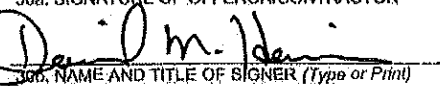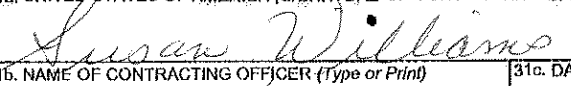| SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS *OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30*	1. REQUISITION NUMBER 1000054813	PAGE 1 OF 8

2. CONTRACT NO. SPE300-17-D-R870	3. AWARD/EFFECTIVE DATE 2017 APR 16	4. ORDER NUMBER	5. SOLICITATION NUMBER SPE300-17-X-0017	6. SOLICITATION ISSUE DATE 2017 MAR 02

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

9. ISSUED BY   CODE   SPE300

DLA TROOP SUPPORT
DIRECTORATE OF SUBSISTENCE
700 ROBBINS AVENUE
PHILADELPHIA PA 19111-5096
USA
Local Admin: Hweon Lee DHL0005 Tel: 215-737-4780
Email: Hweon.Lee@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   NAICS: 311991
[ ] 8 (A)   SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED [ ] SEE SCHEDULE	12. DISCOUNT TERMS Net 10 days	[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING 14. METHOD OF SOLICITATION [X] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE SEE SCHEDULE	16. ADMINISTERED BY CODE SPE300 SEE BLOCK 9 Criticality: PAS: None

17a. CONTRACTOR/ OFFEROR CODE 1TCF8 FACILITY CODE SYSCO MONTANA, INC. DBA SYSCO SYSCO MONTANA 1509 MONAD RD BILLINGS MT 59101-3229 USA TELEPHONE NO. 4062471157	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
	See Schedule				

25. ACCOUNTING AND APPROPRIATION DATA	26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* $150,000.00

[ ] 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   [ ] ARE   [X] 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	[X] 29. AWARD OF CONTRACT: REF. Sysco _____ OFFER DATED 2017-Mar-16 . 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)*
30b. NAME AND TITLE OF SIGNER *(Type or Print)* David Heinen Director of Program Sales	30c. DATE SIGNED 4/5/17	31b. NAME OF CONTRACTING OFFICER *(Type or Print)* Susan Williams	31c. DATE SIGNED 2017 APR 6

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE
32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE		32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
		32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	
38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY		

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	
		42b. RECEIVED AT *(Location)*
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

STANDARD FORM 1449 (REV. 2/2012) **BACK**

SOLICITATION/CONTRACT FORM
The terms and conditions set forth in solicitation SPE300-17-X-0017 are incorporated into subject contract SPE300-17-D-R870.

There is a change to the Contract Performance Period originally listed in solicitation SPE300-17-X-0017. It will now read:
I.   Contract Performance Period
Contract performance will range from April 16, 2017 to July 15, 2017. Contract will be established in FFAVORS Web by Saturday April 8, 2017. Customers will place orders beginning April 16, 2017 for delivery week beginning Sunday April 23, 2017. Prices for delivery week beginning approximately Sunday April 23, 2017 will be from the vendor's catalog prices determined fair and reasonable at time of award and will remain in effect for a 3-month period (90 days).

The following provisions/clauses do not apply and are hereby removed from this contract:
252.204-7009 LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016) DFARS
252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2015)
252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006) DFARS

EFFECTIVE PERIOD OF THE CONTRACT
This is an Indefinite Delivery Purchase Order (IDPO). The term of the contract will be until such time that a long term contract can be awarded and implemented. The maximum dollar value of this IDPO is $150,000.00. This IDPO will not exceed the maximum dollar value of $150,000.00.

ORDERING CATALOGS: The following conditions form a part of SYSCO Montana's offer and are hereby incorporated as part of subject contract.
The USDA School & Reservation customers are required to place orders no later than 10 days before delivery date.
Sysco Montana agrees to the proposed total fixed prices per unit for product delivered to DLA Troop Support's customers on an agreed upon basis.
Sysco Montana will hold the prices for a 3-month period.

FOB TERMS: FOB Destination for all items.

CATALOG#:
*Non-DoD reservation customers will order under SPE300-17-D-R870 throughout the length of the contract. SYSCO Montana will invoice in accordance with the customer's orders.

DELIVERIES AND PERFORMANCE:
The following is the designated plant location for the performance of this contract for all contract line items:
SYSCO Montana, Inc.
1509 Monad Road
Billings, MT 59101-3229

Part 12 Clauses

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 regulations, international traffic in arms regulations and munitions list; license applications; and sensitive nuclear technology information.
(iv) Any other information, marked or otherwise identified in the contract, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies (e.g., privacy, proprietary business information).

"Cyber incident" means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

(b) *Restrictions.* The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party's reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.
(2) The Contractor shall protect the information against unauthorized release or disclosure.
(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.
(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.
(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and
(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) *Subcontracts.* The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

(End of clause)

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016) DFARS

(a) *Definitions*. As used in this clause—

"Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

"Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

"Contractor attributional/proprietary information" means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

"Contractor information system" means an information system belonging to, or operated by or for, the Contractor.

"Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

"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*.

    (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.

(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)

52.216-19 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 $150.00, 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 $25,000.00   ;

(2) Any order for a combination of items in excess of $100,000.00 ; or

(3) A series of orders from the same ordering office within 7 days that together call for quantities exceeding the limitation in paragraph (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 1 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.

(End of clause)

252.232-7010 LEVIES ON CONTRACT PAYMENTS (DEC 2006) DFARS

Attachments

List of Attachments

Description	File Name
ATTACH.1	Attachment 1 RESERVATION - Schedule of