REQUEST FOR QUOTATIONS

THIS RFQ ☐ IS ☒ IS NOT A SMALL BUSINESS SET-ASIDE

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT.FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG. 1	RATING
SPE7M1-27-Q-0130	2026 OCT 30	W25G1Q50720168		DX-A2

5. ISSUED BY

DLA WEAPONS SUPPORT
MARITIME SUPPLY CHAIN
PO BOX 3990
COLUMBUS OH 43218-3990
USA
Buyer: EDWARD ARAGON PMCM66W Tel: 6146930135
Email: EDWARD.ARAGON@DLA.MIL

6. DELIVER BY *(Date)*: 237 DAYS ADO

7. DELIVERY ☐ FOB DESTINATION ☒ OTHER *(See Schedule)*

8. TO:

9. DESTINATION

a. NAME OF CONSIGNEE: See Schedule

b. STREET ADDRESS

c. CITY

d. STATE | e. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5 ON OR BEFORE CLOSE OF BUSINESS *(Date)*

2026 NOV 10

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.

11. SCHEDULE *(See Continuation Sheets)*

See attached schedule to complete quote information.

Quoter must also complete the following:

a. Quotation is valid for 90 days from date specified in Block 10 above unless otherwise indicated: _____ .
b. Prices quoted are:
___ Contained in Commercial Catalog or Published Price List No. _____ dated _____ page _____ .
___ Contained in Internal Price List No. _____dated _____, which may be examined at our facility.
___ Commercial sales of comparable quantities: Quantity _____ ; Price _____;
___ Customer _____.
___ Other (provide basis) _____ _____ .
c. FOB Point: ____ Destination
____ Origin Shipping Point (City, State) _____ .
d. If delivery period shown in Block 6 is unacceptable, provide best possible delivery: _____.
e. Remittance Address (Name, Street, City, State, ZIP): Same as Block 13 unless otherwise indicated below:
_____ _____
_____ _____
_____ _____
_____ _____
f. Vendor FAX Number: _____ Vendor Toll-Free Number: _____ Vendor E-mail: _____

12. DISCOUNT FOR PROMPT PAYMENT	a. 10 CALENDAR DAYS *(%)*	b. 20 CALENDAR DAYS *(%)*	c. 30 CALENDAR DAYS *(%)*	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations ☒ are ☐ are not attached.

13. NAME AND ADDRESS OF QUOTER			14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION	15. DATE OF QUOTATION
a. NAME OF QUOTER	CAGE			
b. STREET ADDRESS			16. SIGNER	
			a. NAME *(Type or Print)*	b. TELEPHONE
c. COUNTY				AREA CODE
d. CITY	e. STATE	f. ZIP CODE	c. TITLE *(Type or Print)*	NUMBER

THE FOLLOWING CLASS DEVIATION SUPERSEDES ANY PRIOR VERSION OF DFARS CLAUSE 252.204-7012.

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (MAY 2024) (DEVIATION 2024-O0013 REVISION 1)
(a) Definitions. As used in this clause Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred. Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company. Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions. Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. Covered defense information means unclassified controlled technical information or other information, as described in the Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is
(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract. Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware. Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system. Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation. Rapidly report means within 72 hours of discovery of any cyber incident. Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical DataOther Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:
(1) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:
(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.
(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.
(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, Revision 2 (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf).
(ii)(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award. (B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place. If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract. (D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) (https://www.fedramp.gov/documents-templates/) and that the cloud service provider complies with requirements in paragraphs through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for

CONTINUED ON NEXT PAGE

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

Cyber incident reporting requirement.

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

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

(ii) Rapidly report cyber incidents to DoD at https://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 https://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 https://public.cyber.mil/eca/.

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

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 (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 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 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 . To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

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

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

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

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

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

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

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

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

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

(m) Subcontracts. The Contractor shall

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial products or commercial services, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to

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

CONTINUED ON NEXT PAGE

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

-End of Clause
**********;

EVALUATION FACTORS FOR AWARD
Award will be made to the offeror(s) whose quote(s) conforms to the solicitation requirements and represents the best value to the Government. Past performance, offered delivery, and price will be evaluated when making a comparative assessment of quotes. An award may be made to other than the lowest priced, technically acceptable, responsible offeror(s).
**********;

C20 Vendor Shipment Module (VSM) (JUN 2025)
**********;

Potential vendors must possess the appropriate security clearance as required by the DD 254 for this item, and as confirmed in the National Industrial Security System (NISS). Without the appropriate clearance, a vendor is NOT eligible for award on this item.

REQUIRED LEVEL: xxx

Any resultant purchase order contract will be DCMA Admin due to DD 254 requirement.

If an item has a DEMIL code requiring mutilation or destruction, then offers of surplus may need investigated to determine whether the items should not exist in the surplus market. DEMIL Code is annotated on the DD 254 Attachment.

Vendors quoting surplus must enter their certs into DIBBS with their quote, or send their certs and label copy to the buyer via email prior to the closing date of the solicitation in order to be considered.

All resultant awards shall be bilateral.

REQUIRED PROVISIONS/CLAUSES:
FAR 52.204-2 Security Requirements (MAR 2021)
DFARS 252.204-7000 Disclosure of Information (OCT 2016)
DFARS 252.226-7003 Drug-Free Work Force (AUG 2024)

BILATERAL CLAUSES
FAR 52.232-23 ASSIGNMENT OF CLAIMS (MAY 2014)
FAR 52.232-23 ALT I ASSIGNMENT OF CLAIMS, ALT I (APR 1984)
FAR 52.242-15 STOP WORK ORDER (AUG 1989)
FAR 52.243-1 CHANGES-FIXED-PRICE (AUG 1987)
DFAR 252.243-7001 PRICING OF CONTRACT MODIFICATION (DEC 1991)
FAR 52.249-1 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED PRICE) (SHORT FORM) (APR 1984)
FAR 52.249-8 DEFAULT (FIXED-PRICE SUPPLY AND SERVICE) (APR 1984)

**********;

DFARS 252.204-7016 Covered Defense Telecommunications Equipment or Services- Representation (DEC 2019)
DFARS 252.204-7017 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services-Representation (MAY 2021)
DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (JAN 2023)
52.240-91 Security Prohibitions and Exclusions (FEB 2026)
**********;

E05 Product Verification Testing (MAY 2020)
(1) Product verification testing (PVT) under this procurement note will only apply when the contracting officer specifically invokes it in writing. The contracting officer may invoke PVT at or after contract award. If the contracting officer invokes PVT at contract award, the contract will explicitly state this testing requirement. If the contracting officer invokes PVT after contract award, the contracting officer shall notify the contractor and the cognizant DCMA ACO. The Government will perform PVT testing at a Government-designated testing laboratory.
(2) The contractor shall not ship or deliver any material until it receives notification of the acceptable PVT results, unless the contracting officer directs it to do so in writing. The Government will provide the PVT results to the contractor within 20 business days after receipt at the Government testing facility, unless the Government specifies otherwise in writing.
(3) The contractor shall provide and maintain an inspection system acceptable to the Government in accordance with FAR Clause 52.246-2 or 52.246-3; and maintain and make available all records evidencing those details if requested by the Government. When the Government finds evidence of risk associated with the contractor's sampling process, the Government may witness and evaluate the contractors sampling process. The contractor shall randomly select samples from the production lot(s), unless the contracting officer specifies otherwise in writing. The contractor shall ship the selected PVT samples with a copy of the system of record receiving report (i.e., WAWF, DD Form 250, or commercial shipping document) and the contractor's signed DD Form 1222. The contractor shall prepare the shipping container(s) by marking the external packages in bold letters, Product Verification Test Samples Do Not Post to Stock," Contract Number: contractor insert and Lot/Item Number: contractor insert adjacent to the MIL-STD-129 (latest revision) identification markings. The contractor shall use a hard copy of the system of record receiving report as a packing list, in accordance with DFARS Appendix F. The contractor shall mark the exterior of the shipping container in accordance with MIL-STD- 129 (latest revision), paragraph 5.11. The contractor shall send samples by traceable means

CONTINUED ON NEXT PAGE

(e.g., certified or registered mail, United Parcel Service, Federal Express). The contractor shall include the following in the interior package:
(a) Hard copies of the contract;
(b) Material certifications/process operation sheets; and
(c) Drawings used to manufacture the units and return shipping information.
(4) The Government will return samples that pass testing and are not destroyed during evaluation to the contractor at the Government expense for the contractor to include as part of the total contract quantity to be delivered under the contract. The contractor and Government may agree to dispose of samples not destroyed when the cost of the item does not justify the shipping expense. If the Government does not return approved samples that pass testing to the contractor, the Government will consider those samples as part of the contract quantity for payment and delivery.
(5) If samples fail testing, the Government may reject the entire contract lot from which the contractor took the samples. The Government may, at its discretion, retain samples that fail testing without obligation to the contractor.
**********;

E07 Evaluation Factor for Origin Inspection
This solicitation contemplates an award based on destination inspection. If an offeror proposes inspection and acceptance at origin, the Government will add an evaluation factor of 2,500 to the offeror’s quoted/offered price for each origin inspection required. If phased deliveries are required or offered, the Government will consider each phase of delivery to result in one inspection for evaluation purposes.
**********;

Delivery shall be offered in terms of a number of days after date of award. There will be no penalty for faster delivery and partial deliveries are acceptable at no additional cost to the government.
**********;

Expedited or Partial Shipments will be accepted as long as there is no additional charge to the Government.
**********;

FAR 52.209-10 PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015);

This solicitation is issued under the First Destination Transportation (FDT) program to reduce the cost of transportation through the use of Government-arranged transportation utilizing Government contracts and rates. If this award is for FMS or has an APO/FPO ship-to address, these instructions do not apply.

For FDT Program Transportation Requirements, see Procurement Note C16 First Destination Transportation (FDT) Program, Government-Arranged Transportation for Manual Awards, C17 First Destination Transportation (FDT) Program Shipments Originating from Outside the Contiguous United States, and Procurement Note C20 Vendor Shipment Module (VSM).
**********;

THIS SOLICITATION INCORPORATES THE TERMS AND CONDITIONS SET FORTH IN THE REVISION OF THE DLA MASTER SOLICITATION FOR EPROCUREMENT AUTOMATED SIMPLIFIED ACQUISITIONS IN EFFECT ON THE SOLICITATION ISSUE DATE. ALL REVISIONS OF THE DLA MASTER SOLICITATION FOR EPROCUREMENT AUTOMATED SIMPLIFIED ACQUISITIONS CAN BE FOUND ON THE WEB AT: http://www.dla.mil/HQ/Acquisition/Offers/eProcurement.aspx
**********;

NORTH AMERICAN INDUSTRY CLASSIFICATION SYSTEM 334419 applies to this solicitation. See http://www.sba.gov/content/table-small-business-size-standards for the corresponding small business size standard.
**********;

PRODUCTION FACILITY CHANGES
UCF SECTION F
UCF SECTION F PRODUCTION FACILITY CHANGES
(a) The performance of any of the work contracted for in any place other than that named in the contract is prohibited unless specifically approved by the Contracting Officer. Written requests for a change in production facilities must be submitted in writing to the Contracting Officer. Changes in production facilities may be approved, provided:
(1) Performance by small business or in labor surplus areas as required by the contract will not be changed;
(2) The change will not cause a delay in delivery or necessitate a change in the purchase description;
(3) The free on board (f.o.b.) point is not changed; and
(4) Each request is supported by a price reduction of 250.00 to cover the Government administrative costs to process the change.
(b) The Government reserves the right to deny approval even if these four elements are met.
(End of Text)
****

****
****
****

CONTINUED ON NEXT PAGE

SECTION B

SUPPLIES/SERVICES: 5999-01-677-6476

ITEM DESCRIPTION:

ELECTRONICS COMPONE

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

RD003, COVERED DEFENSE INFORMATION POTENTIALLY APPLIES

RQ032: EXPORT CONTROL OF TECHNICAL DATA

This item has technical data some or all of which is subject to export-control of either the International Traffic in Arms regulations (ITAR) or the Export Administration Regulations (EAR), and cannot be exported without prior authorization from either the Department of State or the Department of Commerce. Export includes disclosure of technical data to foreign persons and nationals whether located in the United States or abroad. This requirement applies equally to foreign national employees and U.S. companies and their foreign subsidiaries. DFARS 252.225-7048 is applicable to this data.

The Defense Logistics Agency (DLA) limits distribution of export-control technical data to DLA contractors that have an approved US/Canada Joint Certification Program (JCP) certification, have completed the Introduction to Proper Handling of DOD Export-Controlled Technical Data Training and the DLA Export-Controlled Technical Data Questionnaire (both are available at the web address given below), and have been approved by the DLA controlling authority to access the export-controlled data. Instructions for obtaining access to the export-controlled data can be found at:
https://www.dla.mil/Logistics-Operations/Enhanced-Validation/

To be eligible for award, offerors and any sources of supply proposed for use are required to have an approved JCP certification and have been approved by the DLA controlling authority to access export-controlled data managed by DLA. DLA will not delay award in order for an offeror or its supplier to apply for and receive approval by the DLA controlling authority to access the export-controlled data.

A CONFIDENTIAL DOCUMENT IS INCLUDED IN THE
TECHNICAL DATA PACKAGE THAT SUPPORTS THIS
MATERIAL. CONTRACT AWARD FOR THIS ITEM IS
LIMITED TO THOSE CONTRACTORS THAT HAVE A
VALID AND CURRENT SECURITY CLASSIFICATION
LEVEL OF "CONFIDENTIAL" PRIOR TO AWARD. UPON
AWARD OF THE CONTRACT, THE CONTRACTING
OFFICER WILL ARRANGE FOR THE SECURE DISTRIBU-
TION OF THIS CONFIDENTIAL DOCUMENT THROUGH
THE DATA DISTRIBUTION OFFICE, DSCC-VPTC<(>,<)>
COLUMBUS, OHIO.
A CLASSIFIED DRAWING FORMS A PART OF THIS
DATA PACKAGE AND WILL BE SUPPLIED UPON
AWARD FOLLOWING RECEIPT OF
COMPLETED DD FORM 254 FROM
THE CONTRACTING OFFICER.

RD005: Cybersecurity Maturity Model Certification (CMMC) Level 2
Certified Third-Party Assessment Organization (C3PAO)
RD005: Cybersecurity Maturity Model Certification (CMMC) Level 2
Certified Third-Party Assessment Organization (C3PAO)
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

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 5999-01-677-6476 CONT'D

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

RQ011: REMOVAL OF GOVERNMENT IDENTIFICATION FROM NON-ACCEPTED SUPPLIES

RQ017: PHYSICAL IDENTIFICATION/BARE ITEM MARKING

NOTE: THIS IS A RESTRICTED SOURCE ITEM MANUFACTURED TO THE OEM DRAWING(S) CITED HEREIN AND AS OF THE DATE OF THIS SOLICITATION ONLY THE SOURCE(S) CITED BELOW HAS/HAVE BEEN PREQUALIFIED TO MANUFACTURE THE ITEM. OFFERS BASED ON SUPPLYING OTHER MANUFACTURER'S PARTS SHALL BE ACCOMPANIED BY TECHNICAL AND OTHER DATA SUFFICIENT TO EVALUATE THE ITEM FOR THE INTENDED APPLICATION AS PER DLAI 3200.1, ENCL 6. SAID EVALUATION MAY TAKE AN EXTENDED PERIOD OF TIME AND MAY THEREFORE BE APPLICABLE TO FUTURE PROCUREMENTS. FINAL APPROVAL AUTHORITY REST WITH THE GOVERNMENT DESIGN CONTROL ACTIVITY.

CRITICAL APPLICATION ITEM

NETWORKS INTERNATIONAL CORP 0BA69 P/N D-1023

TDP Rev A Gen 1
IAW REFERENCE DRAWING NR 18876 13647005
REVISION NR H DTD 08/09/2017
PART PIECE NUMBER:

TDP Rev A Gen 1
IAW REFERENCE DRAWING NR 18876 MIS-23260
REVISION NR E DTD 04/19/2018
PART PIECE NUMBER:

DLA issues this document using the DoD authorized unit of issue, please refer to the following URL to determine the corresponding ANSI X12 unit of issue.

https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.dla.mil%2FPortals%2F104%2FDocuments%2FDLMS%2FeApplications%2FLogDataAdmin%2FUnit_of_Issue_and_Purchase_Unit.xlsx&wdOrigin=BROWSELINK

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	5999-01-677-6476 ELECTRONICS COMPONENTS SET	1.000	EA	$ _____	$ _____

PRICING TERMS: Firm Fixed Price

QTY VARIANCE: PLUS 0% MINUS 0%

INSPECTION POINT: DESTINATION

ACCEPTANCE POINT: DESTINATION

FOB: ORIGIN DELIVERY DATE: 237 DAYS ADO

PREP FOR DELIVERY:

CONTINUED ON NEXT PAGE

SECTION B

SUPPLY/SERVICE: 5999-01-677-6476 CONT'D

PKGING DATA - MIL-STD-2073-1E
QUP:001 PRES MTHD:41 CLNG/DRY:1 PRESV MAT:00
WRAP MAT:00 CUSH/DUNN MAT:NA CUSH/DUNN THKNESS:C
UNIT CONT:D3 OPI:M
INTRMDTE CONT:E5 INTRMDTE CONT QTY:AAA
PACK CODE:U
MARKING SHALL BE IN ACCORDANCE WITH MIL-STD-129.
SPECIAL MARKING CODE:00 -00 No special marking

PALLETIZATION SHALL BE IN ACCORDANCE WITH RP001: DLA PACKAGING
 REQUIREMENTS FOR PROCUREMENT

BULK BREAK POINT:

W25G1Q

W0L6 USA DEP LETTERKENY
LETTERKENNY ARMY DEPOT
1 OVERCASH AVENUE BLDG 9950
CHAMBERSBURG PA 17201-4150
US

SHIP BY FASTEST TRACEABLE MEANS. DO NOT USE PARCEL POST.

FREIGHT SHIPPING ADDRESS:

W25G1Q

W0L6 USA DEP LETTERKENY
LETTERKENNY ARMY DEPOT
1 OVERCASH AVENUE BLDG 9950
CHAMBERSBURG PA 17201-4150
US

MARKFOR

W25G1Q

W0L6 USA DEP LETTERKENY
LETTERKENNY ARMY DEPOT
1 OVERCASH AVENUE BLDG 9950
CHAMBERSBURG PA 17201-4150
US

M/F: (TCN) W25G1Q50720168
RDD:
PROJ: TP 1
SUPP ADD: W25G1Q SIG: A

FOR GOVERNMENT USE ONLY: (IPD) 03

DIC: A0A DIST: ADV: FC: VF

GOVT USE

ITEM	PR	PRLI	External PR	External PRLI	External Material	Customer RDD/ Need Ship Date
0001	7017091788	0001	N/A	N/A	N/A	03/18/2025

* * * *

SECTION G - CONTRACT ADMINISTRATION DATA

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (PRE-FILLED) (JAN 2023) DFARS

As prescribed in 232.7004 (b), use the following clause:
(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.
Payment request and *receiving report* are defined in the clause at 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.
(b) *Electronic invoicing.* The WAWF system provides the method to electronically process vendor payment requests and receiving reports, as authorized by Defense Federal Acquisition Regulation System (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 System for Award Management at https://www.sam.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.
(f) *WAWF payment instructions.* The Contractor shall use the following information when submitting payment requests and receiving reports in WAWF for this contract or task or delivery order:
(1) *Document type.* The Contractor shall submit payment requests using the following document type(s):
(i) For cost-type line items, including labor-hour or time-and-materials, submit a cost voucher.
(ii) For fixed price line items -
(A) That require shipment of a deliverable, submit the invoice and receiving report specified by the Contracting Officer.
(Contracting Officer: Insert applicable invoice and receiving report document type(s) for fixed price line items that require shipment of a deliverable.)

Invoice (stand-alone) and Receiving Report (stand-alone) or Invoice and Receiving Report (combination)

(B) For services that do not require shipment of a deliverable, submit either the Invoice 2in1, which meets the requirements for the invoice and receiving report, or the applicable invoice and receiving report, as specified by the Contracting Officer.

(Contracting Officer: Insert either "Invoice 2in1" or the applicable invoice and receiving report document type(s) for fixed price line items for services.)
(iii) For customary progress payments based on costs incurred, submit a progress payment request.
(iv) For performance based payments, submit a performance based payment request.
(v) For commercial financing, submit a commercial financing request.
(2) Fast Pay requests are only permitted when Federal Acquisition Regulation (FAR) 52.213-1 is included in the contract.
[Note: The Contractor may use a WAWF "combo" document type to create some combinations of invoice and receiving report in one step.]
(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	Guidance
Pay Official DoDAAC	See Block 12 (SF26), 15 (DD 1155), or 18a (SF1449)	(If blank, see resulting award)
Issue By DoDAAC	See Block 5 (SF26), 6 (DD 1155), or 9 (SF1449)	(If blank, see resulting award)
Admin DoDAAC	See Block 6 (SF26), 7 (DD 1155), or 16 (SF1449)	(If blank, see resulting award)
Inspect By DoDAAC	SEE SECTION B	(If blank, see resulting award)
Ship To Code	SEE SECTION B	(If blank, see resulting award)
Ship From Code	SEE SECTION B	(If blank, see resulting award)
Mark For Code	SEE SECTION B	(If blank, see resulting award)
Service Approver (DoDAAC)		(If blank, see resulting award)

CONTINUED ON NEXT PAGE

SECTION G - CONTRACT ADMINISTRATION DATA (CONTINUED)

Field Name in WAWF	Data to be entered in WAWF	Guidance
Service Acceptor (DoDAAC)		(If blank, see resulting award)
Accept at Other DoDAAC		(If blank, see resulting award)
LPO DoDAAC		(If blank, see resulting award)
DCAA Auditor DoDAAC		(If blank, see resulting award)
Other DoDAAC(s)		(If blank, see resulting award)

(* Contracting Officer: Insert applicable DoDAAC information. If multiple ship to/acceptance locations apply, insert “See Schedule” or “Not applicable.”)
(** Contracting Officer: If the contract provides for progress payments or performance-based payments, insert the DoDAAC for the contract administration office assigned the functions under FAR 42.302(a)(13).)
(4) *Payment request.* The Contractor shall ensure a payment request includes documentation appropriate to the type of payment request in accordance with the payment clause, contract financing clause, or Federal Acquisition Regulation 52.216-7, Allowable Cost and Payment, as applicable.
(5) *Receiving report.* The Contractor shall ensure a receiving report meets the requirements of DFARS Appendix F.
(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.

See administer listed on page 1

(*Contracting Officer: Insert applicable information or “Not applicable.”*)
(2) Contact the WAWF helpdesk at 866-618-5988, if assistance is needed.

(End of Clause)

SECTION I - CONTRACT CLAUSES

52.222-37 EMPLOYMENT REPORTS ON VETERANS (DEVIATION 2026-O0038) (FEB 2026) FAR

52.223-23 SUSTAINABLE PRODUCTS (DEVIATION 2026-O0038) (FEB 2026) FAR

SECTION J - LIST OF ATTACHMENTS

List of Attachments

Description	File Name
ATTACH_DD_FORM_254 _Solicitation	DD254_Solicitation_.pdf

SECTION K - REPRESENTATIONS, CERTIFICATIONS AND STATEMENTS

52.219-31 NOTICE OF SMALL BUSINESS RESERVE (MAR 2020) FAR