ORDER FOR SUPPLIES OR SERVICES

1. CONTRACT/PURCH ORDER/AGREEMENT NO.	2. DELIVERY ORDER/CALL NO.	3. DATE OF ORDER/CALL (YYYYMMMDD)	4. REQUISITION/PURCH REQUEST NO.	5. PRIORITY
SPE5EK-16-V-2722		2016 MAR 15	0059736345	DO-C9

6. ISSUED BY CODE SPE5EK

DLA TROOP SUPPORT
HARDWARE (ACQ III-2)
700 ROBBINS AVENUE
PHILADELPHIA PA 19111
USA
Local Admin: KATHLEEN LEUZZI PHPHDAH Tel: 215-737-2176 Fax: 215-737-5227
Email: KATHLEEN.LEUZZI@DLA.MIL

7. ADMINISTERED BY (*If other than 6*) CODE SPE5EK

DLA TROOP SUPPORT
HARDWARE (ACQ III-2)
700 ROBBINS AVENUE
PHILADELPHIA PA 19111
USA
Criticality: C PAS: None

8. DELIVERY FOB
- [ ] DESTINATION
- [X] OTHER

(See Schedule if other)

9. CONTRACTOR CODE 81982 FACILITY

NAME AND ADDRESS
HYDRO-AIRE, INC. DBA
3000 WINONA AVE
BURBANK CA 91504-2540
USA

10. DELIVER TO FOB POINT BY (*Date*) (YYYYMMMDD)
195 DAYS ADO

11. X IF BUSINESS IS
- [ ] SMALL
- [ ] SMALL DISAD-VANTAGED
- [ ] WOMEN-OWNED

12. DISCOUNT TERMS
Net 30 days

13. MAIL INVOICES TO THE ADDRESS IN BLOCK
See Block 15

14. SHIP TO CODE

SEE SCHEDULE, DO NOT SHIP TO ADDRESSES ON THIS PAGE

15. PAYMENT WILL BE MADE BY CODE SL4701

DEF FIN AND ACCOUNTING SVC
BSM
P O BOX 182317
COLUMBUS OH 43218-2317
USA

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	X	Reference your Offer/Quote dated 2015 AUG 05, 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 (YYYYMMMDD)

[ ] 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

18. ITEM NO.	19. SCHEDULE OF SUPPLIES/SERVICES	20. QUANTITY ORDERED/ ACCEPTED*	21. UNIT	22. UNIT PRICE	23. AMOUNT
	THE PURCHASE ORDER CLAUSES ARE APPLICABLE AS INDICATED IN THE DLA MASTER SOLICITATION FOR EPROCUREMENT AUTOMATED SIMPLIFIED ACQUISITIONS (PART 13) REVISION 31 (DECEMBER 15, 2015) WHICH CAN BE FOUND ON THE WEB AT http://www.dla.mil/Portals/104/Documents/J7Acquisition/Master%20Solicitation%20REV%2031%20DEC%2015.pdf Award sent EDI, Do not duplicate shipment	122			

** 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
MICHELLE GEMMELL
MICHELLE.GEMMELL@DLA.MIL
BY: PHPHACJ
Michelle Gemmell
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 (*YYYYMMMDD*)

d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE

f. TELEPHONE NUMBER

g. E-MAIL ADDRESS

28. SHIP. NO.

29. D.O. VOUCHER NO.

30. INITIALS

31. PAYMENT
[ ] PARTIAL [ ] FINAL

32. PAID BY

33. AMOUNT VERIFIED CORRECT FOR

34. CHECK NUMBER

35. BILL OF LADING NO.

36. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT.
[ ] COMPLETE [ ] PARTIAL [ ] FINAL

a. DATE (*YYYYMMMDD*)

b. SIGNATURE AND TITLE OF CERTIFYING OFFICER

37. RECEIVED AT	38. RECEIVED BY (*Print*)	39. DATE RECEIVED (*YYYYMMMDD*)	40. TOTAL CON-TAINERS	41. S/R ACCOUNT NUMBER	42. S/R VOUCHER NO.

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

(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

CONTINUED ON NEXT PAGE

(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

CONTINUED ON NEXT PAGE

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

CONTINUED ON NEXT PAGE

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

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

(c) *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

CONTINUED ON NEXT PAGE

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.*

CONTINUED ON NEXT PAGE

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)

This is a First Destination Transportation (FDT) program award. If this award is for FMS or has an APO/FPO ship-to address, these instructions do not apply and normal procedures should be followed.

1. CONUS AWARDEES SHIPPING TO ALL LOCATIONS: Transportation requirements for FDT awards are located in DLAD clauses 52.247-9059 F.o.b. Origin, Government Arranged Transportation and 52.247-9058, First Destination Transportation (FDT) Program - Shipments Originating Outside the contiguous United States (OCONUS).

CONTINUED ON NEXT PAGE

2. OCONUS AWARDEE SHIPPING TO CONUS DESTINATION: If awardee is outside the continental United States (OCONUS) and is shipping to a location in the continental United States (CONUS), transportation requirements are located in DLAD clauses 52.247-9058, First Destination Transportation (FDT) Program – Shipments Originating Outside the contiguous United States (OCONUS) and 52.247-9059 F.O.B. Origin, Government Arranged Transportation.

3. OCONUS AWARDEE SHIPPING TO OCONUS LOCATION: If awardee is outside the continental United States (OCONUS) and is shipping to a location outside the continental United States (OCONUS), contact the Transportation Office at delivery@dla.mil with "FDT OCONUS Shipment" in the subject line for instructions. Transportation requirements are located in DLAD clauses 52.247-9058, First Destination Transportation (FDT) Program – Shipments Originating Outside the contiguous United States (OCONUS) and 52.247-9059 F.O.B. Origin, Government Arranged Transportation.

4. OCONUS AWARDEE WITH INSPECTION AND ACCEPTANCE AT ORIGIN: If awardee is outside the continental United States (OCONUS) and Inspection and Acceptance are at Origin, normal DCMA transportation procedures should be followed and paragraphs 1, 2 and 3 above do not apply.

CONTINUED ON NEXT PAGE

SECTION B

PR: 0059736345
SUPPLIES/SERVICES:

5360003818044

SPRING,HELICAL,COMP

SPRING, HELICAL, COMPRESSION
CRES
HYDRO-AIRE DIV CRANE CO
BURBANK CA
WHEN THE PURCHASE ORDER TEXT (POT)
DESCRIBES THE REQUIRED PRODUCT(S) BY NAME AND
PART NUMBER OF A SPECIFIC ENTITY, BY THE NAMES
AND PART NUMBERS OF A NUMBER OF SPECIFIC
ENTITIES, OR BY THE NAME(S) AND PART NUMBER(S)
OF SPECIFIC ENTITY/ENTITIES AS MODIFIED BY
ADDITIONAL REQUIREMENTS SET FORTH IN THE POT
ONLY THAT/THOSE PRODUCT(S) HAVE BEEN DETERMINED
TO MEET THE NEEDS OF THE GOVERNMENT AND ARE
ACCEPTABLE. SUCH PRODUCT(S) ARE EXACT
PRODUCT(S) AS DEFINED IN DLAD 52.217-9002,
CONDITIONS FOR EVALUATION AND ACCEPTANCE OF
OFFERS FOR PART NUMBERED ITEMS.

A VENDOR OFFER/QUOTATION, BID WITHOUT
EXCEPTION, IS A CERTIFICATION THAT THE EXACT
PRODUCT, MANUFACTURED AND/OR SUPPLIED BY ONE
OF THE ENTITIES CITED IN THE POT WILL BE
FURNISHED UNDER THE CONTRACT OR ORDER. ANY
PRODUCT NOT MANUFACTURED AND/OR SUPPLIED
BY ONE OF THE ENTITIES CITED IN THE POT
IS AN ALTERNATE PRODUCT, EVEN THOUGH IT
MIGHT BE MANUFACTURED IN ACCORDANCE WITH THE
DRAWING(S) AND/OR SPECIFICATIONS OF ONE OF THE
ENTITIES CITED IN THE POT.

IF AN ALTERNATE PRODUCT IS FURNISHED UNDER A
CONTRACT OR ORDER FOR AN EXACT PRODUCT, THE
ALTERNATE PRODUCT WILL BE AN UNAUTHORIZED
SUBSTITUTION, AND MAY YIELD CRIMINAL PENALTIES
IN ADDITION TO ANY CIVIL REMEDIES AVAILABLE TO
THE GOVERNMENT.

THIS ITEM IS IDENTIFIED AS A COMMERCIAL ITEM - (TO INCLUDE 'COMMERCIAL
OF A TYPE')

ADEQUATE DATA FOR EVALUATION OF ALTERNATE
OFFERS IS NOT AVAILABLE AT THE PROCUREMENT
AGENCY. THE OFFEROR MUST PROVIDE A COMPLETE
DATA PACKAGE INCLUDING DATA FOR THE APPROVED AND
ALTERNATE PART FOR EVALUATION.

CRITICAL APPLICATION ITEM

HYDRO-AIRE, INC. DBA 81982 P/N 86235

CONTINUED ON NEXT PAGE

SECTION B

CLIN	PR	PRLI	UI	QUANTITY	UNIT PRICE	CURRENCY	TOTAL PRICE
0001	0059736345	0001	EA	122.000			

NSN/MATERIAL:5360003818044

QTY VARIANCE: PLUS 00.00% MINUS 00.00%

INSPECTION POINT: DESTINATION

ACCEPTANCE POINT: DESTINATION

PREP FOR DELIVERY:

PKGING DATA-QUP:025

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.

DELIVER FOB: ORIGIN DELIVER BY: 2016 SEP 26

PARCEL POST ADDRESS:

UY8619
ARIZONA INDUSTRIES FOR THE BLIND
515 N 51ST AVENUE NUMBER 130 DOCK 2
PHOENIX AZ 85043
US

FOR 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:

UY8619
ARIZONA INDUSTRIES FOR THE BLIND
515 N 51ST AVENUE NUMBER 130 DOCK 2
PHOENIX AZ 85043
US

* *