22

PREP FOR DELIVERY:

PKGING DATA-QUP:001

SHALL BE PACKAGED IN ACCORDANCE WITH ASTM D 3951.

Markings Paragraph

When ASTM D3951, Commercial Packaging is specified, the following apply:

- ,,All Section "D" Packaging and Marking Clauses take precedence over ASTM D3951.
- ,,In addition to requirements in MIL-STD-129, when Commercial Packaging is used, the Method of Preservation for all MIL-STD-129 marking and labeling shall be "CP" Commercial Pack.
- ,,The Unit of Issue (U/I) and Quantity per Unit Pack (QUP) as specified in the contract take precedence over QUP in ASTM D3951.

PARCEL POST ADDRESS:

SW3211
DLA DISTRIBUTION DEPOT OKLAHOMA
3301 F AVE CEN REC BLDG 506 DR 22

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 2915-00-605-9903 MFR. CAGE: 81982 P/N: 60-12523 CONT'D

TINKER AFB OK 73145-8000
USFOR TRANSPORTATION ASSISTANCE SEE DLAD 52.247-9034. FOR FIRST DESTINATION TRANSPORTATION (FDT) AWARDS SEE
DLAD 52.247-9059 AND
CONTRACT INSTRUCTIONS INSTEAD.

FREIGHT SHIPPING ADDRESS:

SW3211
DLA DISTRIBUTION DEPOT OKLAHOMA
3301 F AVE CEN REC BLDG 506 DR 22
TINKER AFB OK 73145-8000
US

GOVT USE

ITEM	PR	External		External	External	Customer RDD/ Need Ship Date
		PRLI	PR	PRLI	Material	
0001	0066424596	0001	N/A	N/A	N/A	N/A

CONTINUED ON NEXT PAGE

SECTION A - SOLICITATION/CONTRACT FORM

TECHNICAL REQUIREMENTS

THIS DOCUMENT INCORPORATES TECHNICAL AND/OR QUALITY REQUIREMENTS (IDENTIFIED BY AN 'R' OR AN 'I' NUMBER IN SECTION B) SET FORTH IN FULL TEXT IN THE DLA MASTER LIST OF TECHNICAL AND QUALITY REQUIREMENTS FOUND ON THE WEB AT: <http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx>. FOR SIMPLIFIED ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE SOLICITATION ISSUE DATE OR THE AWARD DATE CONTROLS. FOR LARGE ACQUISITIONS, THE REVISION OF THE MASTER IN EFFECT ON THE RFP ISSUE DATE APPLIES UNLESS A SOLICITATION AMENDMENT INCORPORATES A FOLLOW-ON REVISION, IN WHICH CASE THE AMENDMENT DATE CONTROLS.

SECTION C - SPECIFICATIONS/SOW/SOO/ORD

C03 CONTRACTOR RETENTION OF SUPPLY CHAIN TRACEABILITY DOCUMENTATION (SEP 2016)

SECTION D - PACKAGING AND MARKING

252.211-7006 RADIO FREQUENCY IDENTIFICATION (SEP 2011) DFARS

(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, AP1.1.11:

- (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/rfid/> 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 at http://www.acq.osd.mil/log/rfid/tag_data.htm. 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/>.

(End of clause)

SECTION E - INSPECTION AND ACCEPTANCE

52.246-2 INSPECTION OF SUPPLIES FIXED PRICE (AUG 1996) FAR

52.246-11 HIGHER-LEVEL CONTRACT QUALITY REQUIREMENT (DEC 2014) FAR

The Contractor shall comply with the higher-level quality standard selected below. [If more than one standard is listed, the offeror shall indicate its selection by checking the appropriate block.]

	Title	Number	Date	Tailoring
<input type="checkbox"/>	ISO 9001:2000			
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

[Contracting Officer insert the title, number (if any), date, and tailoring (if any) of the higher-level quality standards.]
(End of clause)

SECTION F - DELIVERIES OR PERFORMANCE

52.211-16 VARIATION IN QUANTITY (APR 1984) FAR

(b) The permissible variation shall be limited to:
00 Percent increase
00 Percent decrease
This increase or decrease shall apply to the total contract quantity .

52.211-17 DELIVERY OF EXCESS QUANTITIES (SEP 1989) FAR

52.242-17 GOVERNMENT DELAY OF WORK (APR 1984) FAR

52.247-29 F.O.B. ORIGIN (FEB 2006) FAR

52.247-65 F.O.B. ORIGIN, PREPAID FREIGHT - SMALL PACKAGE SHIPMENTS (JAN 1991) FAR

52.247-9059 F.O.B. Origin, Government Arranged Transportation (OCT 2013) DLAD

SECTION I - CONTRACT CLAUSES

252.203-7000 REQUIREMENTS RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2011) DFARS**252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013) DFARS****252.203-7997 PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (OCT 2015) DFARS**

(a) The Contractor shall not require employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or contractors 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.

(b) The Contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this clause are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(d)(1) Use of funds appropriated (or otherwise made available) by the Continuing Appropriations Act, 2016 (Pub. L. 114-53) or any other FY 2016 appropriations act that extends to FY 2016 funds the same prohibitions as contained in sections 743 of division E, title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(2) The Government may seek any available remedies in the event the Contractor fails to perform in accordance with the terms and conditions of the contract as a result of Government action under this clause.

(End of clause)

252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992) DFARS**252.204-7004 ALTERNATE A, SYSTEM FOR AWRD MANAGEMENT (FEB 2014) DFARS****252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016) 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 (OCT 2016) DFARS

CONTINUED ON NEXT PAGE

(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)

**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.

CONTINUED ON NEXT PAGE

"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.

(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—

CONTINUED ON NEXT PAGE

(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, 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.

CONTINUED ON NEXT PAGE

(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)

52.211-15 DEFENSE PRIORITY AND ALLOCATION REQUIREMENTS (APR 2008) FAR

52.215-08 ORDER OF PRECEDENCE - UNIFORM CONTRACT FORMAT (OCT 1997) FAR

52.222-50 COMBATTING TRAFFICKING IN PERSONS (MAR 2015) FAR

52.223-18 ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING (AUG 2011) FAR

52.225-13 RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (JUN 2008) FAR

52.232-01 PAYMENTS (APR 1984) FAR

52.232-08 DISCOUNTS FOR PROMPT PAYMENT (FEB 2002) FAR

52.232-11 EXTRAS (APR 1984) FAR

52.232-25 PROMPT PAYMENT (JUL 2013) FAR

252.232-7003 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS AND RECEIVING REPORTS (JUN 2012) DFARS

52.233-01 DISPUTES (MAY 2014) FAR

52.233-03 PROTEST AFTER AWARD (AUG 1996) FAR

52.233-04 APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004) FAR

52.244-06 SUBCONTRACTS FOR COMMERCIAL ITEMS (DEC 2015) FAR

CONTINUED ON NEXT PAGE

52.247-01 COMMERCIAL BILL OF LADING NOTATIONS (FEB 2006) FAR

When the Contracting Officer authorizes supplies to be shipped on a commercial bill of lading and the Contractor will be reimbursed these transportation costs as direct allowable costs, the Contractor shall ensure before shipment is made that the commercial shipping documents are annotated with either of the following notations, as appropriate:

(a) If the Government is shown as the consignor or the consignee, the annotation shall be:

Transportation is for the _____ [name the specific agency] and the actual total transportation charges paid to the carrier(s) by the consignor or consignee are assignable to, and shall be reimbursed by, the Government.

(b) If the Government is not shown as the consignor or the consignee, the annotation shall be:

Transportation is for the _____ [name the specific agency] and the actual total transportation charges paid to the carrier(s) by the consignor or consignee shall be reimbursed by the Government, pursuant to cost-reimbursement contract No. _____.

This may be confirmed by contacting _____ [Name and address of the contract administration office listed in the contract].

(End of clause)

52.247-7023 TRANSPORTATION OF SUPPLIES BY SEA (APR 2014) DFARS**52.249-01 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE) (SHORT FORM) (APR 1984) FAR****52.252-02 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) FAR**

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://www.dla.mil/Acquisition> and <http://farsite.hill.af.mil/>.

(End of Clause)

52.252-06 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984) FAR

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any DoD FAR Supplement (DFARS) (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

52.253-01 COMPUTER GENERATED FORMS (JAN 1991) FAR**252.222-7007 REPRESENTATION REGARDING COMBATING TRAFFICKING IN PERSONS (JAN 2015) DFARS****252.225-7048 EXPORT CONTROLLED ITEMS (JUN 2013) DFARS**

(a) *Definition.* "Export-controlled items," as used in this clause, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes:

(1) "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120.

(2) "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.

(b) The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.

(c) The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.

(d) Nothing in the terms of this contract adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to—

(1) The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, *et seq.*);

(2) The Arms Export Control Act (22 U.S.C. 2751, *et seq.*);

(3) The International Emergency Economic Powers Act (50 U.S.C. 1701, *et seq.*);

(4) The Export Administration Regulations (15 CFR Parts 730-774);

(5) The International Traffic in Arms Regulations (22 CFR Parts 120-130); and

(6) Executive Order 13222, as extended.

(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts.

(End of clause)

CONTINUED ON NEXT PAGE

