SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE 1 OF 13

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
SPE3S1-17-D-Z126	2017 JUN 27			

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME

9. ISSUED BY CODE SPE3S1

DLA TROOP SUPPORT
SUBSISTENCE SUPPLY CHAIN
700 ROBBINS AVENUE
PHILADELPHIA PA 19111-5096
USA
Local Admin: Tiendung Nguyen PSPTRC4 Tel: 215-737-0825 Fax: 215-737-4115
Email: TIENDUNG.NGUYEN@DLA.MIL

10. THIS ACQUISITION IS

- [X] UNRESTRICTED OR [ ] SET ASIDE: _____ % FOR:
- [ ] SMALL BUSINESS
- [ ] HUBZONE SMALL BUSINESS
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] EDWOSB
- [ ] 8 (A)

NAICS: 311999
SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
[X] SEE SCHEDULE	Net 30 days	[ ]	RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE

SEE SCHEDULE

16. ADMINISTERED BY CODE SPE3S1

SEE BLOCK 9
Criticality: PAS: None

17a. CONTRACTOR/ OFFEROR CODE 7E931 FACILITY CODE

NEWVIEW OKLAHOMA, INC.
501 N DOUGLAS AVE
OKLAHOMA CITY OK 73106-5007
USA

TELEPHONE NO. 4056045188

18a. PAYMENT WILL BE MADE BY CODE SL4701

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

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED. [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Award sent EDI, Do not duplicate shipment				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$3,000,000.00

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED.

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED.

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

[ ] 29. AWARD OF CONTRACT: REF. _____ OFFER DATED 0000-00-00. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH, HEREIN IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
tiendung nguyen

30b. NAME AND TITLE OF SIGNER *(Type or Print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or Print)*	31c. DATE SIGNED
		Tiendung Nguyen TIENDUNG.NGUYEN@DLA.MIL PSPTRC4	2017 JUN 26

SCHEDULE OF SUPPLIES:

This contract is a tiered, three (3) year contract. The contract will be effective from June 27, 2017 date of award through 1,095 days.

Notes: Deliveries might fall outside of effective period.

See contract clauses 52.216-18, Ordering and 52.216-22, Indefinite Quantity for ordering and delivery periods.

Price is **FOB Origin** (Please call 1-800-456-5507 for shipping assistance)

NSN: 8970-01-434-3192
FOOD PACKET, SURVIVAL TYPE II, ABANDON SHIP 567 GM, IND, 3 DAY, CID A-A-20331.

	Estimated Quantity	Unit Price (Per Pouch)
Tier 1: Date of award through 365 days thereafter	**52,500**	**$4.90**
Tier 2: From date of 366 days through 730 days thereafter	**52,500**	**$5.00**
Tier 3: From date of 731 days through 1,095 days thereafter	**52,500**	**$5.10**

Minimum Contract (for the 3-Year period) Quantity: 52,500 pouches
Maximum Contract (for the 3-Year period) Quantity: 210,000 pouches

The Government is only obligated to purchase the total minimum quantity contract for the 3-Year period of this item.

All Delivery Orders issued will allow a minimum of 120 days lead-time for delivery.

Inspection and Acceptance points for this contract shall be **Origin** by the Army Veterinary Inspection (AVI)

ELECTRONIC INVOICING BY SUPPLIERS VIA IRAPT (FORMERLY WAWF):

All suppliers are required to process invoices electronically by using iRAPT. Suppliers must have at least two trained company representatives with access to iRAPT. Suppliers shall submit an “Invoice and Receiving Report Combo” document. A copy of the iRAPT Report and a Bill of Lading shall be provided to Tracy Depot foreach individual shipment. The iRAPT report and Bill of lading shall be presented by the truck driver or itmust be attached to the last pallet of a shipment. The iRAPT report is the only acceptable invoice and must becompletely in order to receive payment. This is a condition for contract award. Due to audit readiness, trucks arriving without proper packet shall be rejected.

iRAPT is a secure web based system for electronic invoicing, receipt, acceptance, and property transfer.

iRAPT allows government vendors to submit and track invoices and receipt/acceptance documents over the web and allows government personnel to process those invoices in a real-

time, paperless environment. It is also the only application that will be used to capture the Unique Identification (UID) of Tangible Items information.

iRapt is in accordance with the 2001 National Defense Authorization Act (DFARS 252.232-7003/252.232.7003

Electronic Submission of Payment Requests and Receiving Reports) which requires claims for payment under a

Department of Defense Contract to be submitted in electronic form. As of March 03, 2008, DOD has issued a final rule amending the Defense Federal Acquisition Regulation supplement (DFARS) to require use of the iRAPT formerly Wide Area Workflow as the only acceptable electronic system for submitting requests for payment (invoices and receiving reports) under DOD contracts. For access to the iRAPT formerly WAWF system, please go to the following website: https://wawf.eb.mil/.

iRAPT System Requirements

iRAPT is a free internet application. Contractors should refer to the “Machine

Setup” information on the iRAPT homepage, https://wawf.eb.mil

The minimum system requirements are:
#133 MHz or more Pentium microprocessor (or equivalent)
SVGA Color Monitor (minimum 256 color)
64 MB RAM (minimum)
Internet Access (broadband recommended)

CONTRACT CLAUSES:

52.212-4 -- Contract Terms and Conditions -- Commercial Items (Jan 2017)
http://farsite.hill.af.mil/vmfara.htm

52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Jan 2017)
http://farsite.hill.af.mil/vmfara.htm

52.211-16 -- VARIATION IN QUANTITY (APR 1984) FAR

(a) A variation in the quantity of any item called for by this contract will not be accepted unless the variation has been caused by conditions of loading, shipping, or packing, or allowances in manufacturing processes, and then only to the extent, if any, specified in paragraph (b) of this clause.

(b) The permissible variation shall be limited to:

____2%_____Percent increase [Contracting Officer insert percentage]

____0%_____ Percent decrease [Contracting Officer insert percentage]

This increase or decrease shall apply to each line item.

52.216-19 -- ORDER LIMITATIONS (OCT 1995) FAR

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than **250 pouches**, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor --

(1) Any order for a single item in excess of **210,000 pouches**
(2) Any order for a combination of items in excess **of the maximum quantity;** or

(3) A series of orders from the same ordering office within **2 calendar days** that together call for quantities exceeding the limitation in subparagraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within ___**2**__ days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

52.216-22 -- INDEFINITE QUANTITY (OCT 1995) FAR

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period;

provided, that the Contractor shall not be required to make any deliveries under this contract after _____12**0**_days_____ .

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

(a) The term "f.o.b. origin," as used in this clause, means free of expense to the Government delivered --

(1) On board the indicated type of conveyance of the carrier (or of the Government, if specified) at a designated point in the city, county, and State from which the shipment will be made and from which line-haul transportation service (as distinguished from switching, local drayage, or other terminal service) will begin;

(2) To, and placed on, the carrier's wharf (at shipside, within reach of the ship's loading tackle, when the shipping point is within a port area having water transportation service) or the carrier's freight station;

(3) To a U.S. Postal Service facility; or

(4) If stated in the solicitation, to any Government designated point located within the same city or commercial zone as the f.o.b. origin point specified in the contract (the Federal Motor Carrier Safety Administration prescribes commercial zones at Subpart B of 49 CFR part 372).

(b) The Contractor shall --

(1)

(i) Pack and mark the shipment to comply with contract specifications; or

(ii) In the absence of specifications, prepare the shipment in conformance with carrier requirements to protect the goods and to ensure assessment of the lowest applicable transportation charge;

(2)

(i) Order specified carrier equipment when requested by the Government; or

(ii) If not specified, order appropriate carrier equipment not in excess of capacity to accommodate shipment;

(3) Deliver the shipment in good order and condition to the carrier, and load, stow, trim, block, and/or brace carload or truckload shipment (when loaded by the Contractor) on or in the carrier's conveyance as required by carrier rules and regulations;

(4) Be responsible for any loss of and/or damage to the goods --

(i) Occurring before delivery to the carrier;

(ii) Resulting from improper packing and marking; or

(iii) Resulting from improper loading, stowing, trimming, blocking, and/or bracing of the shipment, if loaded by the Contractor on or in the carrier's conveyance;

(5) Complete the Government bill of lading supplied by the ordering agency or, when a Government bill of lading is not supplied, prepare a commercial bill of lading or other transportation receipt. The bill of lading shall show --

(i) A description of the shipment in terms of the governing freight classification or tariff (or Government rate tender) under which lowest freight rates are applicable;

(ii) The seals affixed to the conveyance with their serial numbers or other identification;

(iii) Lengths and capacities of cars or trucks ordered and furnished;

(iv) Other pertinent information required to effect prompt delivery to the consignee, including name, delivery address, postal address and ZIP code of consignee, routing, etc.;

(v) Special instructions or annotations requested by the ordering agency for commercial bills of lading; e.g., "This shipment is the property of, and the freight charges paid to the carrier(s) will be reimbursed by, the Government"; and

(vi) The signature of the carrier's agent and the date the shipment is received by the carrier; and

(6) Distribute the copies of the bill of lading, or other transportation receipts, as directed by the ordering agency.

(c) These Contractor responsibilities are specified for performance at the plant or plants at which the supplies are to be finally inspected and accepted, unless the facilities for shipment by carrier's equipment are not available at the Contractor's plant, in which case the responsibilities shall be performed f.o.b. the point or points in the same or nearest city where the specified carrier's facilities are available; subject, however, to the following qualifications:

(1) If the Contractor's shipping plant is located in the State of Alaska or Hawaii, the Contractor shall deliver the supplies listed for shipment outside Alaska or Hawaii to the port of loading in Alaska or Hawaii, respectively, as specified in the contract, at Contractor's expense, and to that extent the contract shall be "f.o.b. destination."

(2) Notwithstanding subparagraph (c)(1) of this clause, if the Contractor's shipping plant is located in the State of Hawaii, and the contract requires delivery to be made by container service, the Contractor shall deliver the supplies, at the Contractor's expense, to the container yard in the same or nearest city where seavan container service is available.

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) FAR

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

- FAR: http://farsite.hill.af.mil/vmfara.htm
- DFARS: http://farsite.hill.af.mil/vmfara.htm
- DLAD: http://farsite.hill.af.mil/vmfara.htm

CLAUSE NUMBER TITLE/DATE

52.232-17	Interest (MAY 2014) FAR
52.242-13	Bankruptcy (JUL 1995) FAR
52.242-15	Stop Work Order (AUG 1989) FAR
252.209-7004	Subcontracting with Firms that are Owned or Controlled by the Government of a Terrorist Country (OCT 2015) DFARS
52.225-1	Buy American--Supplies (May 2014) FAR
52.225-3	Buy American--Free Trade Agreements--Israeli Trade Act (May 2014)
252.225-7001	Buy American Act and Balance of Payments Program (Nov 2014) DFARS
252.225-7012	Preference for Certain Domestic Commodities (Dec 2016) DFARS

252.216-7006 – ORDERING (MAY 2011) DFARS

a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the contract schedule. Such orders may be issued from date of award through 3 years or 1095 days thereafter.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c)

(1) If issued electronically, the order is considered "issued" when a copy has been posted to the Electronic Document Access system, and notice has been sent to the Contractor.

(2) If mailed or transmitted by facsimile, a delivery order or task order is considered "issued" when the Government deposits the order in the mail or transmits by facsimile. Mailing includes transmittal by U.S. mail or private delivery services.

(3) Orders may be issued orally only if authorized in the schedule.

52.216-9008 OFFEROR'S QUANTITY LIMITATIONS (JUL 2006)

An offer may be restricted by completing the following section, however such conditional offers may not be acceptable. Stating no restriction, either below or elsewhere in the offer, is express authorization to accept award of the total quantity offered or any part thereof.

[ ] 100% of all items offered or none.

[x] Clearly describe other restrictions, if any, under which the offer is submitted.

(a) Delivery orders will specify delivery no less than _____**120**_____ days from the date of order. Changes or cancellations to delivery orders may be made by giving the Contractor notice no less than __**15**_ days [remembering that days are always calendar days unless otherwise defined] before the required delivery date.

(b) Maximum contract limitation. The maximum quantity or maximum dollar value that may be ordered against this contract is _____**210,000 pouches**_____. The Guaranteed Minimum of this contract is **52,500** pouches.

(c) Guaranteed minimum.

(1) The Government guarantees that it will order under this contract (and under the contract awarded for any partial set-aside) the following minimum, as applicable:

[x] Base period of two or more years.

_**52,500 pouches** _____ (Quantity) multiplied by ___1___.\

252.204-7008 COMPLIANCE WITH SAFEGUARDING COVERED DEFENSE INFORMATION CONTROLS (OCT 2016) DFARS (a) *Definitions*. As used in this provision— "Controlled technical information," "covered contractor information system," and "covered defense information" are defined in clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. (b) The security requirements required by contract clause 252.204-7012, Covered Defense Information and Cyber Incident Reporting, shall be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract. (c) For covered contractor information systems that are not part of an information technology (IT) service or system operated on behalf of the Government (see 252.204-7012(b)(1)(ii))— (1) By submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171), not later than December 31, 2017. (2)(i) If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of— (A) Why a particular security requirement is not applicable; or (B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection. (ii) An authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract. (End of provision) **252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016) DFARS** (a) *Definitions.* As used in this clause— "Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred. "Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions. "Covered defense information" means unclassified information that— (1) Is— (i) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (ii) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and (2) Falls in any of the following categories: (i) Controlled technical information. (ii) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process). (iii) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration PAGE 25 OF 29 PAGES CONTINUATION SHEET REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-5001 **CONTINUED ON NEXT PAGE** regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information. (iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law,

regulations, and Governmentwide policies (e.g., privacy, proprietary business information). “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. (b) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party’s reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause): (1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government’s activities related to clause 252.204-7012, and shall not be used for any other purpose. (2) The Contractor shall protect the information against unauthorized release or disclosure. (3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information. (4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause. (5) A breach of these obligations or restrictions may subject the Contractor to— (i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and (ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause. (c) *Subcontracts*. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government’s activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016) DFARS (a) *Definitions*. As used in this clause— “Adequate security” means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. “Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred. “Contractor attributional/proprietary information” means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company. “Contractor information system” means an information system belonging to, or operated by or for, the Contractor. “Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions. “Covered contractor information system” means an information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. “Covered defense information” means unclassified information that— (i) Is— (A) Provided to the contractor by or on behalf of DoD in connection with the performance of the contract; or (B) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract; and (ii) Falls in any of the following categories: (A) *Controlled technical information*. (B) *Critical information (operations security).* Specific facts identified through the Operations Security process about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan.
and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment (part of Operations Security process). (C) *Export control.* Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. To include dual use items; items identified in export administration regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information. (D) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information). “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. “Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data. “Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware. “Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which information is recorded, stored, or printed within an information system. ‘‘Operationally critical support’’ means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation. “Rapid(ly) report(ing)” means within 72 hours of discovery of any cyber incident. “Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code. (b) *Adequate security*. The Contractor shall provide adequate security for all covered defense information on all covered contractor information systems that support the performance of work under this contract. To provide adequate security, the Contractor shall— (1) Implement

information systems security protections on all covered contractor information systems including, at a minimum— (i) For covered contractor information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government— (A) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract; and (B) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract; or (ii) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1)(i) of this clause— (A) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the 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 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*.
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. (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— PAGE 28 OF 29 PAGES CONTINUATION SHEET REFERENCE NO. OF DOCUMENT BEING CONTINUED: SPE3S1-17-D-5001 (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. (