

ORDER FOR SUPPLIES OR SERVICES										PAGE 1 OF 12	
1. CONTRACT/PURCH ORDER/AGREEMENT NO. SPEFA5-17-P-0514			2. DELIVERY ORDER/CALL NO.		3. DATE OF ORDER/CALL (YYYYMMDD) 2017 FEB 25		4. REQUISITION/PURCH REQUEST NO. N01DLA70060003		5. PRIORITY DO-C9		
6. ISSUED BY DLA AVIATION AT CHERRY POINT, NC FLEET READINESS CENTER EAST PSC BOX 8021 CHERRY POINT NC 28533-0021 USA Local Admin: Parren Tatum DPT0001 Tel: 252-466-2909 Email: Parren.Tatum@dla.mil			CODE SPEFA5		7. ADMINISTERED BY (If other than 6) DLA AVIATION AT CHERRY POINT, NC FLEET READINESS CENTER EAST PSC BOX 8021 CHERRY POINT NC 28533-0021 USA Criticality: A PAS: None			CODE SPEFA5		8. DELIVERY FOB <input checked="" type="checkbox"/> 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) 170 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 2017 FEB 03 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)	
<input type="checkbox"/>				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 \$540.00											
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				6.000					
* 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 Harvey Brooks Harvey.Brooks@dla.mil BY: GPP7839				25. TOTAL			
				26. DIFFERENCES							
27a. QUANTITY IN COLUMN 20 HAS BEEN <input type="checkbox"/> INSPECTED <input type="checkbox"/> RECEIVED <input type="checkbox"/> 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					
						PARTIAL FINAL		32. PAID BY		33. AMOUNT VERIFIED CORRECT FOR	
36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.						31. PAYMENT <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL				34. CHECK NUMBER	
a. DATE (YYYYMMDD)		b. SIGNATURE AND TITLE OF CERTIFYING OFFICER								35. BILL OF LADING NO.	
37. RECEIVED AT		38. RECEIVED BY (Print)		39. DATE RECEIVED (YYYYMMDD)		40. TOTAL CONTAINERS		41. S/R ACCOUNT NUMBER		42. S/R VOUCHER NO.	

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 2 OF 12 PAGES
--------------------	--	--------------------

PER BAM 13-33 06/14/13, DLA Aviation local clauses
IMSP Guidance.

** ATTENTION VENDORS **

PLEASE USE THE FOLLOWING LINK FOR ALL PAYMENT AND WIDE AREA WORKFLOW INFORMATION:

<http://www.dfas.mil/ecommerce/wawf/info.html>
<http://www.dla.mil/WideAreaWorkflow/Pages/default.aspx>

**PLEASE INCLUDE ALL THE ORIGINAL DOCUMENT NUMBERS (ODN's) ON THE PACAKGING SLIPS SO THAT ALL MATERIAL IS
RECEIPTED CORRECTLY FOR ALL DELIVERIES. **

Accelerated and partial deliveries are acceptable

LINE ITEM #1 PR# 67032026
DESCRIPTION: PLATE, ID
PN#- 56285
ODN: N01DLA70060003
FOB - DESTINATION
INSPECTION/ACCEPTANCE POINT - DESTINATION

PLEASE REFER TO YOUR QUOTE # : DATED: E-Mail of 15 Feb 17

OUR AWARD SPEFA517P0514 OR SOLICITATION # SPEFA317Q1013 :

NOTIFICATION OF REJECTION OF UNILATERAL AWARD (MAR 2001)

Unless this is a bilateral award, notice of rejection as described herein is required. The Government's offer to purchase, as evidenced by this order, is made on the basis of your quotation. Although you are not legally obligated to perform on a unilateral purchase order, you should promptly notify the DLA Aviation contract administrator in writing if you do not intend to perform this order by the specified delivery date. Prompt notification means as soon after receiving notice of award as practicable given the circumstances.

FAILURE TO PROVIDE PROMPT NOTICE WILL ADVERSELY AFFECT YOUR PAST PERFORMANCE AUTOMATED BEST VALUE SYSTEM SCORE IF THIS ORDER IS LATER CANCELLED AT OTHER THAN THE GOVERNMENT'S REQUEST.

52.204-21 - Basic Safeguarding of Covered Contractor Information Systems. APPLIES TO ALL SOLICITATIONS AND AWARDS

CONTINUED ON NEXT PAGE

SECTION B

SUPPLIES/SERVICES: 6105-LN0019390
MFR. CAGE: 81982 P/N: 56285

ITEM DESCRIPTION:

PLATE, ID

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.

RP001: DLA PACKAGING REQUIREMENTS FOR PROCUREMENT

MIL-STD-130N(1) DATED 16 NOV 2012.
IDENTIFICATION MARKING OF U.S. MILITARY PROPERTY

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.
NO SHELF LIFE

HYDRO-AIRE, INC. CAGE: 81982 P/N: 56285

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	6105-LN0019390 PLATE, ID	6.000	EA		

PRICING TERMS: Firm Fixed Price

QTY VARIANCE: PLUS 0% MINUS 0%

INSPECTION POINT: DESTINATION

ACCEPTANCE POINT: DESTINATION

FOB: DESTINATION DELIVERY DATE: 2017 AUG 14

PREP FOR DELIVERY:

PKGING DATA-QUP:001

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 6105-LN0019390 MFR. CAGE: 81982 P/N: 56285 CONT'D

SHALL BE PACKAGED STANDARD 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:

N01DLA
FLEET READINESS CENTER DLA
BEACHEY ROAD, BUILDING 148, BAY C
CHERRY POINT NC 28533-5040
US

FREIGHT SHIPPING ADDRESS:

N01DLA
FLEET READINESS CENTER DLA
BEACHEY ROAD, BUILDING 148, BAY C
CHERRY POINT NC 28533-5040
US

GOVT USE

		External		External	External	Customer RDD/
ITEM	PR	PRLI	PR	PRLI	Material	Need Ship Date
0001	0067032026	0001	N/A	N/A	9905015583504	N/A

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 5 OF 12 PAGES
--------------------	--	--------------------

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)

C01 SUPERSEDED PART NUMBERED ITEMS (SEP 2016)

SECTION E - INSPECTION AND ACCEPTANCE

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

SECTION F - DELIVERIES OR PERFORMANCE

52.211-16 VARIATION IN QUANTITY (APR 1984) FAR

(b) The permissible variation shall be limited to:

0 Percent increase

0 Percent decrease

This increase or decrease shall apply to ALL .

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

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

52.247-34 F.O.B. DESTINATION (NOV 1991) FAR

SECTION G - CONTRACT ADMINISTRATION DATA

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013) DFARS

(a) Definitions. As used in this clause—

“Department of Defense Activity Address Code (DoDAAC)” is a six position code that uniquely identifies a unit, activity, or organization.

“Document type” means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

“Local processing office (LPO)” is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall—

(1) Have a designated electronic business point of contact in the Central Contractor Registration at <https://www.acquisition.gov>; and

(2) Be registered to use WAWF at <https://wawf.eb.mil/> following the step-by-step procedures for self-registration available at this web site.

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 6 OF 12 PAGES
--------------------	--	--------------------

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the “Web Based Training” link on the WAWF home page at <https://wawf.eb.mil/>

(e) WAWF methods of document submission. Document submissions may be via web entry, Electronic Data Interchange, or File Transfer Protocol **or Payweb**

- (1) To access PayWeb, the vendor may go to the following site: <https://onronline.onr.navy.mil/payweb/>
- (2) For instructions on PayWeb payment request submission, please contact the office identified below:

(Contracting Officer: Insert applicable ONR Regional Office information)]

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).
COMBO
Note: If a “Combo” document type is identified but not supportable by the Contractor’s business systems, an “Invoice” (stand-alone) and “Receiving Report” (stand-alone) document type may be used instead.)

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

DESTINATION

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table*

Field Name in WAWF	Data to be entered in WAWF
Pay Official DoDAAC	SEE PG 1 BLK 15
Issue By DoDAAC	SEE PG 1, BLK 6
Admin DoDAAC	SEE PG 1, BLK 7
Inspect By DoDAAC	SEE SEC B
Ship To Code	SEE SEC B
Ship From Code	SEE PG 1, BLK 9
Mark For Code	SEE SEC B
Service Approver (DoDAAC)	N/A
Service Acceptor (DoDAAC)	N/A
Accept at Other DoDAAC	N/A
LPO DoDAAC	N/A
DCAA Auditor DoDAAC	N/A
Other DoDAAC(s)	N/A

(*Contracting Officer: Insert applicable DoDAAC information or “See schedule” if multiple ship to/acceptance locations apply, or “Not applicable.”)

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the e-mail address identified below in the “Send Additional Email Notifications” field of WAWF once a document is submitted in the system.

(g) WAWF point of contact.

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 7 OF 12 PAGES
--------------------	--	--------------------

(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.
(End of clause)

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

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016) FAR

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

(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

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 8 OF 12 PAGES
--------------------	--	--------------------

- (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.
- “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.

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 9 OF 12 PAGES
--------------------	--	--------------------

"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—

(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

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 10 OF 12 PAGES
	<p>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</p> <p>(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</p> <p>(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.</p> <p>(c) <i>Cyber incident reporting requirement.</i></p> <p>(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—</p> <p>(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</p> <p>(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.</p> <p>(2) <i>Cyber incident report.</i> The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.</p> <p>(3) <i>Medium assurance certificate requirement.</i> In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.</p> <p>(d) <i>Malicious software.</i> 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.</p> <p>(e) <i>Media preservation and protection.</i> 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.</p> <p>(f) <i>Access to additional information or equipment necessary for forensic analysis.</i> Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.</p> <p>(g) <i>Cyber incident damage assessment activities.</i> 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.</p> <p>(h) <i>DoD safeguarding and use of contractor attributional/proprietary information.</i> 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.</p> <p>(i) <i>Use and release of contractor attributional/proprietary information not created by or for DoD.</i> 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—</p> <p>(1) To entities with missions that may be affected by such information;</p> <p>(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;</p> <p>(3) To Government entities that conduct counterintelligence or law enforcement investigations;</p> <p>(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</p> <p>(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.</p> <p>(j) <i>Use and release of contractor attributional/proprietary information created by or for DoD.</i> 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</p>	

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 11 OF 12 PAGES
--------------------	--	---------------------

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

52.222-50 COMBATING TRAFFICKING IN PERSONS (MAR 2015), ALT I (MAR 2015) FAR

(B) The following directive(s) or notice(s) applicable to employees performing work at the contract place(s) of performance as indicated below:

Document Title:	Document may be obtained from:	Applies performance to in/at:

[Contracting Officer shall insert title of directive/notice; indicate the document is attached or provide source (such as website link) for obtaining document; and, indicate the contract performance location outside the U.S. to which the document applies.]

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

252.247-7023 TRANSPORTATION OF SUPPLIES BY SEA (APR 2014) DFARS

CONTINUED ON NEXT PAGE

CONTINUATION SHEET	REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPEFA5-17-P-0514	PAGE 12 OF 12 PAGES
--------------------	--	---------------------

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)