AWARD/CONTRACT J

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE	OF	PAGES
	DO-C9	1		11

2. CONTRACT *(Proc. Inst. Ident.)* NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
SPE7MC-16-C-0053	SEE BLOCK 20C	0061276618

5. ISSUED BY CODE SPE7MC

DLA LAND AND MARITIME
MARITIME HARDWARE/ELECTRICAL
P O BOX 3990
COLUMBUS OH 43218-3990
USA
Local Admin: William Manning PMCMKKD Tel: 614-692-9748 Fax: 614-692-2474
Email: DLA.Maritime.Postaward.FMSE2@dla.mil

6. ADMINISTERED BY (*If other than Item 5*) CODE S0512A

DCMA LOS ANGELES
16111 PLUMMER STREET,BUILDING 10, 2
BLDG 10, 2ND FLOOR
NORTH HILLS CA 91343-2036
USA
Criticality: B PAS: None

7. NAME AND ADDRESS OF CONTRACTOR (*No., street, city, county, State and ZIP Code*)

HYDRO-AIRE, INC.
3000 WINONA AVE
BURBANK CA 91504-2540
USA

CODE 81982 FACILITY CODE

8. DELIVERY

[X] FOB ORIGIN [ ] OTHER (*See below*)

9. DISCOUNT FOR PROMPT PAYMENT

Net 30 days

10. SUBMIT INVOICES *(4 copies unless otherwise specified)* TO THE ADDRESS SHOWN IN ITEM 12

11. SHIP TO/MARK FOR CODE

SEE SCHEDULE, DO NOT SHIP TO ADDRESS ON THIS PAGE

12. PAYMENT WILL BE MADE BY CODE SL4701

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

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:

[X] 10 U.S.C. 2304(c) 1 [ ] 41 U.S.C. 253(c)

14. ACCOUNTING AND APPROPRIATION DATA

BX: 97X4930 5CBX 001 2620 S33189 $461875.00

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	Award sent EDI, Do not duplicate shipment	25.000			

15G. TOTAL AMOUNT OF CONTRACT

16. TABLE OF CONTENTS

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

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. [X] CONTRACTOR'S NEGOTIATED AGREEMENT *(Contractor is required to sign this document and return* 1 *copies to issuing office.)* Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (*Attachments are listed herein.*)

18. [ ] SEALED-BID AWARD *(Contractor is not required to sign this document.)* Your bid on Solicitation Number _____, including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)

19A. NAME AND TITLE OF SIGNER *(Type or Print)*

20A. NAME OF CONTRACTING OFFICER

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
BY _____ *(Signature of person authorized to sign)*		BY _____ *(Signature of Contracting Officer)*	

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 FOB Origin, Government Arranged Transportation and 52.247-9058, First Destination Transportation (FDT) Program - Shipments Originating Outside the contiguous United States (OCONUS).

2. OCONUS AWARDEE SHIPPING TO CONUS DESTINATION: If awardee is outside the continental United States (OCONUS) and 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 FOB 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 (FDT) Program - Shipments originating outside the contiguous United States (OCONUS) and 52.247-9059 FOB 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.

TIME OF DELIVERY
The following delivery schedule applies to this award.

Delivery Schedule:
Item number: 0001
Quantity: 25 EA
Days: 388

Liquidated damages ( ) are (X) are not applicable.
Note: Accelerated delivery is acceptable at no additional cost to the Government

CONTINUED ON NEXT PAGE

SECTION B

SUPPLIES/SERVICES: 4810-00-529-4083

ITEM DESCRIPTION:

VALVE, DIRECTIONAL FLOW CONTROL

If this NSN provides Contract Data Requirement Lists (CDRLs) as part of the Technical Data Package, the line items from this solicitation are not to be separately priced. Offerors must factor into the end item unit price all costs associated with the preparation and delivery of the data deliverables in the contract.

SOLENOID OPERATED 3 PORTS

52.246-11 Higher Level Contract Quality Requirement (Manufacturers)

FAR CLAUSE 52.246-11 APPLIES. A QUALITY MANAGEMENT PROGRAM MEETING THE REQUIREMENTS OF ISO 9001:2008; A PROGRAM COMPARABLE TO ISO 9001:2008 (EXAMPLE SAE AS 9100), THE FOLLOWING TAILORED VERSION OF ISO 9001:2008; OR A PROGRAM COMPARABLE TO THE TAILORED VERSION OF ISO 9001:2008 (EXAMPLE SAE AS 9003) IS REQUIRED. MIL-I-45208 AND MIL-Q-9858 ARE OBSOLETE AND NO LONGER CONSIDERED SUITABLE WHEN HIGHER LEVEL QUALITY IS REQUIRED. IN THE TAILORED VERSION OF THE ISO 9001:2008, ANY REFERENCES WHICH CITE THE ENTIRE INTERNATIONAL STANDARD ARE INTERPRETED AS EXCLUSIONS TO THIS DOCUMENT.
DLA TAILORED HIGHER LEVEL QUALITY CLAUSE FROM ISO 9001:2008

4.1 General requirements, [excluding reference to 1.2 and excluding NOTE 3 c)]
4.2.1 General, [excluding subparagraph a)]
4.2.2 Quality manual, [excluding subparagraph a)]
4.2.3 Control of documents
4.2.4 Control of records
5.1 Management commitment
5.3 Quality policy
6.2.2 Competence, training and awareness
6.4 Work environment
7.1 Planning of product realization, [excluding NOTE 2]
7.2.1 Determination of requirements related to the product
7.2.2 Review of requirements related to the product
7.2.3 Customer communication
7.3.7 Control of design and development changes
7.4.1 Purchasing process
7.4.3 Verification of purchased product
7.5.1 Control of production and service provision
7.5.3 Identification and traceability
7.5.4 Customer property
7.5.5 Preservation of product
7.6 Control of monitoring and measuring equipment
8.1 General, [excluding subparagraph b) and subparagraph c)]
8.2.2 Internal audit
8.2.4 Monitoring and measurement of product

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 4810-00-529-4083 CONT'D

8.3 Control of nonconforming product
8.5.2 Corrective action
8.5.3 Preventive action

NO DATA IS AVAILABLE. THE ALTERNATE OFFEROR IS REQUIRED TO PROVIDE A COMPLETE DATA PACKAGE INCLUDING DATA FOR THE APPROVED AND ALTERNATE PART FOR EVALUATION.

CLAUSE 52.246-15, CERTIFICATE OF CONFORMANCE, IS NOT AUTHORIZED FOR THIS NSN.

THIS IS AN AIR FORCE DESIGNATED CRITICAL SAFETY ITEM (CSI).
.
SOURCE INSPECTION REQUIRED
.
ALL REQUESTS FOR WAIVERS OR DEVIATIONS MUST BE FORWARDED TO THE DSC CONTRACTING OFFICER FOR REVIEW AND APPROVAL.
.
ALL ITEMS OF SUPPLY SHALL BE MARKED IAW MIL-STD-129. IN ADDITION, EACH UNIT PACK WILL BE MARKED WITH LOT AND SERIAL NUMBER (IF AVAILABLE), CONTRACTOR'S CAGE CODE, ACTUAL MANUFACTURER'S CAGE CODE AND PART NUMBER.

CRITICAL APPLICATION ITEM

HYDRO-AIRE, INC. DBA 81982 P/N 21899

Critical Safety Item

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	4810-00-529-4083 VALVE,DIRECTIONAL F	25.000	EA		

PRICING TERMS: Firm Fixed Price

QTY VARIANCE: PLUS 0% MINUS 0%

INSPECTION POINT: ORIGIN

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 4810-00-529-4083 CONT'D

ACCEPTANCE POINT: ORIGIN

FOB: ORIGIN DELIVERY DATE: 2017 JUN 02

PLACE of INSPECTION for PACKAGING:
9A289
DOUBLE J PACKAGING CO INC
9834 GLENOAKS BLVD
SUN VALLEY CA 91352-1046
USA

PREP FOR DELIVERY:

PKGING DATA - MIL-STD-2073-1D, 15 DEC 1999
QUP:001 PRES MTHD:41 CLNG/DRY:1 PRESV MAT:00
WRAP MAT:CA CUSH/DUNN MAT:BG CUSH/DUNN THKNESS:A
UNIT CONT:E5 OPI:M
INTRMDTE CONT:E5 INTRMDTE CONT QTY:012
PACK CODE:U
MARKING SHALL BE IN ACCORDANCE WITH MIL-STD-129.
SPECIAL MARKING CODE:ZZ -ZZ Special Requirements

PALLETIZATION SHALL BE IN ACCORDANCE WITH MD00100452 REV B DATED JULY 01, 2008

VALVE OPENINGS SHALL BE CLOSED WITH NONCORROSIVE
PLASTIC PLUGS OR END CAPS TO ENSURE NO DEBRIS
WILL CONTAMINATE VALVE FLOW WHEN IN OPERATION.

EACH UNIT PACKAGE WILL BE MARKED WITH THE NSN,
CONTRACT NUMBER, LOT NUMBER, CONTRACTOR CAGE
CODE, MANUFACTURER CAGE CODE, AND PART NUMBER.

PARCEL POST ADDRESS:

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

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

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 4810-00-529-4083 CONT'D

US

GOVT USE

ITEM	PR	PRLI	External PR	External PRLI	External Material	Customer RDD/ Need Ship Date
0001	0061276618	0001	N/A	N/A	N/A	N/A

****

CONTINUED ON NEXT PAGE

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.
(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).

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.
See Award
(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 Award
Issue By DoDAAC	See Award
Admin DoDAAC	See Award
Inspect By DoDAAC	See Award
Ship To Code	See Award
Ship From Code	See Award
Mark For Code	
Service Approver (DoDAAC)	

CONTINUED ON NEXT PAGE

Service Acceptor (DoDAAC)	
Accept at Other DoDAAC	
LPO DoDAAC	
DCAA Auditor DoDAAC	
Other DoDAAC(s)	

(*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.
No additional e-mail notifications are required.
(g) WAWF point of contact.
(1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.
Local Contract Administrator - See Page 1 of Award
(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.
(End of clause)

SECTION I - CONTRACT CLAUSES

252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (DEC 2015) DFARS

(a) *Definitions.* As used in this provision—
"Controlled technical information," "covered contractor information system," and "covered defense information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.
(b) The security requirements required by contract clause 252.204-7012, Covered Defense Information and Cyber Incident Reporting, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract.
(c) For covered contractor information systems that are not part of an information technology (IT) service or system operated on behalf of the Government (see 252.204-7012(b)(1)(ii))—
(1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171), not later than December 31, 2017.
(2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—
(A) Why a particular security requirement is not applicable; or
(B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
(ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.
(End of provision)

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

(a) *Definitions.* As used in this clause—
"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

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

252.247-7024 NOTIFICATION OF TRANSPORTATION OF SUPPLIES BY SEA (MAR 2000) DFARS

SECTION J - LIST OF ATTACHMENTS

List of Attachments

Description	File Name
ATTACH.SF33	SF33SPE7MC16R0072.pdf