

**SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS**

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER

PAGE 1 OF 41

|                                                                                                                                                                                                                                                                                         |  |                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                 |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------------------------------------------------------------------------------------------------------|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|---------------------------------|--|------------|--|
| 2. CONTRACT NO.<br>[REDACTED]                                                                                                                                                                                                                                                           |  | 3. AWARD/EFFECTIVE DATE<br>01-Jul-2019                                                                                  |  | 4. ORDER NUMBER                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  | 5. SOLICITATION NUMBER<br>HTC71119RW002                                                                                         |  | 6. SOLICITATION ISSUE DATE<br>11-Jan-2019                                                                                                                                                        |  |                                 |  |            |  |
| 7. FOR SOLICITATION INFORMATION CALL:                                                                                                                                                                                                                                                   |  | a. NAME<br>ASHLEY BAKER                                                                                                 |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  | b. TELEPHONE NUMBER (No Collect Calls)<br>618-220-7109                                                                          |  | 8. OFFER DUE DATE/LOCAL TIME<br>03:00 PM 11 Feb 2019                                                                                                                                             |  |                                 |  |            |  |
| 9. ISSUED BY<br><br>USTRANSCOM-AQ - HTC711<br>508 SCOTT DR<br>SCOTT AFB IL 62225-5357<br><br>TEL: CONTACT BUYER<br>FAX: CONTACT BUYER                                                                                                                                                   |  | CODE<br>HTC711                                                                                                          |  | 10. THIS ACQUISITION IS<br><input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: _____ % FOR:<br><input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB)<br><input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM<br><input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> EDWOSB<br>NAICS: 488510<br>SIZE STANDARD: \$15,000,000<br>8(A) |  |                                                                                                                                 |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| 11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED<br><input type="checkbox"/> SEE SCHEDULE                                                                                                                                                                                        |  | 12. DISCOUNT TERMS<br>Net 30 Days                                                                                       |  | <input type="checkbox"/> 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  | 13b. RATING                                                                                                                     |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
|                                                                                                                                                                                                                                                                                         |  |                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  | 14. METHOD OF SOLICITATION<br><input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input checked="" type="checkbox"/> RFP |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| 15. DELIVER TO<br><br>SEE SCHEDULE                                                                                                                                                                                                                                                      |  | CODE                                                                                                                    |  | 16. ADMINISTERED BY<br><br>SEE ITEM 9                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |  |                                                                                                                                 |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| 17a. CONTRACTOR/OFFEROR<br>[REDACTED]<br>[REDACTED]<br>[REDACTED]<br>[REDACTED]<br>TELEPHONE NO. [REDACTED]                                                                                                                                                                             |  | CODE<br>[REDACTED]                                                                                                      |  | FACILITY CODE<br>[REDACTED]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |  | 18a. PAYMENT WILL BE MADE BY<br>HQ SDDC G8<br>1 SOLDIER WAY BLDG 1900W<br>SCOTT AFB IL 62225-5006                               |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| <input type="checkbox"/> 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 <input type="checkbox"/> 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)<br>\$ [REDACTED]                                                                                                                                     |  |                                 |  |            |  |
| <input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED                                                                        |  |                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                 |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| <input type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA <input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED                                                                                  |  |                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                 |  |                                                                                                                                                                                                  |  |                                 |  |            |  |
| <input type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 0 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. |  |                                                                                                                         |  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |  |                                                                                                                                 |  | <input type="checkbox"/> 29. AWARD OF CONTRACT: REF. OFFER DATED . 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<br>(TYPE OR PRINT)                                                                                                                                                                                                                                        |  |                                                                                                                         |  | 30c. DATE SIGNED                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |  | 31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)<br>[REDACTED]<br>TEL: [REDACTED]<br>EMAIL: [REDACTED]                          |  |                                                                                                                                                                                                  |  | 31c. DATE SIGNED<br>31-May-2019 |  |            |  |

**SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS  
(CONTINUED)**

PAGE 2 OF 41

| 19.<br>ITEM NO. | 20.<br>SCHEDULE OF SUPPLIES/ SERVICES | 21.<br>QUANTITY | 22.<br>UNIT | 23.<br>UNIT PRICE | 24.<br>AMOUNT |
|-----------------|---------------------------------------|-----------------|-------------|-------------------|---------------|
|                 | <b>SEE SCHEDULE</b>                   |                 |             |                   |               |

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 NUMBER

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

Section SF 1449 - CONTINUATION SHEET

| ITEM NO | SUPPLIES/SERVICES                                                                                                                                            | MAX<br>QUANTITY | UNIT   | UNIT PRICE     | MAX AMOUNT |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|----------------|------------|
| 0001    | Base Period<br>FFP<br>Multimodal Transportation Services<br>Period of Performance 1 July 2019-30 June 2021<br><br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 24              | Months |                |            |
|         |                                                                                                                                                              |                 |        | MAX<br>NET AMT |            |

| ITEM NO | SUPPLIES/SERVICES                                                                                                                                                                                                                                                                                                                                                                                                                        | MAX<br>QUANTITY | UNIT | UNIT PRICE     | MAX AMOUNT |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|------|----------------|------------|
| 0002    | Minimum Guarantee<br>FFP<br>This CLIN is to facilitate payment of the Contract Minimum Guarantee. Payment of Minimum Guarantee will be made via Delivery order if minimum is not met via ordering of transportation services. Once the contractor receives \$2,500 in shipments during the first year of performance, the minimum guarantee will be met and the funds will be deobligated.<br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 1               | Each |                |            |
|         |                                                                                                                                                                                                                                                                                                                                                                                                                                          |                 |      | MAX<br>NET AMT |            |

[REDACTED]

| ITEM NO                     | SUPPLIES/SERVICES                                                                                                                                                | MAX<br>QUANTITY | UNIT   | UNIT PRICE | MAX AMOUNT |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|------------|------------|
| 1001<br>EXERCISED<br>OPTION | Option Period 1<br>FFP<br>Multimodal Transportation Services<br>Period of Performance 1 July 2021-30 June 2023<br><br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 24              | Months | [REDACTED] | [REDACTED] |

---

MAX  
NET AMT

[REDACTED]

| ITEM NO                     | SUPPLIES/SERVICES                                                                                                                                                | MAX<br>QUANTITY | UNIT   | UNIT PRICE | MAX AMOUNT |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|------------|------------|
| 2001<br>EXERCISED<br>OPTION | Option Period 2<br>FFP<br>Multimodal Transportation Services<br>Period of Performance 1 July 2023-30 June 2025<br><br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 24              | Months | [REDACTED] | [REDACTED] |

---

MAX  
NET AMT

[REDACTED]

[REDACTED]

| ITEM NO        | SUPPLIES/SERVICES                                                                                                                                                | MAX<br>QUANTITY | UNIT   | UNIT PRICE     | MAX AMOUNT |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|----------------|------------|
| 3001<br>OPTION | Option Period 3<br>FFP<br>Multimodal Transportation Services<br>Period of Performance 1 July 2025-30 June 2027<br><br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 24              | Months | [REDACTED]     | [REDACTED] |
|                |                                                                                                                                                                  |                 |        | MAX<br>NET AMT | [REDACTED] |

| ITEM NO        | SUPPLIES/SERVICES                                                                                                                                                | MAX<br>QUANTITY | UNIT   | UNIT PRICE     | MAX AMOUNT |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--------|----------------|------------|
| 4001<br>OPTION | Option Period 4<br>FFP<br>Multimodal Transportation Services<br>Period of Performance 1 July 2027-30 June 2029<br><br>FOB: Destination<br>SIGNAL CODE: A<br>V111 | 24              | Months | [REDACTED]     | [REDACTED] |
|                |                                                                                                                                                                  |                 |        | MAX<br>NET AMT | [REDACTED] |

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

| CLIN | INSPECT AT  | INSPECT BY | ACCEPT AT   | ACCEPT BY  |
|------|-------------|------------|-------------|------------|
| 0001 | Destination | Government | Destination | Government |
| 0002 | Destination | Government | Destination | Government |
| 1001 | Destination | Government | Destination | Government |

|      |             |            |             |            |
|------|-------------|------------|-------------|------------|
| 2001 | Destination | Government | Destination | Government |
| 3001 | Destination | Government | Destination | Government |
| 4001 | Destination | Government | Destination | Government |

## DELIVERY INFORMATION

| CLIN | DELIVERY DATE                     | QUANTITY | SHIP TO ADDRESS         | DODAAC /<br>CAGE |
|------|-----------------------------------|----------|-------------------------|------------------|
| 0001 | POP 01-JUL-2019 TO<br>30-JUN-2021 | N/A      | N/A<br>FOB: Destination |                  |
| 0002 | POP 01-JUL-2019 TO<br>30-JUN-2020 | N/A      | N/A<br>FOB: Destination |                  |
| 1001 | POP 01-JUL-2021 TO<br>30-JUN-2023 | N/A      | N/A<br>FOB: Destination |                  |
| 2001 | POP 01-JUL-2023 TO<br>30-JUN-2025 | N/A      | N/A<br>FOB: Destination |                  |
| 3001 | POP 01-JUL-2025 TO<br>30-JUN-2027 | N/A      | N/A<br>FOB: Destination |                  |
| 4001 | POP 01-JUL-2027 TO<br>30-JUN-2029 | N/A      | N/A<br>FOB: Destination |                  |

## ADDITIONAL LANGUAGE

### **1. Recompensation**

**1.1** The Government will initially establish the awardee pool by competitively awarding multiple-award IDIQ contracts. As future task order requirements within the program ceiling totals materialize, over the life cycle of this program, the Government will compete those requirements amongst all existing IDIQ contract holders to determine if the contract holders can adequately fulfill the needed capability. The Government reserves the right to reopen the competition under this solicitation if there is shortfall in meeting the requirements among the existing IDIQ contract holders or if it is in the Government's best interest to add new contractors to the original pool of IDIQ contract holders. When/if the Government decides to reopen the solicitation, an announcement will be posted via FedBizOps allowing new CRAF/VISA offerors the opportunity to compete in a full and open competition for an IDIQ contract and task orders to meet the new requirements. Any existing IDIQ contract holder will not re-compete for an IDIQ contract. The competitions will use the same evaluation methodology and documentation (updated to reflect changes in regulatory provisions, requirements and certifications) as the original competition. Once a new awardee(s) is selected, that awardee(s) will be included in the awardee pool and will compete for future task orders. Subsequent to a reopened competition, initial and new IDIQ awardees can compete for future task orders. The ordering period for new contractors being added to the initial awardee pool will coincide with initial awardees ordering period, inclusive of options, but shall not extend the overall term of the contract beyond the original ordering period nor shall it reestablish the contract base period, inclusive of options.

### **2. Option Period**

**2.1** A sixty day preliminary notice will be given to the contractors informing it of the Government's intent to exercise the option. The Government may extend the term of the contract by written notice to the contractors no later

than thirty calendar days before the contract expires. Additionally, a contractor may request its option period not be exercised prior to the preliminary notification being issued under clause 52.217-9.

#### CLAUSES INCORPORATED BY REFERENCE

|                                |                                                                                                                          |          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------|
| 52.203-3                       | Gratuities                                                                                                               | APR 1984 |
| 52.203-6                       | Restrictions On Subcontractor Sales To The Government                                                                    | SEP 2006 |
| 52.203-6 Alt I                 | Restrictions On Subcontractor Sales To The Government (Sep 2006) -- Alternate I                                          | OCT 1995 |
| 52.204-10                      | Reporting Executive Compensation and First-Tier Subcontract Awards                                                       | OCT 2018 |
| 52.204-15                      | Service Contract Reporting Requirements for Indefinite-Delivery Contracts                                                | OCT 2016 |
| 52.204-18                      | Commercial and Government Entity Code Maintenance                                                                        | JUL 2016 |
| 52.204-21                      | Basic Safeguarding of Covered Contractor Information Systems                                                             | JUN 2016 |
| 52.209-6                       | Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment | OCT 2015 |
| 52.209-9                       | Updates of Publicly Available Information Regarding Responsibility Matters                                               | OCT 2018 |
| 52.209-10                      | Prohibition on Contracting With Inverted Domestic Corporations                                                           | NOV 2015 |
| 52.212-4                       | Contract Terms and Conditions--Commercial Items                                                                          | OCT 2018 |
| 52.219-9 (Dev)(Alt I, II, III) | Small Business Subcontracting Plan (DEVIATION 2016-O0009)                                                                | AUG 2016 |
| 52.219-16                      | Liquidated Damages-Subcontracting Plan                                                                                   | JAN 1999 |
| 52.222-3                       | Convict Labor                                                                                                            | JUN 2003 |
| 52.222-43                      | Fair Labor Standards Act And Service Contract Labor Standards - Price Adjustment (Multiple Year And Option Contracts)    | AUG 2018 |
| 52.225-13                      | Restrictions on Certain Foreign Purchases                                                                                | JUN 2008 |
| 52.228-3                       | Worker's Compensation Insurance (Defense Base Act)                                                                       | JUL 2014 |
| 52.232-29                      | Terms for Financing of Purchases of Commercial Items                                                                     | FEB 2002 |
| 52.232-33                      | Payment by Electronic Funds Transfer--System for Award Management                                                        | OCT 2018 |
| 52.232-40                      | Providing Accelerated Payments to Small Business Subcontractors                                                          | DEC 2013 |
| 52.233-3                       | Protest After Award                                                                                                      | AUG 1996 |
| 52.223-18                      | Encouraging Contractor Policies To Ban Text Messaging While Driving                                                      | AUG 2011 |
| 52.233-4                       | Applicable Law for Breach of Contract Claim                                                                              | OCT 2004 |
| 52.251-1                       | Government Supply Sources                                                                                                | APR 2012 |
| 52.242-5                       | Payments to Small Business Subcontractors                                                                                | JAN 2017 |
| 252.201-7000                   | Contracting Officer's Representative                                                                                     | DEC 1991 |
| 252.203-7000                   | Requirements Relating to Compensation of Former DoD Officials                                                            | SEP 2011 |
| 252.203-7002                   | Requirement to Inform Employees of Whistleblower Rights                                                                  | SEP 2013 |
| 252.203-7003                   | Agency Office of the Inspector General                                                                                   | DEC 2012 |
| 252.204-7012                   | Safeguarding Covered Defense Information and Cyber Incident Reporting                                                    | OCT 2016 |
| 252.204-7015                   | Notice of Authorized Disclosure of Information for Litigation Support                                                    | MAY 2016 |

|                    |                                                                                                                                             |          |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------|----------|
| 252.204-7018       | Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services                                                  | JAN 2021 |
| 252.205-7000       | Provision Of Information To Cooperative Agreement Holders                                                                                   | DEC 1991 |
| 252.216-7010       | Postaward Debriefings for Task Orders and Delivery Orders                                                                                   | MAR 2022 |
| 252.219-7003       | Small Business Subcontracting Plan (DOD Contracts)                                                                                          | APR 2018 |
| 252.222-7002       | Compliance With Local Labor Laws (Overseas)                                                                                                 | JUN 1997 |
| 252.225-7012       | Preference For Certain Domestic Commodities                                                                                                 | DEC 2017 |
| 252.225-7040       | Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States                                                        | OCT 2023 |
| 252.225-7048       | Export-Controlled Items                                                                                                                     | JUN 2013 |
| 252.225-7979 (Dev) | Additional Access to Contractor and Subcontractor Records in the United States Central Command Theater of Operations (DEVIATION 2018-O0008) | DEC 2017 |
| 252.225-7980 (Dev) | Contractor Personnel Performing in the United States Africa Command Area of Responsibility. (DEVIATION 2016-O0008)                          | JUN 2016 |
| 252.225-7981 (Dev) | Additional Access to Contractor and Subcontractor Records (Other than USCENTCOM) (DEVIATION 2015-O0016)                                     | SEP 2015 |
| 252.225-7993 (Dev) | Prohibition on Providing Funds to the Enemy (Deviation 2015-O0016)                                                                          | SEP 2015 |
| 252.225-7995 (Dev) | Contractor Personnel Performing in the United States Central Command Area of Responsibility (Deviation 2017-O0004)                          | SEP 2017 |
| 252.225-7997 (Dev) | Contractor Demobilization (Deviation 2013-O0017)                                                                                            | AUG 2013 |
| 252.226-7001       | Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns                      | SEP 2004 |
| 252.228-7003       | Capture and Detention                                                                                                                       | DEC 1991 |
| 252.229-7014       | Taxes--Foreign Contracts in Afghanistan                                                                                                     | DEC 2015 |
| 252.232-7003       | Electronic Submission of Payment Requests and Receiving Reports                                                                             | JUN 2012 |
| 252.232-7010       | Levies on Contract Payments                                                                                                                 | DEC 2006 |
| 252.237-7010       | Prohibition on Interrogation of Detainees by Contractor Personnel                                                                           | JUN 2013 |
| 252.243-7002       | Requests for Equitable Adjustment                                                                                                           | DEC 2012 |
| 252.244-7000       | Subcontracts for Commercial Items                                                                                                           | JUN 2013 |
| 252.247-7003       | Pass-Through of Motor Carrier Fuel Surcharge Adjustment To The Cost Bearer                                                                  | JUN 2013 |
| 252.247-7027       | Riding Gang Member Requirements                                                                                                             | MAY 2018 |
| 252.251-7000       | Ordering From Government Supply Sources                                                                                                     | AUG 2012 |

#### CLAUSES INCORPORATED BY FULL TEXT

#### 52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)


(a) Definitions. As used in this clause—

*Backhaul* means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

*Covered foreign country* means The People's Republic of China.

*Covered telecommunications equipment or services* means—



- 
- (1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
  - (2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
  - (3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
  - (4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

*Critical technology* means—

- (1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
- (2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-
  - (i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
  - (ii) For reasons relating to regional stability or surreptitious listening;
- (3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
- (4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
- (5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
- (6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

*Interconnection arrangements* means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

*Reasonable inquiry* means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

[REDACTED]

*Roaming* means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

*Substantial or essential component* means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

- (1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
- (2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at <https://dibnet.dod.mil>. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at <https://dibnet.dod.mil>.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

- (i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity

identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

#### 52.212-5

Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services (May 2024)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115-91).

(3) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).

(4) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015).

(5) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801).

(6) 52.233-3, Protest After Award (Aug 1996) (31 U.S.C. 3553).

(7) 52.233-4, Applicable Law for Breach of Contract Claim (Oct 2004) (Public Laws 108-77 and 108-78 ( 19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[Contracting Officer check as appropriate.]

(1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Jun 2020), with Alternate I (Nov 2021) (41 U.S.C. 4704 and 10 U.S.C. 4655).

  X   (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509)).

\_\_\_(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub. L. 111-5). (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009.)

\_\_\_(4) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712); this clause does not apply to contracts of DoD, NASA, the Coast Guard, or applicable elements of the intelligence community—see FAR 3.900(a).

\_\_\_(5) 52.204-10, Reporting Executive Compensation and First-Tier Subcontract Awards (Jun 2020) (Pub. L. 109-282) ( 31 U.S.C. 6101 note).

\_\_\_(6) [Reserved].

\_\_\_(7) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

\_\_\_(8) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (9) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328).

\_\_\_(10) 52.204-28, Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (Dec 2023) (Pub. L. 115–390, title II).

X (11) (i) 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (Dec 2023) (Pub. L. 115–390, title II).

\_\_\_(ii) Alternate I (Dec 2023) of 52.204-30.

\_\_\_(12) 52.209-6, Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment. (Nov 2021) (31 U.S.C. 6101 note).

\_\_\_(13) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

\_\_\_(14) [Reserved].

\_\_\_(15) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Oct 2022) (15 U.S.C. 657a).

\_\_\_\_(16) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2022) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

\_\_\_\_(17) [Reserved]

\_\_\_\_(18) (i) 52.219-6, Notice of Total Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

\_\_\_\_(ii) Alternate I (Mar 2020) of 52.219-6.

\_\_\_\_(19) (i) 52.219-7, Notice of Partial Small Business Set-Aside (Nov 2020) (15 U.S.C. 644).

\_\_\_\_(ii) Alternate I (Mar 2020) of 52.219-7.

X\_\_\_\_(20) 52.219-8, Utilization of Small Business Concerns (Feb 2024) (15 U.S.C. 637(d)(2) and (3)).

\_\_\_\_(21) (i) 52.219-9, Small Business Subcontracting Plan (Sep 2023) (15 U.S.C. 637(d)(4)).

\_\_\_\_(ii) Alternate I (Nov 2016) of 52.219-9.

\_\_\_\_(iii) Alternate II (Nov 2016) of 52.219-9.

\_\_\_\_(iv) Alternate III (Jun 2020) of 52.219-9.

\_\_\_\_(v) Alternate IV (Sep 2023) of 52.219-9.

\_\_\_\_(22) (i) 52.219-13, Notice of Set-Aside of Orders (Mar 2020) (15 U.S.C. 644(r)).

\_\_\_\_(ii) Alternate I (Mar 2020) of 52.219-13.

\_\_\_\_(23) 52.219-14, Limitations on Subcontracting (Oct 2022) (15 U.S.C. 637s).

\_\_\_\_(24) 52.219-16, Liquidated Damages—Subcontracting Plan (Sep 2021) (15 U.S.C. 637(d)(4)(F)(i)).

\_\_\_\_(25) 52.219-27, Notice of Set-Aside for, or Sole-Source Award to, Service-Disabled Veteran-Owned Small Business (SDVOSB) Concerns Eligible Under the SDVOSB Program (Feb 2024) (15 U.S.C. 657f).

\_\_\_\_(26) (i) 52.219-28, Post Award Small Business Program Rerepresentation (Feb 2024) (15 U.S.C. 632(a)(2)).

\_\_\_\_(ii) Alternate I (Mar 2020) of 52.219-28.

\_\_\_\_(27) 52.219-29, Notice of Set-Aside for, or Sole-Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Oct 2022) (15 U.S.C. 637(m)).

\_\_\_\_(28) 52.219-30, Notice of Set-Aside for, or Sole-Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Oct 2022) (15 U.S.C. 637(m)).

\_\_\_\_(29) 52.219-32, Orders Issued Directly Under Small Business Reserves (Mar 2020) (15 U.S.C. 644(r)).

\_\_\_\_(30) 52.219-33, Nonmanufacturer Rule (Sep 2021) (15U.S.C. 637(a)(17)).

\_\_\_\_(31) 52.222-3, Convict Labor (Jun 2003) (E.O.11755).

\_\_\_\_(32) 52.222-19, Child Labor-Cooperation with Authorities and Remedies (Feb 2024).

X (33) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

X (34) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O.11246).

\_\_\_\_(ii) Alternate I (Feb 1999) of 52.222-26.

X (35) (i) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).

\_\_\_\_(ii) Alternate I (Jul 2014) of 52.222-35.

X (36) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).

\_\_\_\_(ii) Alternate I (Jul 2014) of 52.222-36.

X (37) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).

X (38) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (39) (i) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O. 13627).

\_\_\_\_(ii) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

X (40) 52.222-54, Employment Eligibility Verification (May 2022) (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial products or commercial services as prescribed in FAR 22.1803.)

\_\_\_\_(41) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA–Designated Items (May 2008) ( 42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

\_\_\_\_(ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

\_\_\_\_(42) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (May 2024) (42 U.S.C. 7671, et seq.).

\_\_\_\_(43) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (May 2024) (42 U.S.C. 7671, et seq.).

\_\_\_\_(44) 52.223-20, Aerosols (May 2024) (42 U.S.C. 7671, et seq.).

\_\_\_\_(45) 52.223-21, Foams (May 2024) (42 U.S.C. 7671, et seq.).

\_\_\_\_(46) 52.223-23, Sustainable Products and Services (May 2024) (E.O. 14057, 7 U.S.C. 8102, 42 U.S.C. 6962, 42 U.S.C. 8259b, and 42 U.S.C. 7671).

\_\_\_\_(47) (i) 52.224-3 Privacy Training (Jan 2017) (5 U.S.C. 552 a).



\_\_\_\_(ii) Alternate I (Jan 2017) of [52.224-3](#).

\_\_\_\_(48) (i) [52.225-1](#), Buy American-Supplies (Oct 2022) ([41 U.S.C. chapter 83](#)).

\_\_\_\_(ii) Alternate I (Oct 2022) of [52.225-1](#).

\_\_\_\_(49) (i) [52.225-3](#), Buy American-Free Trade Agreements-Israeli Trade Act (NOV 2023) ([19 U.S.C. 3301 note](#), [19 U.S.C. 2112 note](#), [19 U.S.C. 3805 note](#), [19 U.S.C. 4001 note](#), 19 U.S.C. chapter 29 (sections 4501-4732), Public Law 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

\_\_\_\_(ii) Alternate I [Reserved].

\_\_\_\_(iii) Alternate II (Dec 2022) of [52.225-3](#).

\_\_\_\_(iv) Alternate III (Feb 2024) of [52.225-3](#).

\_\_\_\_(v) Alternate IV (Oct 2022) of [52.225-3](#).

\_\_\_\_(50) [52.225-5](#), Trade Agreements (NOV 2023) ([19 U.S.C. 2501](#), et seq., [19 U.S.C. 3301 note](#)).

\_\_\_\_(51) [52.225-13](#), Restrictions on Certain Foreign Purchases (Feb 2021) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

\_\_\_\_(52) [52.225-26](#), Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

\_\_\_\_(53) [52.226-4](#), Notice of Disaster or Emergency Area Set-Aside (Nov 2007) ([42 U.S.C. 5150](#)).

\_\_\_\_(54) [52.226-5](#), Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) ([42 U.S.C. 5150](#)).

(55) [52.226-8](#), Encouraging Contractor Policies to Ban Text Messaging While Driving (May 2024) ([E.O. 13513](#)).

\_\_\_\_(56) 52.229-12, Tax on Certain Foreign Procurements (Feb 2021).

\_\_\_\_(57) 52.232-29, Terms for Financing of Purchases of Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

\_\_\_\_(58) 52.232-30, Installment Payments for Commercial Products and Commercial Services (Nov 2021) (41 U.S.C. 4505, 10 U.S.C. 3805).

\_\_\_\_(59) 52.232-33, Payment by Electronic Funds Transfer-System for Award Management (Oct2018) (31 U.S.C. 3332).

\_\_\_\_(60) 52.232-34, Payment by Electronic Funds Transfer-Other than System for Award Management (Jul 2013) (31 U.S.C. 3332).

\_\_\_\_(61) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

\_\_\_\_(62) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

\_\_\_\_(63) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).

X (64) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631).

\_\_\_\_(ii) Alternate I (Apr 2003) of 52.247-64.

\_\_\_\_(iii) Alternate II (Nov 2021) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial products and commercial services:

[Contracting Officer check as appropriate.]

X (1) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter67).

\_\_\_\_(2) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

\_\_\_\_(3) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment

(Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(4) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards-Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(5) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(6) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

X (7) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).

X (8) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).

(9) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792).

(d) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, as defined in FAR 2.101, on the date of award of this contract, and does not contain the clause at 52.215-2, Audit and Records-Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1), in a subcontract for commercial products or commercial services. Unless otherwise indicated

below, the extent of the flow down shall be as required by the clause-

- (i) 52.203-13, Contractor Code of Business Ethics and Conduct (Nov 2021) (41 U.S.C. 3509).
- (ii) 52.203-17, Contractor Employee Whistleblower Rights (Nov 2023) (41 U.S.C. 4712).
- (iii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (iv) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab Covered Entities (Dec 2023) (Section 1634 of Pub. L. 115-91).
- (v) 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Nov 2021) (Section 889(a)(1)(A) of Pub. L. 115-232).
- (vi) 52.204-27, Prohibition on a ByteDance Covered Application (Jun 2023) (Section 102 of Division R of Pub. L. 117-328).
- (vii)
  - (A) 52.204–30, Federal Acquisition Supply Chain Security Act Orders—Prohibition. (Dec 2023) (Pub. L. 115–390, title II).
  - (B) Alternate I (Dec 2023) of 52.204–30.
- (viii) 52.219-8, Utilization of Small Business Concerns (Feb 2024) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds the applicable threshold specified in FAR 19.702(a) on the date of subcontract award, the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.
- (ix) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- (x) 52.222-26, Equal Opportunity (Sep 2015) (E.O.11246).
- (xi) 52.222-35, Equal Opportunity for Veterans (Jun 2020) (38 U.S.C. 4212).
- (xii) 52.222-36, Equal Opportunity for Workers with Disabilities (Jun 2020) (29 U.S.C. 793).
- (xiii) 52.222-37, Employment Reports on Veterans (Jun 2020) (38 U.S.C. 4212).
- (xiv) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.
- (xv) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
- (xvi)
  - (A) 52.222-50, Combating Trafficking in Persons (Nov 2021) (22 U.S.C. chapter 78 and E.O 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 and E.O. 13627).

(xvii) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements (May 2014) (41 U.S.C. chapter 67).

(xviii) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Requirements (May 2014) (41 U.S.C. chapter 67).

(xix) 52.222-54, Employment Eligibility Verification (May 2022) (E.O. 12989).

(xx) 52.222-55, Minimum Wages for Contractor Workers Under Executive Order 14026 (Jan 2022).

(xxi) 52.222-62, Paid Sick Leave Under Executive Order 13706 (Jan 2022) (E.O. 13706).

(xxii)

(A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xxiii) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. Subtitle A, Part V, Subpart G Note).

(xxiv) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations (Jun 2020) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxv) 52.232-40, Providing Accelerated Payments to Small Business Subcontractors (Mar 2023) (31 U.S.C. 3903 and 10 U.S.C. 3801). Flow down required in accordance with paragraph (c) of 52.232-40.

(xxvi) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Nov 2021) (46 U.S.C. 55305 and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial products and commercial services a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

## CLAUSES INCORPORATED BY FULL TEXT

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

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than 1 Port Call File Number (PCFN) 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 200 PCFNs;

(2) Any order for a combination of items in excess of 200 PCFNs; 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 24 hours 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)

#### 52.216-22 INDEFINITE QUANTITY. (OCT 1995)

(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 14 calendar days after contract expiration. If the contractor is in possession of any cargo after 14 calendar days following contract expiration, the contractor shall return the cargo to the consignor.

(End of clause)

#### 52.216-32 TASK-ORDER AND DELIVERY-ORDER OMBUDSMAN (SEPT 2019)

(a) In accordance with 41 U.S.C. 4106(g), the Agency has designated the following task-order and delivery-order Ombudsman for this contract. The Ombudsman must review complaints from the Contractor concerning all task-order and delivery-order actions for this contract and ensure the Contractor is afforded a fair opportunity for consideration in the award of orders, consistent with the procedures in the contract.

Chief, Business Support and Policy Division  
Email: transcom.scott.tcaq.mbx.ombudsman@mail.mil  
Telephone Number: 618-220-5434 FAX: 618-220-6248

(b) Consulting an ombudsman does not alter or postpone the timeline for any other process (e.g., protests).

(c) Before consulting with the Ombudsman, the Contractor is encouraged to first address complaints with the Contracting Officer for resolution. When requested by the Contractor, the Ombudsman may keep the identity of the concerned party or entity confidential, unless prohibited by law or agency procedure.

(End of clause)

#### 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within **30 calendar days of contract expiration**.

(End of clause)

#### 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 calendar days of contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 10 years and 6 months.

(End of clause)

#### 52.219-28 POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (JULY 2013)

(a) Definitions. As used in this clause--

Long-term contract means a contract of more than five years in duration, including options. However, the term does not include contracts that exceed five years in duration because the period of performance has been extended for a cumulative period not to exceed six months under the clause at 52.217-8, Option to Extend Services, or other appropriate authority.

Small business concern means a concern, including its affiliates, that is independently owned and operated, not dominant in the field of operation in which it is bidding on Government contracts, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (c) of this clause. Such a concern is "not dominant in its field of operation" when it does not exercise a controlling or major influence on a national basis in a kind of business activity in which a number of business concerns are primarily engaged. In determining whether dominance exists, consideration shall be given to all appropriate factors, including volume of business, number of employees, financial resources, competitive status or position, ownership or control of materials, processes, patents, license agreements, facilities, sales territory, and nature of business activity.

(b) If the Contractor represented that it was a small business concern prior to award of this contract, the Contractor shall rerepresent its size status according to paragraph (e) of this clause or, if applicable, paragraph (g) of this clause, upon the occurrence of any of the following:

(1) Within 30 days after execution of a novation agreement or within 30 days after modification of the contract to include this clause, if the novation agreement was executed prior to inclusion of this clause in the contract.

(2) Within 30 days after a merger or acquisition that does not require a novation or within 30 days after modification of the contract to include this clause, if the merger or acquisition occurred prior to inclusion of this clause in the contract.

(3) For long-term contracts--

(i) Within 60 to 120 days prior to the end of the fifth year of the contract; and

(ii) Within 60 to 120 days prior to the date specified in the contract for exercising any option thereafter.

(c) The Contractor shall rerepresent its size status in accordance with the size standard in effect at the time of this rerepresentation that corresponds to the North American Industry Classification System (NAICS) code assigned to this contract. The small business size standard corresponding to this NAICS code can be found at <http://www.sba.gov/content/table-small-business-size-standards>.

(d) The small business size standard for a Contractor providing a product which it does not manufacture itself, for a contract other than a construction or service contract, is 500 employees.

(e) Except as provided in paragraph (g) of this clause, the Contractor shall make the representation required by paragraph (b) of this clause by validating or updating all its representations in the Representations and Certifications section of the System for Award Management (SAM) and its other data in SAM, as necessary, to ensure that they reflect the Contractor's current status. The

Contractor shall notify the contracting office in writing within the timeframes specified in paragraph (b) of this clause that the data have been validated or updated, and provide the date of the validation or update.

(f) If the Contractor represented that it was other than a small business concern prior to award of this contract, the Contractor may, but is not required to, take the actions required by paragraphs (e) or (g) of this clause.

(g) If the Contractor does not have representations and certifications in SAM, or does not have a representation in SAM for the NAICS code applicable to this contract, the Contractor is required to complete the following rerepresentation and submit it to the contracting office, along with the contract number and the date on which the rerepresentation was completed:

The Contractor represents that it ( ) is, ( ) is not a small business concern under NAICS Code - assigned to contract number .

(Contractor to sign and date and insert authorized signer's name and title).



(End of clause)

#### 52.222-42 STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES (MAY 2014)

In compliance with the Service Contract Labor Standards statute and the regulations of the Secretary of Labor (29 CFR part 4), this clause identifies the classes of service employees expected to be employed under the contract and states the wages and fringe benefits payable to each if they were employed by the contracting agency subject to the provisions of 5 U.S.C. 5341 or 5332.

THIS STATEMENT IS FOR INFORMATION ONLY: IT IS NOT A WAGE DETERMINATION

Employee Class Monetary Wage-Fringe Benefits

| Employee Class                                   | Monetary Wage – Fringe Benefits |
|--------------------------------------------------|---------------------------------|
| Forklift Operator                                | WG-5                            |
| Blocker & Bracer                                 | WG-8                            |
| Line Handler                                     | WG-8                            |
| Stevedore I                                      | WG-7                            |
| Stevedore II                                     | WG-9                            |
| Truck Driver, Light                              | WG-6                            |
| Truck Driver, Medium                             | WG-7                            |
| Truck Driver, Heavy                              | WG-8                            |
| Truck Driver, Tractor-Trailer                    | WG-8                            |
| General Schedule: First Pilot                    | GS-11 Step 1/\$29.33 per hour   |
| General Schedule: Co-Pilot                       | GS-10 Step 1/\$26.70 per hour   |
| General Schedule: Flight Dispatcher              | GS-07 Step 1/\$19.82 per hour   |
| General Schedule: Second Officer/Flight Engineer | GS-09 Step 1/\$24.24 per hour   |

The fringe benefit for all classifications is 36.25% of the wage rate.

(End of clause)

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

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):

<https://www.acquisition.gov/>

(End of clause)

#### 52.222-50 COMBATING TRAFFICKING IN PERSONS (MAR 2015) ALTERNATE I (MAR 2015)

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

“Agent” means any individual, including a director, an officer, an employee, or an independent contractor, authorized to act on behalf of the organization.

“Coercion” means—

- (1) Threats of serious harm to or physical restraint against any person;
- (2) Any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or
- (3) The abuse or threatened abuse of the legal process.

“Commercial sex act” means any sex act on account of which anything of value is given to or received by any person.

“Commercially available off-the-shelf (COTS) item” means--

- (1) Any item of supply (including construction material) that is—
  - (i) A commercial item (as defined in paragraph (1) of the definition at FAR 2.101);
  - (ii) Sold in substantial quantities in the commercial marketplace; and
  - (iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and
- (2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

“Debt bondage” means the status or condition of a debtor arising from a pledge by the debtor of his or her personal services or of those of a person under his or her control as a security for debt, if the value of those services as reasonably assessed is not applied toward the liquidation of the debt or the length and nature of those services are not respectively limited and defined.

“Employee” means an employee of the Contractor directly engaged in the performance of work under the contract who has other than a minimal impact or involvement in contract performance.

“Forced labor” means knowingly providing or obtaining the labor or services of a person—

- (1) By threats of serious harm to, or physical restraint against, that person or another person;
- (2) By means of any scheme, plan, or pattern intended to cause the person to believe that, if the person did not perform such labor or services, that person or another person would suffer serious harm or physical restraint; or
- (3) By means of the abuse or threatened abuse of law or the legal process.

“Involuntary servitude” includes a condition of servitude induced by means of—

- (1) Any scheme, plan, or pattern intended to cause a person to believe that, if the person did not enter into or continue in such conditions, that person or another person would suffer serious harm or physical restraint; or
- (2) The abuse or threatened abuse of the legal process.

“Severe forms of trafficking in persons” means—

(1) Sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such act has not attained 18 years of age; or

(2) The recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

“Sex trafficking” means the recruitment, harboring, transportation, provision, or obtaining of a person for the purpose of a commercial sex act.

“Subcontract” means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.

“Subcontractor” means any supplier, distributor, vendor, or firm that furnishes supplies or services to or for a prime contractor or another subcontractor.

“United States” means the 50 States, the District of Columbia, and outlying areas.

(b) *Policy.* The United States Government has adopted a policy prohibiting trafficking in persons including the trafficking-related activities of this clause. Contractors, contractor employees, and their agents shall not—

(1) Engage in severe forms of trafficking in persons during the period of performance of the contract;

(2) Procure commercial sex acts during the period of performance of the contract;

(3) Use forced labor in the performance of the contract;

(4) Destroy, conceal, confiscate, or otherwise deny access by an employee to the employee's identity or immigration documents, such as passports or drivers' licenses, regardless of issuing authority;

(5)(i) Use misleading or fraudulent practices during the recruitment of employees or offering of employment, such as failing to disclose, in a format and language accessible to the worker, basic information or making material misrepresentations during the recruitment of employees regarding the key terms and conditions of employment, including wages and fringe benefits, the location of work, the living conditions, housing and associated costs (if employer or agent provided or arranged), any significant cost to be charged to the employee, and, if applicable, the hazardous nature of the work;

(ii) Use recruiters that do not comply with local labor laws of the country in which the recruiting takes place;

(6) Charge employees recruitment fees;

(7)(i) Fail to provide return transportation or pay for the cost of return transportation upon the end of employment--

(A) For an employee who is not a national of the country in which the work is taking place and who was brought into that country for the purpose of working on a U.S. Government contract or subcontract (for portions of contracts performed outside the United States); or

(B) For an employee who is not a United States national and who was brought into the United States for the purpose of working on a U.S. Government contract or subcontract, if the payment of such costs is required under existing temporary worker programs or pursuant to a written agreement with the employee (for portions of contracts performed inside the United States); except that--

(ii) The requirements of paragraphs (b)(7)(i) of this clause shall not apply to an employee who is--

(A) Legally permitted to remain in the country of employment and who chooses to do so; or

(B) Exempted by an authorized official of the contracting agency from the requirement to provide return transportation or pay for the cost of return transportation;

(iii) The requirements of paragraph (b)(7)(i) of this clause are modified for a victim of trafficking in persons who is seeking victim services or legal redress in the country of employment, or for a witness in an enforcement action related to trafficking in persons. The contractor shall provide the return transportation or pay the cost of return transportation in a way that does not obstruct the victim services, legal redress, or witness activity. For example, the contractor shall not only offer return transportation to a witness at a time when the witness is still needed to testify. This paragraph does not apply when the exemptions at paragraph (b)(7)(ii) of this clause apply.

(8) Provide or arrange housing that fails to meet the host country housing and safety standards; or

(9) If required by law or contract, fail to provide an employment contract, recruitment agreement, or other required work document in writing. Such written work document shall be in a language the employee understands. If the employee must relocate to perform the work, the work document shall be provided to the employee at least five days prior to the employee relocating. The employee's work document shall include, but is not limited to, details about work description, wages, prohibition on charging recruitment fees, work location(s), living accommodations and associated costs, time off, roundtrip transportation arrangements, grievance process, and the content of applicable laws and regulations that prohibit trafficking in persons.

(c) *Contractor requirements.* The Contractor shall—

(1) Notify its employees of—

(i) (A) The United States Government's policy prohibiting trafficking in persons described in paragraph (b) of this clause; and

(B) The following directive(s) or notice(s) applicable to employees performing work at the contract place(s) of performance as indicated below:

| Document Title | Document may be obtained from: | Applies to performance in/at: |
|----------------|--------------------------------|-------------------------------|
| _____          | _____                          | _____                         |
| _____          | _____                          | _____                         |
| _____          | _____                          | _____                         |

[ \_\_\_\_ Contracting Officer shall insert title of directive/notice; indicate the document is attached or provide source (such as website link) for obtaining document; and, indicate the contract performance location outside the United States to which the document applies.]

(ii) The actions that will be taken against employees or agents for violations of this policy. Such actions for employees may include, but are not limited to, removal from the contract, reduction in benefits, or termination of employment; and

(2) Take appropriate action, up to and including termination, against employees, agents, or subcontractors that violate the policy in paragraph (b) of this clause.

(d) *Notification.* (1) The Contractor shall inform the Contracting Officer and the agency Inspector General immediately of—

(i) Any credible information it receives from any source (including host country law enforcement) that alleges a Contractor employee, subcontractor, subcontractor employee, or their agent has engaged in conduct that violates the policy in paragraph (b) of this clause (see also 18 U.S.C. 1351, Fraud in Foreign Labor Contracting, and 52.203-13(b)(3)(i)(A), if that clause is included in the solicitation or contract, which requires disclosure to the agency Office of the Inspector General when the Contractor has credible evidence of fraud); and

(ii) Any actions taken against a Contractor employee, subcontractor, subcontractor employee, or their agent pursuant to this clause.

(2) If the allegation may be associated with more than one contract, the Contractor shall inform the contracting officer for the contract with the highest dollar value.

(e) *Remedies.* In addition to other remedies available to the Government, the Contractor's failure to comply with the requirements of paragraphs (c), (d), (g), (h), or (i) of this clause may result in—

(1) Requiring the Contractor to remove a Contractor employee or employees from the performance of the contract;

(2) Requiring the Contractor to terminate a subcontract;

(3) Suspension of contract payments until the Contractor has taken appropriate remedial action;

(4) Loss of award fee, consistent with the award fee plan, for the performance period in which the Government determined Contractor non-compliance;

(5) Declining to exercise available options under the contract;

(6) Termination of the contract for default or cause, in accordance with the termination clause of this contract; or

(7) Suspension or debarment.

(f) *Mitigating and aggravating factors.* When determining remedies, the Contracting Officer may consider the following:

(1) *Mitigating factors.* The Contractor had a Trafficking in Persons compliance plan or an awareness program at the time of the violation, was in compliance with the plan, and has taken appropriate remedial actions for the violation, that may include reparation to victims for such violations.

(2) *Aggravating factors.* The Contractor failed to abate an alleged violation or enforce the requirements of a compliance plan, when directed by the Contracting Officer to do so.

(g) *Full cooperation.*

(1) The Contractor shall, at a minimum—

(i) Disclose to the agency Inspector General information sufficient to identify the nature and extent of an offense and the individuals responsible for the conduct;

(ii) Provide timely and complete responses to Government auditors' and investigators' requests for documents;

(iii) Cooperate fully in providing reasonable access to its facilities and staff (both inside and outside the U.S.) to allow contracting agencies and other responsible Federal agencies to conduct audits, investigations, or other actions to ascertain compliance with the Trafficking Victims Protection Act of 2000 (22 U.S.C. chapter 78), E.O. 13627, or any other applicable law or regulation establishing restrictions on trafficking in persons, the procurement of commercial sex acts, or the use of forced labor; and

(iv) Protect all employees suspected of being victims of or witnesses to prohibited activities, prior to returning to the country from which the employee was recruited, and shall not prevent or hinder the ability of these employees from cooperating fully with Government authorities.

(2) The requirement for full cooperation does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not—

(i) Require the Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine;

(ii) Require any officer, director, owner, employee, or agent of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; or

(iii) Restrict the Contractor from—

(A) Conducting an internal investigation; or

(B) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.

(h) *Compliance plan.*

(1) This paragraph (h) applies to any portion of the contract that—

(i) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and

(ii) Has an estimated value that exceeds \$500,000.

(2) The Contractor shall maintain a compliance plan during the performance of the contract that is appropriate—

(i) To the size and complexity of the contract; and

(ii) To the nature and scope of the activities to be performed for the Government, including the number of non-United States citizens expected to be employed and the risk that the contract or subcontract will involve services or supplies susceptible to trafficking in persons.

(3) *Minimum requirements.* The compliance plan must include, at a minimum, the following:

(i) An awareness program to inform contractor employees about the Government's policy prohibiting trafficking-related activities described in paragraph (b) of this clause, the activities prohibited, and the actions that will be taken against the employee for violations. Additional information about Trafficking in Persons and examples of awareness programs can be found at the Web site for the Department of State's Office to Monitor and Combat Trafficking in Persons at <http://www.state.gov/j/tip/>.

(ii) A process for employees to report, without fear of retaliation, activity inconsistent with the policy prohibiting trafficking in persons, including a means to make available to all employees the hotline phone number of the Global Human Trafficking Hotline at 1-844-888-FREE and its email address at [help@befree.org](mailto:help@befree.org).

(iii) A recruitment and wage plan that only permits the use of recruitment companies with trained employees, prohibits charging recruitment fees to the employee, and ensures that wages meet applicable host-country legal requirements or explains any variance.

(iv) A housing plan, if the Contractor or subcontractor intends to provide or arrange housing, that ensures that the housing meets host-country housing and safety standards.

(v) Procedures to prevent agents and subcontractors at any tier and at any dollar value from engaging in trafficking in persons (including activities in paragraph (b) of this clause) and to monitor, detect, and terminate any agents, subcontracts, or subcontractor employees that have engaged in such activities.

*(4) Posting.*

(i) The Contractor shall post the relevant contents of the compliance plan, no later than the initiation of contract performance, at the workplace (unless the work is to be performed in the field or not in a fixed location) and on the Contractor's Web site (if one is maintained). If posting at the workplace or on the Web site is impracticable, the Contractor shall provide the relevant contents of the compliance plan to each worker in writing.

(ii) The Contractor shall provide the compliance plan to the Contracting Officer upon request.

*(5) Certification.* Annually after receiving an award, the Contractor shall submit a certification to the Contracting Officer that—

(i) It has implemented a compliance plan to prevent any prohibited activities identified at paragraph (b) of this clause and to monitor, detect, and terminate any agent, subcontract or subcontractor employee engaging in prohibited activities; and

(ii) After having conducted due diligence, either—

(A) To the best of the Contractor's knowledge and belief, neither it nor any of its agents, subcontractors, or their agents is engaged in any such activities; or

(B) If abuses relating to any of the prohibited activities identified in paragraph (b) of this clause have been found, the Contractor or subcontractor has taken the appropriate remedial and referral actions.

*(i) Subcontracts.*

(1) The Contractor shall include the substance of this clause, including this paragraph (i), in all subcontracts and in all contracts with agents. The requirements in paragraph (h) of this clause apply only to any portion of the subcontract that—

(A) Is for supplies, other than commercially available off-the-shelf items, acquired outside the United States, or services to be performed outside the United States; and

(B) Has an estimated value that exceeds \$500,000.

(2) If any subcontractor is required by this clause to submit a certification, the Contractor shall require submission prior to the award of the subcontract and annually thereafter. The certification shall cover the items in paragraph (h)(5) of this clause.

(End of clause)

252.216-7006 ORDERING (MAY 2011)

(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 the effective date of the base period (and any option periods, if exercised).

(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.

(End of Clause)

252.223-7999 ENSURING ADEQUATE COVID-19 SAFETY PROTOCOLS FOR FEDERAL CONTRACTORS (DEVIATION 2021-O0009) (OCT 2021)

(a) Definition. As used in this clause –

United States or its outlying areas means—

(1) The fifty States;

(2) The District of Columbia;

(3) The commonwealths of Puerto Rico and the Northern Mariana Islands;

(4) The territories of American Samoa, Guam, and the United States Virgin Islands; and

(5) The minor outlying islands of Baker Island, Howland Island, Jarvis Island, Johnston Atoll, Kingman Reef, Midway Islands, Navassa Island, Palmyra Atoll, and Wake Atoll.

(b) Authority. This clause implements Executive Order 14042, Ensuring Adequate COVID Safety Protocols for Federal Contractors, dated September 9, 2021 (published in the Federal Register on September 14, 2021, 86 FR 50985).



(c) Compliance. The Contractor shall comply with all guidance, including guidance conveyed through Frequently Asked Questions, as amended during the performance of this contract, for contractor or subcontractor workplace locations published by the Safer Federal Workforce Task Force (Task Force Guidance) at <https://www.saferfederalworkforce.gov/contractors/>.

(d) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts at any tier that exceed the simplified acquisition threshold, as defined in Federal Acquisition Regulation 2.101 on the date of subcontract award, and are for services, including construction, performed in whole or in part within the United States or its outlying areas.

(End of clause)

252.225-7043 ANTITERRORISM/FORCE PROTECTION POLICY FOR DEFENSE CONTRACTORS  
OUTSIDE THE UNITED STATES (JUN 2015)

(a) Definition. United States, as used in this clause, means, the 50 States, the District of Columbia, and outlying areas.

(b) Except as provided in paragraph (c) of this clause, the Contractor and its subcontractors, if performing or traveling outside the United States under this contract, shall--

- (1) Affiliate with the Overseas Security Advisory Council, if the Contractor or subcontractor is a U.S. entity;
- (2) Ensure that Contractor and subcontractor personnel who are U.S. nationals and are in-country on a non-transitory basis, register with the U.S. Embassy, and that Contractor and subcontractor personnel who are third country nationals comply with any security related requirements of the Embassy of their nationality;
- (3) Provide, to Contractor and subcontractor personnel, antiterrorism/force protection awareness information commensurate with that which the Department of Defense (DoD) provides to its military and civilian personnel and their families, to the extent such information can be made available prior to travel outside the United States; and
- (4) Obtain and comply with the most current antiterrorism/force protection guidance for Contractor and subcontractor personnel.

(c) The requirements of this clause do not apply to any subcontractor that is--

- (1) A foreign government;
- (2) A representative of a foreign government; or
- (3) A foreign corporation wholly owned by a foreign government.

(d) Information and guidance pertaining to DoD antiterrorism/force protection can be obtained from USTRANSCOM/TCJ3-FP Commercial: (618) 229-7711.

(End of clause)

5152.225-5902 - FITNESS FOR DUTY AND MEDICAL/DENTAL CARE LIMITATIONS (JUN 2015)

- (a) The contractor shall ensure the individuals they deploy are in compliance with the current USCENTCOM Individual Protection and Individual/Unit Deployment Policy, including TAB A, Amplification of the Minimal Standards of Fitness for Deployment to the CENTCOM AOR, unless a waiver is obtained in accordance with TAB C, CENTCOM Waiver Request. The current guidance is located at <http://www2.centcom.mil/sites/contracts/Pages/GCP.aspx>.
- (b) The contractor shall perform the requirements of this contract notwithstanding the fitness for duty of deployed employees, the provisions for care offered under this section, and redeployment of individuals determined to be unfit.
- (c) Contractor personnel who deploy for multiple tours, which exceed 12 months in total, must be re-evaluated for fitness to deploy every 12 months IAW the current USCENTCOM Individual Protection and Individual/Unit Deployment Policy standards. An examination will remain valid for 15 months from the date of the physical. This allows an examination to be valid up to 90 days prior to deployment. Once a deployment begins, the examination will only be good for a maximum of 12 months. Any medical waivers received will be valid for a maximum of 12 months. Failure to obtain an updated medical waiver before the expiration of the current waiver renders the employee unfit and subject to redeployment.
- (d) The contractor bears the responsibility for ensuring all employees are aware of the conditions and medical treatment available at the performance location. The contractor shall include this information in all subcontracts with performance in the theater of operations.
- (e) In accordance with military directives (DoDI 3020.41, DoDI 6000.11, CFC FRAGO 09-1038, DoD Federal Acquisition Regulation Supplement (DFARS) PGI 225.74), resuscitative care, stabilization, hospitalization at a Role 3 military treatment facility (MTF) for emergency life-limb-eyesight care will be provided along with assistance for urgent patient movement. Subject to availability, an MTF may provide reimbursable treatment for emergency medical or dental services (e.g., broken bones, lacerations, broken teeth or lost fillings).
- (f) Routine and primary medical care are not authorized. Pharmaceutical services are not authorized for known or routine prescription drug needs of the individual. Routine dental care, examinations and cleanings are not authorized.
- (g) Notwithstanding any other provision of the contract, the contractor shall be liable for any and all medically-related services or patient movement rendered. To view reimbursement rates that will be charged for services at all DoD deployed medical facilities please go to the following website:  
<http://comptroller.defense.gov/FinancialManagement/Reports/rates2014.aspx>.

(End of Clause)

#### 5152.225-5907 - MEDICAL SCREENING AND VACCINATION REQUIREMENTS FOR CONTRACTOR EMPLOYEES OPERATING IN THE CENTCOM AREA OF RESPONSIBILITY (AOR) (JUN 2015)

- (a) All contractor employees are required to be medically, dentally, and psychologically fit for deployment and performance of their contracted duties as outlined in the Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.225-7995, Contractor Personnel Performing in the United States Central Command Area of Responsibility. This clause requires all contractor personnel to meet the theater specific medical qualifications established by the Geographic Combatant Commander before deploying to, being granted installation access, or performing work under the resultant contract. In the USCENTCOM Area of Operation (AOR), the required medical screening, immunizations, and vaccinations are specified in the current USCENTCOM individual Protection and Individual Unit Deployment Policy and DoD Instruction (DODI) 3020.41, Operational Contract Support (OCS). Current medical screening, immunization, and vaccination requirements are available at <http://www2.centcom.mil/sites/contracts/Pages/GCP.aspx>. The current DODI is available at

<http://www.dtic.mil/whs/directives/corres/ins1.html>. The current list of immunization and vaccination requirements are available at <http://www.vaccines.mil>.

(b) The USCENTCOM policy requires contractors to ensure adequate health management is available for Tuberculosis (TB) screening, diagnosis, treatment, and isolation during the life of the contract. This includes management and compliance with all prescribed public health actions regarding TB and the responsibility to ensure adequate health management is available at the Contractor's medical provider or local economy provider's location for all contractor and subcontractor employees throughout the life of the contract. The contractor shall maintain medical screening documentation, in English, and make it available to the Contracting Officer, military public health personnel, or Base Operations Center installation access badging personnel upon request.

(1) U.S. Citizens are considered Small-Risk Nationals (SRNs) as the U.S. has less than 25 TB cases per 100,000 persons. A TB testing method of either a TB skin test (TST) or Interferon Gamma Release Assay (IGRA) may be used for pre-deployment and annual re-screening of all U.S. Citizens employed under the contract. For a contact investigation, all personnel with a positive TST or IGRA will be evaluated for potential active TB with a symptom screen, exposure history and CXR. A physical copy of all TST, IGRA, and/or CXRs and radiographic interpretation must be provided at the deployment center designated in the contract, or as otherwise directed by the Contracting Officer, prior to deployment and prior to installation access badge renewal.

(2) Other Country Nationals (OCNs) and Local Nationals (LNs) shall have pre-deployment/employment testing for TB using a Chest x-ray (CXR) and a symptom survey completed within 3 months prior to the start of deployment/employment, with annual re-screening prior to installation access badge renewal. This is the only way to verify interval changes should an active case of TB occur. When conducting annual re-screening, the Contractor's medical provider or local economy provider will look for interval changes from prior CXR's and review any changes in the symptom survey. A physical copy of the CXR film with radiographic interpretation showing negative TB results must be provided to the Base Operations Center prior to the start of deployment/employment, with annual re-screening prior to installation access badge renewal.

(3) After arrival in the USCENTCOM AOR, all cases of suspected or confirmed active TB must be reported to the theater Preventive Medicine (PM) Physician and/or TB Consultant within 24 hours. Contact tracing, and medical coding, have specific requirements. After consultation with the Theater PM or TB Consultant, the contractor or subcontractor with suspected or confirmed TB are required to be evacuated to the closest civilian hospital for treatment. The Contractor is responsible for management and compliance with all prescribed public health actions. The employee, contractor/sub-contractor shall be transported out of theater following three (3) consecutive negative sputum smears.

(c) All employees, contractors and sub-contractors, involved in food service, water and/or ice production facilities must be pre-screened prior to deployment and re-screened annually for signs and symptoms of infectious diseases. This includes a stool sample test for ova and parasites. Additionally, all employees, contractors and sub-contractors, will have completed: (1) the full series of immunization for Typhoid and Hepatitis "A" (full series) immunizations per the Centers for Disease Control and Prevention guidelines (e.g. typhoid vaccination booster is required every 2 years); (2) the required TB tests; and (3) screening for Hepatitis B and C.

(d) Proof of pre-deployment and deployment medical screening, immunizations, and vaccinations (in English) for employees, contractors and sub-contractors shall be made available to the designated Government representative throughout the life of the contract, and provided to the Contracting Officer, for a minimum of six (6) years and (3) months from the date of final payment under the contract.

(End of Clause)

The following is a summary of the type of support the Government will provide the contractor. Services will be provided to contractors at the same level as they are provided to military and DoD civilian personnel. In the event of any discrepancy between this summary and the description of services in the Statement of Work, this clause will take precedence. These services are only provided at the following locations: Bagram and Kandahar. When contractor employees are in transit, all checked blocks are considered authorized. NOTE: The services marked in this special clause must be consistent with information marked on the approved GFLSV form.

#### U.S. Citizens

|                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> APO/FPO/MPO/DPO/<br>Postal Service<br><input type="checkbox"/> Authorized Weapon *****<br><input type="checkbox"/> Billeting***<br><input type="checkbox"/> CAAF*<br><input checked="" type="checkbox"/> Controlled Access Card (CAC)<br><input checked="" type="checkbox"/> Installation Access Badge<br><input type="checkbox"/> Military Exchange<br><input type="checkbox"/> Embassy Services Kabul** | <input type="checkbox"/> DFACs****<br><br><input type="checkbox"/> Excess Baggage<br><input checked="" type="checkbox"/> Fuel Authorized<br><input type="checkbox"/> Govt Furnished Meals****<br><input type="checkbox"/> Military Banking<br><input type="checkbox"/> Laundry<br><input type="checkbox"/> None | <input type="checkbox"/> Mil Issue Equip<br><br><input type="checkbox"/> MILAIR(inter/intra theater)<br><input type="checkbox"/> MWR<br><br><input type="checkbox"/> Transportation<br><input type="checkbox"/> Military Clothing |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Third-Country National (TCN) Employees

|                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> N/A<br><input type="checkbox"/> Authorized Weapon*****<br><input type="checkbox"/> Billeting***<br><input type="checkbox"/> CAAF*<br><input type="checkbox"/> Controlled Access Card (CAC)<br><input checked="" type="checkbox"/> Installation Access Badge<br><input type="checkbox"/> Military Exchange | <input type="checkbox"/> DFACs****<br><input type="checkbox"/> Excess Baggage<br><input type="checkbox"/> Fuel Authorized<br><input type="checkbox"/> Govt Furnished Meals****<br><input type="checkbox"/> Military Banking<br><input type="checkbox"/> Laundry<br><input type="checkbox"/> None | <input type="checkbox"/> Mil Issue Equip<br><input type="checkbox"/> MILAIR (inter/intra theater)<br><input type="checkbox"/> MWR<br><input type="checkbox"/> Military Clothing<br><input type="checkbox"/> Transportation<br><input type="checkbox"/> All |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Local National (LN) Employees

|                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> N/A<br><input type="checkbox"/> Authorized Weapon*****<br><br><input type="checkbox"/> Billeting***<br><input type="checkbox"/> CAAF*<br><input type="checkbox"/> Controlled Access Card (CAC)<br><input type="checkbox"/> Installation Access Badge<br><input type="checkbox"/> Military Exchange<br><input type="checkbox"/> Dependents Authorized | <input type="checkbox"/> DFACs****<br><input type="checkbox"/> Excess Baggage<br><br><input type="checkbox"/> Fuel Authorized<br><input type="checkbox"/> Govt Furnished Meals****<br><input type="checkbox"/> Military Banking<br><input type="checkbox"/> Laundry<br><input checked="" type="checkbox"/> None | <input type="checkbox"/> Mil Issue Equip<br><input type="checkbox"/> MILAIR(intra theater)<br><br><input type="checkbox"/> MWR<br><input type="checkbox"/> Military Clothing<br><input type="checkbox"/> Transportation<br><input type="checkbox"/> All |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

\* CAAF is defined as Contractors Authorized to Accompany Forces.

\*\* Applies to US Embassy Life Support in Afghanistan only. See special note below regarding Embassy support.

\*\*\* Afghanistan Life Support. Due to the drawdown of base life support facilities throughout the country, standards will be lowering to an "expeditionary" environment. Expeditionary standards will be base specific, and may include down grading from permanent housing (b-huts, hardened buildings) to temporary tents or other facilities.

\*\*\*\* Check the "DFAC" AND "Government Furnished Meals" boxes if the contractor will have access to the DFAC at no cost. "Government Furnished Meals" (GFM) is defined as meals at no cost to the contractor (e.g, MREs, or meals at the DFAC. If GFM is checked, "DFAC" must also be checked.

Due to drawdown efforts, DFACS may not be operational. Hot meals may drop from three per day to one or none per day. MREs may be substituted for DFAC-provided meals; however, contractors will receive the same meal standards as provided to military and DoD civilian personnel.

\*\*\*\*\*Military Banking indicates “approved use of military finance offices to either obtain an Eagle Cash Card or cash checks.

\*\*\*\*\*Authorized Weapon indicates this is a private security contract requirement and contractor employees, upon approval, will be authorized to carry a weapon. If the service is NOT a private security contract, the checking of this box does NOT authorize weapons for self-defense without the approval of the USFOR-A Commander in accordance with USFOR-A policy. After award, the contractor may request arming for self-defense off a U.S. installation to the Contracting Officer’s Representative and in CAAMS.

SPECIAL NOTE – US Embassy Afghanistan Life Support: The type and amount of support that the U.S. Embassy Mission in Kabul, Afghanistan, provides to contractors, if any, must be coordinated in advance between the U.S. Mission and the contracting agency in accordance with Department of State Foreign Affairs Handbook, 2-FAH-2. Contractors are not authorized to deploy personnel requiring US Mission support prior to receiving clearance from the Contracting Officer.

SPECIAL NOTE ON MILAIR – MILAIR is allowed for the transportation of DoD contractor personnel (US, TCN, LN) as required by their contract and as approved in writing by the Contracting Officer or Contracting Officer Representative. Transportation is also allowed for contractor equipment required to perform the contract when that equipment travels with the contractor employee (e.g., special radio test equipment, when the contractor is responsible for radio testing or repair)

(End of Clause)

#### 5152.225-5910 CONTRACTOR HEALTH AND SAFETY (DEC 2011)

(a) Contractors shall comply with National Electrical Code (NEC) 2008 for repairs and upgrades to existing construction and NEC 2011 standards shall apply for new construction, contract specifications, and MIL Standards/Regulations. All infrastructure to include, but not limited to, living quarters, showers, and restrooms shall be installed and maintained in compliance with these standards and must be properly supported and staffed to ensure perpetual Code compliance, prevent hazards and to quickly correct any hazards to maximize safety of those who use or work at the infrastructure.

(b) For existing employee living quarters the contractor shall provide maintenance, conduct repairs, and perform upgrades in compliance with NEC 2008 standards. For new employee living quarters, the contractor shall provide maintenance, conduct repairs, and make upgrades in compliance with NEC 2011 standards. The government has the authority to enter and inspect contractor employee living quarters at any time to ensure the prime contractor is complying with safety compliance standards.

(c) The contractor shall correct all deficiencies within a reasonable amount of time of becoming aware of the deficiency either by notice from the government or a third party, or by self discovery of the deficiency by the contractor. Further guidance can be found on:

UFC: [http://www.wbdg.org/ccb.browse\\_cat.php?o=29&c=4](http://www.wbdg.org/ccb.browse_cat.php?o=29&c=4)

NFPA 70: <http://www.nfpa.org>

NESC: <http://www.standards.ieee.org/nesc>

(End of Clause)

#### 5152.225-5914 COMMODITY SHIPPING INSTRUCTIONS (AUG 2011)

(a) USFOR-A FRAGO 10-200. United States Forces Afghanistan (USFOR-A) has directed that all shipments into and out of the Combined Joint Operations Area - Afghanistan (CJOA-A) be coordinated through the Defense

Transportation System (DTS) in order to expedite the customs clearance process and facilitate the use of in-transit visibility for all cargo in the CJOA-A

(b) Information regarding the Defense Transportation System (DTS). For instructions on shipping commodity items via commercial means using DTS, see the following websites:

1. Defense Transportation Regulation – Part II Cargo Movement - Shipper, Trans-shipper, and Receiver Requirements and Procedures:  
[http://www.transcom.mil/dtr/part-ii/dtr\\_part\\_ii\\_203.pdf](http://www.transcom.mil/dtr/part-ii/dtr_part_ii_203.pdf)

2. Defense Transportation Regulation – Part II 4 Cargo Movement – Cargo Routing and Movement: [http://www.transcom.mil/dtr/part-ii/dtr\\_part\\_ii\\_202.pdf](http://www.transcom.mil/dtr/part-ii/dtr_part_ii_202.pdf)

3. Defense Transportation Regulation – Part V - Department of Defense Customs and Border Clearance Policies and Procedures: [http://www.transcom.mil/dtr/part-v/dtr\\_part\\_v\\_512.pdf](http://www.transcom.mil/dtr/part-v/dtr_part_v_512.pdf)

(c) Responsibilities of the vendor carrier representative, shipping expeditor, and/or customs broker:

1. Afghanistan Import Customs Clearance Request Procedures: The carrier, shipping expeditor, and/or customs broker is responsible for being knowledgeable about the Afghan Customs Clearance Procedures.
2. Status of Customs Clearance Requests: All inquiries regarding the status of a customs clearance request prior to its submission to Department of Defense (DoD) Customs and after its return to the carrier representative or shipping expeditor should be directed to the carrier or shipping agent.
3. Customs Required Documents: The carrier representative or shipping expeditor is required to provide the DoD Contracting Officer Representative (COR) with all documentation that will satisfy the requirements of the Government of the Islamic Republic of Afghanistan (GIROA).

(d) Required Customs Documents: Documents must be originals (or copies with a company stamp). Electronic copies or photocopied documents will not be accepted by GIROA. The carrier is responsible for checking the current requirements for documentation with the Afghanistan Customs Department (ACD) as specified by the U.S. Embassy Afghanistan's SOP for Customs Clearance Requests Operations (<http://trade.gov/static/AFGCustomsSOP.pdf>) and paragraph 4 below.

1. The U.S. Ambassador Afghanistan diplomatic note guarantees that the U.S. Government (USG) shipments are exempt from Afghanistan Customs duties and taxes. USG shipments do not provide commercial carriers with the authority to unnecessarily delay shipments or holdover shipments in commercial storage lots and warehouses while en route to its final destination. The U.S. Embassy expects that shipments will be expedited as soon as customs clearance paperwork is received from the respective GIROA officials.
2. Imports: Documentation must list the year, make, model, and color of the commodity, the commodity Identification Number (if applicable) and for vehicles, the Engine Block Number. The following documentation is required for all import shipments:
  - a. An original Customs Clearance Request (CCR) prepared by the COR in accordance with Afghanistan customs guidance referenced in paragraph 4 below.
  - b. Bills of Lading (for shipments by sea), Airway Bills (for shipments by air) or Commodity Movement Request (CMRs) (for overland shipments). In the consignee block, type in "US Military". This will help the Afghan Customs officials to recognize that the shipment belongs to the US Military and, therefore, the shipment is subject to tax exemption provisions as specified under the current Diplomatic Note or Military Technical Agreement (MTA).
  - c. Shipping Invoices.
  - d. Packing Lists. Required only if the shipping invoice does not list the cargo.
  - e. An Afghan Government Tax Exemption Form (Muaffi Nama) purchased from the Department of Customs and Revenue and prepared in the local language by the carrier representative, shipping agent, or customs broker.
  - f. A Diplomatic Note, prepared by DoD Customs, to the Ministry of Foreign Affairs requesting the initiation of customs formalities with the Ministry of Finance, Department of Customs and Exemptions. Please note that DoD Customs is not responsible for registering vehicles.
  - g. Commercially-owned equipment such as vehicles, construction machinery or generators that are leased and imported to Afghanistan for the performance of a USG contract may be subject to taxes and duties as determined by GIROA. If commercially-owned equipment is imported into Afghanistan in a duty-free status, that duty-free status only applies as long as the equipment is under the exclusive use of the USG contract. If the equipment is released at

the end of the contract, applicable GIRoA duties and taxes will apply to the owner if the equipment is not exported from Afghanistan or transferred to another USG contract.

h. USG-owned vehicles must be exported at the conclusion of the project period or transferred to another USG entity. Under certain conditions, the USG may transfer equipment or vehicles to GIRoA.

3. Exports: The following documentation is required for all export shipments:

a. An original CCR prepared by the COR. If COR is not available, the Contracting Officer (KO) will prepare the CCR.

b. Invoices.

c. Packing Lists. Required only if the shipping invoice does not list the cargo.

d. A Diplomatic Note, prepared by the DoD Customs Cell, to the Ministry of Foreign Affairs requesting the initiation of customs formalities with the Ministry of Finance, Department of Customs and Exemptions.

4. Customs requirements from the GIRoA may change with little notice. For current detailed instructions on customs guidelines in Afghanistan, refer to "The Instruction for Customs Clearance Request (Import/Export) Operations." In all cases, the carrier is required to obtain a copy of this document, found at the following link: <http://trade.gov/static/AFGCustomsSOP.pdf>

(e) Point of contact (POC) for customs issues is the USFOR-A Joint Security Office (JSO) J3 at DSN: 318-449-0306 or 449-0302. Commercial to DSN conversion from the United States is (732) 327-5130, choose option #1, and then dial 88-318 followed by your seven-digit DSN number.

(End of Clause)

#### 5152.225-5915 CONTRACTOR ACCOUNTABILITY AND PERSONNEL RECOVERY (JUN 2014)

(a) Contract performance may require work in dangerous or austere conditions. Except as otherwise provided in the contract, the contractor accepts the risks associated with required contract performance in such operations.

(1) Unaccounted Personnel: It is the expectation of the USG that any contractor brought into Afghanistan for the sole purposes of performance of work on a USG contract must be accounted for at all times by their respective employers. Additionally, contractors who maintain living quarters on a USG base shall verify the location of each of its employees' living quarters a minimum of once a month. If a DoD contracted employee becomes missing and evidence does not indicate foul play, a Personnel Recovery (PR) event is NOT automatically triggered. Such an event will be treated as an accountability battle drill by the employer's chain of command or civilian equivalent.

(2) Contractor Responsibilities: The contractor is responsible to take all necessary steps to locate and investigate the unaccounted for employee(s) whereabouts to the maximum extent practicable. To assist in this process, contractors may use the Operational Contracting Support Drawdown Cell as a resource to track or research employee's last known location and/or to view LOA's. All missing personnel will be immediately reported to the installation division Personnel Recovery Officer (PRO), Mayor's cell, Military Police Station and/or the Criminal Investigative Division, and the Base Defense Operations Center (BDOC).

(3) Contractor Provided Information: If it is determined that a potential criminal act has occurred, the USD PRO (or USFOR-A Personnel Recovery Division (PRD) with prior coordination) will attempt to validate the missing person's identity through the employer. The contractor shall provide the information to PRD within 12 hours of request. The required information the contractor should keep on file includes but is not limited to: copy of the individual's Letter of Authorization generated by the Synchronized Pre-deployment and Operational Tracker System (SPOT), copy of passport and visas, housing information of where the individual resides such as room number and location, DD Form 93, Record of Emergency Data, copy of badging, and contact information for known friends or associates.

(b) If USFOR-A PRD determines through investigation that the unaccounted personnel have voluntarily left the installation either seeking employment with another contractor or other non-mission related reasons, PRD will notify the contractor. The contractor shall ensure that all government-related documents such as LOA's, visas, etc. are terminated/reconciled appropriately within 24 hours of notification by PRD in accordance with subparagraph (a)(8) of DFARS clause 252.225-7997 entitled "Contractor Demobilization". Contractors who fail to account for their personnel or whose employees create PR events will be held in breach of their contract and face all remedies available to the Contracting Officer.

(c) Contractors shall notify the Contracting Officer, as soon as practicable, whenever employee kidnappings, serious injuries or deaths occur. Report the following information:

Contract Number  
Contract Description & Location  
Company Name

Reporting party:  
Name  
Phone number  
e-mail address

Victim:  
Name  
Gender (Male/Female)  
Age  
Nationality  
Country of permanent residence

Incident:  
Description  
Location  
Date and time

Other Pertinent Information

(End of Clause)

#### 5152.225-5916 MANDATORY ELIGIBILITY FOR INSTALLATION ACCESS (OCT 2015)

(a) U.S. and Coalition Commanders possess inherent authority to maintain law and order, provide security, and impose discipline necessary to protect the inhabitants of U.S. and/or Coalition installations, U.S. and Coalition personnel operating outside of installations, and U.S. or Coalition-funded developmental projects in Afghanistan. This authority allows commanders to administratively and physically control access to installations and/or project sites, and to bar contractors – including prime contractors, subcontractors at any tier, and any employees, from an installation or site. A commander's inherent force protection (FP) authority is independent of an agency's contracting authority, and it may not be superseded by any contractual term or provision.

(b) The prime Contractor/Vendor acknowledges that: submission of a bid, offer, or a proposal; acceptance of contract award of any type; or continuing effort under any contract that includes this clause; requires that the prime Contractor/Vendor, and all subcontractors under any affected contracts be initially eligible – and remain eligible during the entire period of contract performance to include any warrant period – for installation access to a U.S. and/or Coalition installation, regardless of whether the performance will take place on or off a U.S. or Coalition installation.



(c) To be eligible for installation access, Contractors and subcontractors at all tiers are required to register for installation access in the Joint Contingency Contracting System (JCCS) and are responsible for keeping the information in the this system updated at all times. Prime Contractors and subcontractors at any tier may verify their registration at <https://www.jccs.gov/jccscoe/> by selecting the “Vendors Login” module and logging in with their user name and password. The offeror must be registered, approved, and eligible for installation access prior to award, and remain eligible for installation access for the life of the contract.

(1) The offeror is required to submit a listing of all proposed subcontractors , at all tiers, to the contracting officer with the submission of the proposal, and provide updates during the life of the contract when subcontractors are added or removed. If no subcontractors are expected to perform during the life of the contract, the offeror must submit a negative response to the Contracting Officer with its proposal. After award, the prime contractor must submit a negative response to the contracting officer at the beginning of each performance period.

(2) Failure to be approved in JCCS – and thereby be eligible for installation access at the Prime and subcontractor levels – or failure to inform the contracting officer of the names of all prospective subcontractors (or provide a negative reply), may render the offerors/contractor ineligible for award or continued performance. Additionally, any firm that is declared ineligible for installation access will be deemed non-responsible until such time as that firm is again deemed eligible by the appropriate access approval authority.

(d) Installation access determinations arise from the Combatant Commander’s inherent authority and are separate and distinct from any law, regulation, or policy regarding suspension and debarment authority. Contractor queries or requests for reconsideration related to U.S. or Coalition installation base access eligibility must be directed to the authority responsible for base access decisions.

(End of Clause)

#### LIST OF ATTACHMENTS

| Attachment #  | Name                                                  | Revision | Version Date  |
|---------------|-------------------------------------------------------|----------|---------------|
| Attachment 1  | Performance Work Statement                            | Rev5     | 15 June 2023  |
| Attachment 2  | Invoicing and Payment                                 | Rev2     | 24 June 2021  |
| Attachment 3  | Ordering Procedures                                   |          |               |
| Attachment 4  | Reports and Formats                                   | Rev3     | 11 May 2023   |
| Attachment 5  | Yubikey Authorized Approver List and Issued List      | Rev1     | 24 June 2021  |
| Attachment 6  | Special Provisions for DLA Prime Vendor Program Cargo | Rev1     | 24 June 2021  |
| Attachment 7  | NIST 800-171 POAM                                     | Rev3     | 15 June 2023  |
| Attachment 8  | Wage Determinations                                   | Rev3     | 07 July 2023  |
| Attachment 9  | SHARP                                                 | Rev1     | 24 June 2021  |
| Attachment 10 | FEV Template                                          |          | 13 March 2023 |
| Attachment 11 | DD 254                                                |          |               |
| Attachment 12 | Subcontracting Plan                                   |          |               |

### Multimodal 3 (MM-3) Performance Work Statement

#### TABLE OF CONTENTS

|           |                                                                       |    |
|-----------|-----------------------------------------------------------------------|----|
| SECTION 1 | GENERAL REQUIREMENTS.....                                             | 3  |
| 1.1       | Scope of Contract .....                                               | 3  |
| 1.2       | Requirement for Participation and Good Standing in CRAF or VISA ..... | 3  |
| 1.3       | Contractor Personnel .....                                            | 3  |
| 1.4       | Customer Service.....                                                 | 3  |
| 1.5       | Cargo .....                                                           | 3  |
| 1.6       | Contractor-Provided Equipment .....                                   | 4  |
| 1.7       | Government Furnished Containers (GFC).....                            | 4  |
| 1.8       | Hazardous Cargo .....                                                 | 4  |
| 1.9       | Scheduling .....                                                      | 4  |
| 1.10      | Cargo Available Date .....                                            | 5  |
| 1.11      | Providing Empty Containers to Shippers.....                           | 5  |
| 1.12      | Perishables Transportation.....                                       | 5  |
| 1.13      | Pre-Alert Notification .....                                          | 6  |
| 1.14      | Required Delivery Date (RDD) .....                                    | 6  |
| 1.15      | Delivery Notification and Receipt .....                               | 6  |
| 1.16      | Concept of Operations (CONOPS).....                                   | 7  |
| 1.17      | Operational Reports .....                                             | 7  |
| 1.18      | Booking Reconciliation Tool (BRT) .....                               | 7  |
| 1.19      | Cargo Clearance (Sealift).....                                        | 7  |
| 1.20      | Prior Permission Required (PPR) Process .....                         | 8  |
| 1.21      | Restrictions on Subcontracting to Air Contractors .....               | 9  |
| 1.22      | Sexual Harassment/Assault Response & Prevention (SHARP).....          | 9  |
| 1.23      | Good Order and Condition .....                                        | 10 |
| 1.24      | Invoice Submission.....                                               | 10 |
| SECTION 2 | PERFORMANCE MEASURES .....                                            | 10 |
| 2.1       | Performance Requirements.....                                         | 10 |
| 2.2       | Performance Measures and Performance Standards.....                   | 10 |
| 2.3       | Performance Objectives.....                                           | 10 |
| 2.4       | Performance Objective Assessment.....                                 | 11 |
| 2.5       | Performance Rating .....                                              | 11 |
| 2.6       | Limited Use .....                                                     | 13 |
| SECTION 3 | EXCEPTIONS TO NORMAL SERVICE.....                                     | 13 |
| 3.1       | Cancellation/No Show .....                                            | 13 |
| 3.2       | Cargo Rolls.....                                                      | 13 |
| 3.3       | Rerouting of Cargo .....                                              | 13 |

|                                                                                                       |                                                                            |    |
|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|----|
| 3.4                                                                                                   | Broken/Replacement of Seals .....                                          | 13 |
| 3.5                                                                                                   | Transportation Discrepancy Reports (TDR) .....                             | 14 |
| 3.6                                                                                                   | Containerization for the Convenience of the Contractor .....               | 14 |
| 3.7                                                                                                   | Live Load / Unload.....                                                    | 14 |
| 3.8                                                                                                   | Defense Logistics Agency-Energy Ground and Aviation Fuel.....              | 14 |
| SECTION 4 ACCESSORIALS.....                                                                           |                                                                            | 15 |
| 4.1                                                                                                   | Cargo Concealment .....                                                    | 15 |
| 4.2                                                                                                   | Exterior Cargo Rinsing Service .....                                       | 15 |
| 4.3                                                                                                   | Exterior Cargo Washing Service .....                                       | 15 |
| 4.4                                                                                                   | Interior Cargo Washing Service.....                                        | 16 |
| SECURITY (PHYSICAL, PERSONNEL, INFORMATION, ANTITERRORISM / FORCE<br>PROTECTION AND INDUSTRIAL) ..... |                                                                            | 16 |
| 4.5                                                                                                   | General Security Information .....                                         | 16 |
| 4.6                                                                                                   | Additional Security Requirements (Transportation Security).....            | 16 |
| 4.7                                                                                                   | Citizenship and Clearance Requirements .....                               | 16 |
| 4.8                                                                                                   | Security Clearance Requirements .....                                      | 16 |
| 4.9                                                                                                   | Facilities Clearance (FCL).....                                            | 17 |
| 4.10                                                                                                  | Access to Scott Air Force Base or USTRANSCOM Facilities.....               | 17 |
| 4.11                                                                                                  | Classified Information at Contractor Headquarters .....                    | 17 |
| 4.12                                                                                                  | Classified Meetings .....                                                  | 17 |
| 4.13                                                                                                  | Derogatory Information .....                                               | 17 |
| 4.14                                                                                                  | Security Regulation Guidance: .....                                        | 17 |
| 4.15                                                                                                  | USTRANSCOM Force Protection (Industrial Security) Points of Contact: ..... | 18 |
| 4.16                                                                                                  | SDDC G34 Protection Division (Industrial Security) Point of Contact:.....  | 18 |
| 4.17                                                                                                  | Foreign Entity Vetting .....                                               | 18 |
| 4.18                                                                                                  | Electronic Systems Access .....                                            | 19 |
| 4.19                                                                                                  | Aircraft Recovery Process .....                                            | 20 |
| 4.20                                                                                                  | Incident Reporting .....                                                   | 20 |
| 4.21                                                                                                  | General Cyber Security Requirements.....                                   | 20 |
| SECTION 5 ELECTRONIC DATA INTERCHANGE (EDI) TRANSACTIONS AND DAILY ITV .....                          |                                                                            | 25 |
| 5.1                                                                                                   | EDI Transactions .....                                                     | 25 |
| 5.2                                                                                                   | Shipment Status Reporting .....                                            | 26 |
| SECTION 6 Liability .....                                                                             |                                                                            | 27 |
| 6.1                                                                                                   | Liability for Lost or Damaged Cargo.....                                   | 27 |
| 6.2                                                                                                   | Contractor Bodily Injury and Property Damage Liability .....               | 28 |
| SECTION 7 ACRONYMS AND DEFINITIONS .....                                                              |                                                                            | 28 |
| 7.1                                                                                                   | Acronyms.....                                                              | 28 |
| 7.2                                                                                                   | Definitions .....                                                          | 31 |
| SECTION 8 DELIVERABLES .....                                                                          |                                                                            | 36 |

## **SECTION 1 GENERAL REQUIREMENTS**

### **1.1 Scope of Contract**

1.1.1 This contract's purpose is to provide international, commercial, door to door, cargo transportation services. Multiple or single modes (e.g. airlift, sealift, linehaul) of transportation may be used in any combination to move cargo globally. The Government reserves the right to require transportation of cargo through a particular SPOE, SPOD, APOE, and/or APOD. Cargo moved under this contract will not transit the Pakistan Ground Line of Communication (PAKGLOC) unless otherwise specified in the RFQ.

1.1.2 The contractor shall provide all personnel, training, supervision, equipment, Prior Permission Required (PPRs) Request and Authorization, Diplomatic Clearances (DIPS), and customs clearance procedures necessary to perform international commercial transportation services to move Department of Defense (DoD) and other Government Agency approved cargo.

1.1.3 The Contractor is responsible to have proper equipment and personnel necessary to be self-sufficient at all ports and installations. Shippers will be responsible to load/unload ground conveyances at origin/final destination.

### **1.2 Requirement for Participation and Good Standing in CRAF or VISA**

1.2.1 Contractors shall be Department of Defense approved carriers, not in a suspended non-use status (carrier in good standing), participating in the Civil Reserve Air Fleet (CRAF) or Voluntary Intermodal Sealift Agreement (VISA) throughout the performance of this contract. For CRAF, the contractor shall be a U.S. registered air carrier operating under Federal Aviation Regulations, Part 121, and possessing a current certificate issued by the FAA pursuant to Federal Aviation Regulations, Part 121. For VISA, the contractor shall be the owner/operator of U.S. Flag vessels and shall comply with the Cargo Preference Act of 1904.

### **1.3 Contractor Personnel**

1.3.1 The contractor shall provide a point of contact who is fluent in English and is authorized to provide oversight of the performance of this contract. The name of this person shall be designated in writing to the Contracting Officer prior to the contract start date.

1.3.2 The contractor shall attend periodic performance review and feedback meetings (e.g., quarterly, semi-annual, or annual) at no additional charge. These will, typically, be held via telephone.

1.3.3 In preparation for exercising each option period, approximately once every two years, SDDC and TRANSCOM will hold a Multimodal Carrier Conference to review the progress of the contract and discuss changes to the contract.

### **1.4 Customer Service**

The contractor shall submit points of contact who can respond to Government activities on a 24/7 basis to provide expert assistance in answering questions, exchanging information, and resolving problems. The contractor shall provide specific points of contact no later than 7 days after contract award.

### **1.5 Cargo**

1.5.1 Cargo may consist of containers, pallets, breakbulk, rolling stock, tricons or quadcons. (No commercial Flatracks or Open Top containers will be booked.)

1.5.2 Cargo may be booked as container or breakbulk cargo, depending on shipper requirements. Breakbulk or

Government-owned/leased containers will retain surface shipping configurations throughout transport, to include airlift. Breakbulk cargo may be containerized for sealift and/or linehaul convenience at no cost to the Government.

1.5.3 Contractor-owned/provided containers will be unstuffed and reconfigured on commercial equipment (e.g. Air Configured Pallets) prior to airlift, as described in subsequent sections, unless otherwise identified in the RFQ requirements.

## **1.6 Contractor-Provided Equipment**

1.6.1 Container Standards. Upon request, contractors shall provide containers with clearly marked container numbers that are clean, dry, empty, odor free, suitable for protecting cargo from damage and comply with International Standardization Organization (ISO), International Maritime Organization (IMO), and Convention of Safe Containers (CSC) standards.

1.6.2 Substitution of Equipment: When the contractor has accepted a booking and does not provide the conveyance listed in the booking, the contractor shall provide a suitable alternative agreed upon by the shipper and the Ordering Officer (OO) at no additional cost to the Government.

1.6.3 Chassis Requirements. For origin CONUS shipments, any containers delivered to the Government or spotted by the contractor must be on a contractor-provided chassis that supports stuffing/unstuffing operations by the Government. The chassis must remain with the container while in the custody of the Government; unless this requirement is waived by the cognizant Contracting Officer. Blanket waivers for specific areas or destinations may be issued by the cognizant Contracting Officer upon request. See 1.7.2 for further chassis requirements.

## **1.7 Government Furnished Containers (GFC)**

1.7.1 GFC includes 8.0'- 9.5' high x 8' wide x 20/40' long ISO dry cargo containers, reefer containers and flat racks. GFC may be Government-owned or leased containers.

1.7.2 The contractor shall provide a chassis for GFC shipments, unless this requirement is waived by the local shipping/receiving facility or custom of the trade does not normally call for the use of chassis.

1.7.3 The contractor shall be liable for loss or damage to the GFC resulting from the contractor's negligence while in the contractor's possession.

1.7.4 Contractor has the right to refuse a GFC for shipment if it is not properly numbered, or if it does not comply with ISO, IMO and CSC Standards unless it is booked as breakbulk. Before making any changes to improperly numbered containers, the Contractor shall coordinate with cognizant COR. When a GFC is booked as breakbulk, the contractor does not have the right to refuse the shipment.

## **1.8 Hazardous Cargo**

The Government will package, prepare, mark/label and certify all hazardous materials in accordance with Air Force Manual (AFMAN 24-204), International Civil Aviation Organization (ICAO) Directives, International Maritime Dangerous Goods Code (IMDGC) and Code of Federal Regulations, Title 49 (49 CFR). Cargo may include hazardous material Classes 2 through 9 as defined in the International Air Transportation Association (IATA) Dangerous Goods Regulation. If cargo does not comply with aforementioned regulations, the contractor may refuse to transport noncompliant hazardous cargo.

## **1.9 Scheduling**

1.9.1 The contractor shall provide and maintain vessel schedules in Integrated Booking System (IBS) prior to submission of the Contractor's offer for offers that require ocean movement.

1.9.2 The contractor shall provide the Voyage Document Number (VOYDOC) and/or flight itinerary as specified

in the RFQ.

1.9.3 The contractor shall provide the subcontractor name and any additional information requested by the Contracting Officer if actual carriage of cargo is not performed by the prime contractor.

1.9.4 Vessel schedule or flight itinerary changes that occur prior to scheduled departure may result in cancellation of booked cargo at no cost to the Government.

#### **1.10 Cargo Available Date**

1.10.1 This is the date cargo is available to be picked up from the shipper. RFQs may require cargo to be picked up within an established number of days from the available date. In those situations, the contractor shall pickup all cargo within the timeframe established in the RFQ and the accepted booking.

1.10.2 When a Required Pick-up Date is provided in the RFQ, the Contractor shall pick-up all cargo before or on the date listed.

1.10.3 Contractor shall coordinate pick up dates/times directly with shipper at least 24 hours prior to available date but making contact after receipt of award is preferred.

1.10.4 The contractor shall pick up cargo at Afghanistan origins within the specified number of days in the accepted booking.

#### **1.11 Providing Empty Containers to Shippers**

##### **1.11.1 Spot Date**

At least 24 hours prior to the spot date annotated in the booking, the contractor shall notify the cognizant Ordering Officer and shipper of any containers, which cannot be spotted to meet booking requirements.

##### **1.11.2 Drop and Pick Service**

1.11.2.1 When requested by the Ordering Officer, the contractor shall provide drop and pick service or round robin drop and pick which shall be included in the contractor's rate.

1.11.2.2 The contractor shall spot the requested equipment at the location on or before the date and time specified in the booking.

#### **1.12 Perishables Transportation**

1.12.1 Upon discharge at the POD, the Contractor will be responsible for the unstuffing, storage, preparation, aircraft loading/unloading and final delivery of perishables.

1.12.2 The Contractor must perform all unstuffing, storage and preparation actions at a VETCOM-approved facility and have the proper equipment and personnel necessary to be self-sufficient. The Contractor shall ensure that all cargo is properly and safely prepared for shipment to final destination and adhere to all Required Delivery Dates (RDDs) specified in the bookings.

1.12.3 The Contractor will stage cargo in a secured facility/location until airlift. Customs clearance, transportation to the aircraft, loading/unloading of cargo to/from the aircraft and final delivery to the consignee shall be performed by the Contractor.

1.12.4 Cold chain requirements: The Contractor shall be responsible for proper product storage, segregation and delivery in acceptable condition.

1.12.5 In order for frozen items to be accepted, the following criteria must be observed:

1. Packages must be solid, not soft, upon arrival;
2. Container and wrapping must be intact, not damaged, and in a solid condition;
3. Packages must be free of drop and show no evidence of thawing and re-freezing (i.e. watermarks on boxes, off odor) or dehydration;
4. Cello wrapped packages must not be discolored or show other signs of freezer burn.

1.12.6 The Contractor shall maintain temperature- for all freeze, protection-from-heat and chilled cargo throughout the transportation process to include but not limited to, unstuffing, storage, preparation, aircraft loading/unloading and delivery processes in accordance with the temperature range and variance specified in the IBS booking. As a general guide:

1. Freeze items must be maintained at 0 degrees F;
2. Protection-from-heat items must be maintained below 70 degrees F;
3. Chilled items must be maintained at 32-40 degrees F;
4. Ice cream must be maintained at -10 to 0 degrees F.

1.12.7 DLA Prime Vendors are the primary shippers of perishable cargo under this contract. Further requirements for Prime Vendors are identified in Attachment 6.

### **1.13 Pre-Alert Notification**

1.13.1 No later than (NLT) 12 hours prior to arrival, the contractor shall provide the destination Aerial Port with the cargo arrival date, time, and quantity.

1.13.2 The contractor shall provide the contact information for a contractor representative, who is fluent in English, and available in person or via telephone during aircraft or truck arrival or departure. This representative shall be responsible for providing necessary information and coordinating with Government personnel and have the full authority to react to and effect necessary changes.

### **1.14 Required Delivery Date (RDD)**

1.14.1 The contractor shall deliver all cargo by the RDD specified in the accepted booking.

### **1.15 Delivery Notification and Receipt**

1.15.1 The Contractor shall schedule a date and approximate time for all deliveries with the consignee or consignee's agent at least 2 working days prior to any actual delivery of cargo. Does not apply to shipments to Afghanistan.

1.15.2 The Contractor shall not deliver cargo on the same day as notification unless approved by the consignee. Does not apply to shipments to Afghanistan.

1.15.3 The Contractor shall deliver cargo on a specific day if requested by the consignee provided the contractor can accommodate the request using the contractor's normal service.

1.15.4 The Contractor shall provide a delivery receipt for the consignee or consignee's agent to sign to acknowledge receipt of the containers or pieces and to annotate any exceptions.

1.15.5 The Contractor shall display a placard on the cargo or conveyance with identifying marks where required by local practice.

1.15.6 A signed delivery receipt with no damage noted does not preclude the Government from pursuing a claim for damages discovered after delivery. If damage is later discovered, the Contractor will be notified and requested to

survey cargo.

1.15.7 Delivery receipt shall contain the following information: carrier, Port Call File Number (PCFN), IBS, Transportation Control Number (TCN), container number (if applicable), consignee DoDAAC, final destination location, truck number, driver name, date cargo arrived at final destination, date/time cargo in-gated at final destination, date/time cargo off-loaded at final destination, printed consignee name, consignee's signature, remarks section. Additional information may be included as necessary. The Contractor shall maintain a copy of the delivery receipt.

#### **1.16 Concept of Operations (CONOPS)**

1.16.1 The contractor shall provide a complete CONOPS report 14 days prior to available date for every task order and booking awarded. CONOPS shall be provided to the Contracting Office.

1.16.2 Upon Government request, the Contractor will provide a complete CONOPS report to SDDC for review prior to cargo being booked. CONOPS requirements will be provided at time of the request.

#### **1.17 Operational Reports**

The Contractor shall submit specific cargo movement information in accordance with the requirements outlined in Attachment 4.

#### **1.18 Booking Reconciliation Tool (BRT)**

1.18.1 The Contractor shall submit any booking modification requests via BRT for cargo booked in IBS. BRT is a module of the Pipeline Asset Tool (PAT).

#### **1.19 Cargo Clearance (Sealift)**

1.19.1 The responsibilities for cargo clearance under this contract are shared between the Contractor and the Government.

1.19.2 For cargo entering via seaports/airports in the countries listed in Table 1.19.2 below, the Government has principal responsibility for cargo clearance and performs the majority of tasks incident to clearance. These include the preparation of documents or entry into automated systems but, by local practice, the Government may require the Contractor to perform tasks such as document pickup and delivery, presentation of documents to appropriate officials and payment of processing fees.

1.19.2.1 Costs incurred by the Contractor to provide these incidental services shall be included in applicable pricing.

1.19.2.2 Table 1.19.2 is a list of locations where the Government has principal responsibility for cargo clearance.

| <u>Table 1.19.2</u>                       |
|-------------------------------------------|
| United States territories and possessions |
| Kuwait                                    |

1.19.2.3 Government Arranged Cargo Clearance.

1.19.2.3.1 Government (shipper) prepares a cargo clearance documents, including customs clearance paperwork. (Does not include any contractor provided documents).

1.19.2.3.2 Government may submit to customs or give to the contractor for the contractor to combine with contractor documents (such as a bill of lading) and deliver to customs officials, pay minor processing fees, obtain approvals and notify any other stakeholders when clearance is approved.



1.19.3 Contractor-Arranged Cargo Clearance: Contractor acts on behalf of Government to complete all necessary clearance actions.

1.19.3.1 When Contractor-Arranged Cargo Clearance is ordered by the Government, the Contractor has principal responsibility for customs clearance in addition to cargo clearance.

1.19.3.2 Contractor-Arranged Cargo Clearance, as required by local practice, includes these additional services:

1.19.3.2.1 Coordinate with shipper/consignee and local customs authorities to obtain and/or prepare (except for signature) all necessary documentation for both customs and cargo clearance;

1.19.3.2.2 Provide prepared forms/documents to receiver/Government for signature;

1.19.3.2.3 Deliver documents to the customs office, and ensure that documentation is provided to all local entities as required to permit release and on-carriage of cargo to final destination.

1.19.4 Additional countries may be added to Table 1.19.2 should it be determined that the Government has increased its presence in a country, and that the Government shall provide clearance services as described by 1.19.2.

1.19.5 Countries shall be removed from Table 1.19.2 via bilateral modification should it be determined that the Government has decreased its presence in those countries, and that the Government can no longer provide clearance services as described by paragraph 1.19.2.

1.19.6 The shipper will provide the Contractor with appropriate shipper generated customs documents in a timely manner.

1.19.7 Notification of Cargo Held by Customs

1.19.7.1 The Contractor shall promptly notify the cognizant COR and SDDC Battalion within 24 hours if cargo is held up by customs, or if the local authorities require direct Government intervention for either cargo or customs clearance.

1.19.8 The Contractor will ensure that cargo remains within designated customs free zones and/or that cargo remains customs cleared by host nations. The contractor will be required to coordinate all activities with the host nation to implement the requirements in this work statement to include duty-free customs clearance, transit and landing rights as ordered by the Government.

## **1.20 Prior Permission Required (PPR) Process**

1.20.1 The Government will provide the Contractor with all cargo data necessary for the completion of aircraft clearance including customs, and similar documents. The Contractor shall retain responsibility for furnishing appropriate agencies all required manifest, and border clearance documents, covering all cargo aboard the aircraft upon entry into the foreign country. The Contractor shall also be responsible for payment of any charges, fees, or taxes based upon use of terminal facilities by or for cargo. The Government is not obligated to pay, or reimburse the Contractor for payment, of any such charges. The International Flight Information Manual (IFIM) in conjunction with the host nation's Aeronautical Information Publication (AIP) includes the process and/or points of contacts for obtaining civilian clearances. When a foreign country requires that a carrier under contract to USTRANSCOM submit a clearance request through US diplomatic channels for approval, this fact, along with the procedures to be followed, will be noted in the DOD Foreign Clearance Guide (FCG), DoD 4500.54-M, <https://www.fcg.pentagon.mil>. Contractors shall adhere to the guidelines outlined in this appendix when operating missions under this contract that require clearances to be submitted through US diplomatic channels and shall consult the DOD Foreign Clearance Guide for specific US Defense Attaché Office (USDAO) requirements or country restrictions to supplement IFIM and AIP requirements. Contractors can obtain a user name and password for access to the on-line FCG by contacting HQ USAF/A5XP by e-mail at [fcg@pentagon.af.mil](mailto:fcg@pentagon.af.mil) or by calling (703) 614-0130.

1.20.2 The Contractor shall adhere to the theater application process and operate in accordance with the approved PPR. It is the Contractor's responsibility to be aware of all airfield restrictions outlined in the NOTAMS. NOTAMS can be found at the following website: <https://isfcc.ncia.nato.int/default.aspx>.

1.20.3 Contractor will obtain PPRs prior to each airlift mission through the United States Central Command Deployment Distribution Operations Center (CDDOC) or respective airfield managers. Additional information on airfield slot times for all strategic, fixed-wing flights can be obtained from the following website: <https://isfcc.ncia.nato.int/default.aspx>.

1.20.4 In the event the Contractor cannot comply with the approved PPR, the Contractor shall immediately coordinate with the local airfield manager and the CDDOC.

1.20.5 The Contractor is responsible for obtaining necessary landing rights or privileges and visas, passports, restricted area passes and gate passes for crews, route support personnel and Contractor employees to ensure total compliance with all local security requirements.

1.20.6 The Contractor shall comply with all International Overflight Requirements.

## **1.21 Restrictions on Subcontracting to Air Contractors**

1.21.1 The Contractor shall not use air contractors listed on the European Banned Carrier Listing at [https://ec.europa.eu/transport/modes/air/safety/air-ban\\_en](https://ec.europa.eu/transport/modes/air/safety/air-ban_en), the Excluded Parties Listing, at <https://www.sam.gov/portal/public/SAM/>, and the Department of Treasury: Office of Foreign Assets Control, Special Designated Listing at <http://www.ustreas.gov/offices/enforcement/ofac/sdn/>.

## **1.22 Sexual Harassment/Assault Response & Prevention (SHARP)**

1.22.1 Sexual Assault and Sexual Harassment Policy. The Contractor shall ensure all employees performing work in Afghanistan shall comply with the Sexual Assault and Sexual Harassment Policy outlined in Attachment 9.

1.22.2 Sexual Harassment Policy Compliance: The Contractor shall certify that all employees performing work under this contract in Afghanistan shall have been fully trained per the requirements in Attachment 9 and in their own language. The contractor shall provide the COR an annual certification stating all employees performing in Afghanistan have been fully trained per the requirements herein.

1.22.3 The Contractor shall conduct training of all employees performing in Afghanistan annually to prevent sexual assault and sexual harassment.

1.22.3.1 This training must, at a minimum, ensure that all the Contractor employees performing work in Afghanistan understand the definitions and policy outlined in Attachment 9.

1.22.4 Each employee performing work in Afghanistan shall be in compliance with the training requirement and shall be reported to the Contracting Officer Representative prior to the employee being allowed access to the worksite.

1.22.5 The Department of Defense has adopted a policy to prevent sexual assault and sexual harassment. Contractors and contractor employees in Afghanistan shall not –

1.22.5.1 Commit acts of sexual assault against any person on any camp, post, installation, or other United States enclave; or

1.22.5.2 Sexually harass any person on any camp, post, installation, or other United States enclave.

1.22.6 The Contractor shall enforce standards for discipline, appearance, conduct, and courtesy IAW the published CENTCOM, USFOR-A and/or Base Commander Standards. For Contractors at Bagram Airfield (BAF) or for

contractors transiting BAF, they must abide by the Commander Bagram Airfield (COMBAF) Standards of Conduct while performing at any level (prime or subcontractor) on BAF and any other installation and facility for which COMBAF standards are applicable, and as designated applicable to contractor personnel. COMBAF Standards are available from the COR.

### 1.23 Good Order and Condition

Cargo shall be delivered to the consignee in the same order and condition as when turned over to the Contractor for shipment.

### 1.24 Invoice Submission

Final invoices may be submitted only after services included on the invoice have been satisfactorily performed (Ref FAR 32.905). Final invoices with proper documentation shall be submitted to SDDC G8 within the timelines established in Attachment 2– Invoicing and Payment.

## SECTION 2 PERFORMANCE MEASURES

### 2.1 Performance Requirements

All cargo booked under this contract shall be moved in accordance with the terms of the contract. The Government strategy for assessing the Contractor's performance under this contract focuses on two business lines: Unit Moves and Other Than Unit Moves (OTUM). Contractor performance will be measured for each geographical lane they service (e.g. NORTCOM to CENTCOM), separated by Unit Moves and OTUMs using the PAT Carrier Performance Portal (CPP). Contractors should request access to PAT CPP to manage and track performance.

### 2.2 Performance Measures and Performance Standards

To evaluate the contractor's success in meeting the stated Performance Objectives, the Government will monitor and measure contractor performance under this contract using the Performance Measures identified in **Table 2.2**. There may be more than one Performance Measure for a single Performance Objective. Data points for Performance Objectives 1 and 2 represent one container or piece of cargo as booked.

| <b>Table 2.2</b>                    |                        |                                                                                                                              |                            |               |                               |
|-------------------------------------|------------------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------|-------------------------------|
| <b>Performance Objective</b>        | <b>Description</b>     | <b>Performance Measure</b>                                                                                                   | <b>Performance Average</b> | <b>Weight</b> | <b>Performance Assessment</b> |
| <b>1</b>                            | Required Delivery Date | Cargo shall be delivered not later than the Required Delivery Date as accepted in the booking.                               | $x\%$                      | $0.75$        | $x * .75$                     |
| <b>2</b>                            | In-transit Visibility  | The Contractor shall provide to the Government accurate EDI transactions required by Section 2 within 24 hours of the event. | $y\%$                      | $0.25$        | $y * .25$                     |
| <b>Contractor Performance Score</b> |                        |                                                                                                                              |                            | <b>1.00</b>   | <b>Total %</b>                |

### 2.3 Performance Objectives

#### 2.3.1 Performance Objective No. 1: On-Time Delivery

2.3.1.1 The Contractor shall deliver the cargo no later than the Required Delivery Date (RDD) specified in the accepted booking.

2.3.2 Performance Objective No. 2: ITV

2.3.2.1 The Contractor shall provide accurate and timely shipment status reports using the Electronic Data Interchange (EDI) as required by SECTION 5.

Required transactions for containers: W, I, AE, VD, VA, UV, OA, X1, RD/EC

Required transactions for breakbulk: W, I, AE, VD, VA, UV, OA, X1

Required transactions for Movements Not Booked within the SDDC IBS System: W, I, VD, VA, OA, and X1

2.3.2.2 Although required, RD or EC will not be measured with the other required EDI transactions, the Government recognizes that in some cases RD submission may occur after or before shipment RDD.

2.3.2.3 The event transactions I, VD, VA, and OA must be submitted for each air and sea leg. For example, if the shipment is booked with both a sea leg and an air leg then there would be two sets of the above transactions. However, if it is just a sea leg or an air leg, then there would be only one set of the transactions.

2.3.2.4 The ITV performance objective is calculated based on a weighted score of EDI submission considered at 50% weight and submission timeliness considered at 50% weight. Each transaction will be independently measured. For example, if the Contractor submits the twelve required transactions but only nine are timely, the Contractor would receive 87.5%  $[(.5(12/12) + .5 (9/12)]$  credit for ITV on that shipment.

2.3.2.5 The ITV measure is independent of the on-time delivery performance measure; although failure to submit an X1 transaction will be considered equivalent to a missed RDD, unless conditions described in SECTION 5 apply. In either case, X1 is a mandatory EDI transaction for all shipments.

**2.4 Performance Objective Assessment**

2.4.1 CPP Procedures for Monthly Scorecards

2.4.1.1 On the 1st calendar day of every month, the Contractor will review its performance data for the previous month using the History tab under Historical Reporting in CPP. EDI transaction will be accepted in CPP until the 5th calendar day of the month. Contractors may submit for credit in CPP for timeliness, submission, on time delivery and exclusions until the 8th calendar day.

2.4.1.2 On the 20th calendar day of the month, the Contractors may view their monthly scorecard in CPP. Contractors will have 4 additional calendar days to dispute any discrepancies in performance assessment data with the SDDC HQ CORs.

2.4.2 The SDDC HQ COR will coordinate with the Contractor to attempt to resolve disputed performance assessment data prior to the posting of the Monthly Performance Rating. The Government will accomplish audits of contractor submitted performance data to ensure accuracy.

**2.5 Performance Rating**

2.5.1 The Contractor's Performance Rating will be assigned for each geographical lane they service; separated by Unit Moves and Other than Unit Moves (OTUM).

2.5.2 The performance ratings are provided in Table 2.5 below.

|                  |
|------------------|
| <b>Table 2.5</b> |
|------------------|

| Rating                              | Definition                                                                                                                                                                                                                  |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Exceptional                         | 95% - 100%                                                                                                                                                                                                                  |
| Very Good                           | 90% - 94.9%                                                                                                                                                                                                                 |
| Satisfactory                        | 85% - 89.9%                                                                                                                                                                                                                 |
| Marginal                            | 78% - 84.9%                                                                                                                                                                                                                 |
| Unsatisfactory                      | 77.9% and under                                                                                                                                                                                                             |
| Neutral/Unknown<br><i>No Volume</i> | Has an Initial- Neutral/Unknown rating for the month and meets all other contractual requirements. No CDRs issued. Please note a Neutral/Unknown rating will not be evaluated favorably or unfavorably on past performance. |

2.5.3 For purposes of evaluating and awarding task orders, the Government will utilize a two-month rolling average of the Performance Ratings referenced above. The rating used for evaluating and awarding task orders will become effective one month after performance has ended for a particular month. For example, the two-month rolling average for the months of September and October will become effective on the first day of December. A month's rating will be utilized for all RFQ's closing in the same month. For example, January's ratings will be used for all RFQ's with a close date in January.

2.5.4 In the event the performance ratings are not complete in sufficient time for them to be utilized in an award decision, the Contractor's Performance Rating from the previous month shall be used for those decisions. Once the Performance Rating for the month have been established, they will be utilized for future award decisions.

#### 2.5.5 Quality Control

2.5.5.1 The Contractor shall promptly notify the cognizant Contracting Officer Representative (COR) of any problems or failures that may affect performance. The COR may issue a Contract Discrepancy Report (CDR) when the Contractor fails to meet the terms and conditions of the contract. Upon request, the Contractor shall provide the COR with a written plan of corrective action, including a proposed timeline, within 10 business days after the request. This plan shall describe proposed Contractor actions to correct the problem or deficiency and bring performance back in compliance with identified performance standards and shall be on the Contractor's official letterhead.

2.5.5.2 The Contracting Officer may issue a Cure Notice when the Contractor fails to meet the terms and conditions of the contract. The Contractor shall provide the Contracting Officer with a written plan of corrective action, including a proposed timeline, within 2 business days of receiving the Cure Notice. The response shall be submitted on the Contractor's official letterhead.

## **2.6 Limited Use**

2.6.1 The Contractor may be put into limited use status by the Contracting Officer for service failures including, but not limited to, the following:

1. Unauthorized deviations to CRAF or VISA preference submitted in the RFQ when the change was not due to the fault of the Government. This includes Cargo Preference violations.
2. Lost/damaged/pilfered shipments exceeding 0.5% of all shipments during any three month period.

2.6.2 The Contractor will be notified via a letter issued from the Contracting Officer that the Contractor is in jeopardy of being put on limited use. The letter will outline, at a minimum, the reason the Contractor is being considered for limited use status, the proposed amount of time of the limited use status, and any other pertinent information.

2.6.3 The Contractor shall respond with a remedy to the issue. If the Contracting Officer determines the remedy is insufficient the Contractor will be notified in writing they are officially in limited use status.

2.6.4 Contractors in limited use status may only be offered bookings if no other contractor is available or if no other contractor has equal or higher flag service available.

## **SECTION 3 EXCEPTIONS TO NORMAL SERVICE**

### **3.1 Cancellation/No Show**

3.1.1 The Government may unilaterally cancel the Multimodal booking without penalty, provided notification is given to the Contractor. The Government will provide cancellation notice at least 24 hours prior to scheduled pickup at origin. Special situations shall be addressed by the Contracting Officer.

3.1.2 The Contractor shall notify the cognizant COR of cargo not tendered to the Contractor in time to meet the booked departure that has not been cancelled or rebooked.

### **3.2 Cargo Rolls**

3.2.1 For cargo that misses the booked departure through no fault of the Contractor, the Contractor shall move cargo on the next scheduled departure after receipt of cargo from the Government. Contractor shall notify shipper and origin OO at time of occurrence and request a cargo roll using the Pipeline Asset Tool (PAT), Booking Reconciliation Tool (BRT).

3.2.2 When the Government notifies the Contractor cargo is not available for a booked movement, the Contractor shall then designate a new vessel, aircraft, or other mode of conveyance based on the revised availability of cargo. Should the rolled cargo not show for the follow on designated departure, the booking shall be cancelled and the cargo rebooked.

3.2.3 The Contractor shall in no event hold the Government liable for demurrage, dead freight or associated charges by failing to release cargo in time to meet a specified pickup.

### **3.3 Rerouting of Cargo**

Any changes in the booked routing must be coordinated with the Ordering Officer. Delays due to route changes made by the Contractor will not result in additional monetary compensation. If the Government reroutes cargo compensation will be negotiated with the Contracting Officer on a case-by-case basis.

### **3.4 Broken/Replacement of Seals**

The Contractor shall notify the Shipper, Ordering Officer, and COR electronically within 24 hours of discovery that

cargo has been tampered with and if a seal on unit cargo has been broken and/or replaced while the cargo is in the possession of the Contractor. A complete written report of the circumstances and reasons shall be provided to the cognizant COR.

### **3.5 Transportation Discrepancy Reports (TDR)**

Except in relation to claim processing timelines (including but not limited to Defense Transportation Regulation (DTR), Volume II, Chapter 210, paragraph F.1.a.(1)), the Government will process cargo claims in accordance with the DTR, Volume II, Chapter 210. The Contractor agrees to cooperate with Government efforts to resolve claims for loss or damage to Government cargo."

### **3.6 Containerization for the Convenience of the Contractor**

For breakbulk cargo booked by the Government, the Contractor may, in its discretion, containerize such cargo for operational convenience without any additional cost or expense to the Government. However, breakbulk cargo containerized for Contractor's convenience must be de-containerized and made available for customer pick up within 2 working days after discharge, and is considered breakbulk cargo.

### **3.7 Live Load / Unload**

3.7.1 The Contractor shall provide live load and/or live unload service at the origin and/or destination as follows:

3.7.1.1 When agreed to by the shipper when the Contractor schedules pickup.

3.7.1.2 When agreed to by the receiver when the Contractor schedules delivery.

3.7.2 The Contractor and the shipper/receiver shall set a live load/unload appointment (date and time and specific location). In the event the Contractor arrives 15 minutes or later after the agreed time, the shipper/receiver may load/unload the cargo immediately or reschedule the loading/unloading for a later time. Shippers/Receivers may also cancel the appointment and reschedule for a different day at no additional cost to the Government.

3.7.3 When indicated in the RFQ, the Contractor shall pick up empty Government owned or leased containers from locations separate from the designated loading location and deliver them to the shipper for loading. The Contractor shall include the cost of this service in their offer. The container shall be spotted at the shipper's location using rules for live load, drop and pick or pool as would apply for a contractor provided container.

3.7.4 Shipments delivered with evidence of tampering or loss shall be investigated by base security; drivers may be detained for questioning by base security. If investigation determines no tampering occurred, applicable wait time rates will be paid. If the investigation determines that tampering/pilferage has occurred, driver wait time will not be payable.

### **3.8 Defense Logistics Agency-Energy Ground and Aviation Fuel**

3.8.1 Defense Logistics Agency - Energy (DLA-E) Ground and Aviation Fuel. If the Contractor is authorized to purchase fuel from DLA-E, a Fuel Purchase Agreement (FPA) must be completed. DD Form 1896 DOD Fuel Identaplates will be prepared for the prime contractor (carrier) and the prime contractor may distribute the identaplates out to their respective subcontractor(s). The identaplate will reflect the prime contractor's DoDAAC account and other information needed by the contractor to identify their subcontractor. It is the responsibility of the prime contractor to manage and account for the identaplates. Cash purchases are not authorized. Payment for fuel is a contractor responsibility and is not a reimbursable expense.

3.8.2 If DLA-E fuel supply levels become a concern, the Government reserves the right to restrict the amount of fuel to be uplifted or rescind the Contractor's ability to purchase DLA-E fuel.

3.8.3 Additional information can be found at <http://www.desc.dla.mil/dcm/files/desc-i-3.pdf>.

## **SECTION 4 ACCESSORIALS**

The following accessorial services, when required, will be ordered in the RFQ and should be priced into the Contractor's all inclusive price per pound rate. Any required accessories not listed below will be included in the special instructions in the RFQ.

### **4.1 Cargo Concealment**

4.1.1 When service is ordered, the Contractor will conceal/cover any non-containerized cargo that is in the open on a given conveyance. The Contractor shall provide necessary material to cover cargo completely so that the cargo is concealed from view while being transported. Concealment materials shall be weather resistant, non-transparent and shall remain secured and in place during the complete transit of cargo. The Contractor shall repair or replace any material used for concealment if damaged in transit. In addition, concealment material shall remain on the cargo until final destination unless otherwise directed by the Government. The Contractor shall be responsible for the removal and the disposal of such material, unless otherwise directed by the Government.

4.1.2 Concealment material may include tarps, crates, and any other material deemed necessary, by mutual agreement between the Contractor and the Ordering Officer. The Government may request specific material depending on the nature of the cargo.

### **4.2 Exterior Cargo Rinsing Service**

4.2.1 The purpose of cargo rinsing service is to remove road dirt and other contaminants from cargo that was cleaned and found to be acceptable for entry into the US prior to tendering to the Contractor. Contractor shall clean cargo to a condition acceptable for entry.

4.2.2 Includes costs to move cargo to the rinse facility or to move rinse equipment to the cargo.

4.2.3 The Contractor may choose where to perform the rinsing service unless location is specifically directed by the Ordering Officer.

4.2.4 Contractor shall re-rinse cargo at POD if rejected by customs/agriculture authorities, at no cost to the Government if it is determined that rejection occurred at fault of the Contractor.

4.2.5 For cargo containerized by the Government, rinsing service applies to exterior of container. For cargo containerized at contractor's convenience, rinsing applies to exterior of cargo.

### **4.3 Exterior Cargo Washing Service**

4.3.1 All cargo entering the US must be free from contaminated soil and pests. "Cargo will not be loaded aboard a final conveyance in a foreign country, for movement to the US, unless it is free of animal and plant contamination or pest infestations as required by the US Port of entry Customs Border Protection-Agriculture Inspection Service officials (CBP-AIS) and USDA Animal and Plant Health Inspection Services (APHIS)." Washing of cargo must comply with the following: 7 CFR 330.300, Defense Transportation Regulation (DTR) 4500.9R, Part V, Chapter 502, 505, and Chapter 506. Detailed cleaning and inspection procedures can be found in the Armed Forces Pest Management Board Technical Guide No. 31, Contingency Retrograde Wash-downs: Cleaning and Inspection Procedures.

4.3.2 Accessorial Rate includes costs to move cargo to the wash facility or to move the wash equipment to the cargo.

4.3.3 The Contractor may choose where to perform the washing service, unless the location is specifically directed by the Ordering Officer.

4.3.4 When washing services are ordered, Contractor shall re-wash cargo at POD if rejected by



customs/agriculture authorities at no cost to the Government if it is determined that rejection occurred at fault of Contractor.

4.3.5 For cargo containerized by the Government, washing service applies to exterior of container. For cargo containerized at contractor's convenience, washing applies to exterior of cargo.

#### **4.4 Interior Cargo Washing Service**

4.4.1 The vehicle cab and all interior storage and tool compartments must either be swept, compressed air cleaned, sprayed with water, and/or wet/dry vacuumed; including the floor, under the seats, trunk, spare tire & spare tire well. When utilizing water pressure machines or steam to clean, cover the dashboards and areas where electronics may be damaged with plastic or other protective lining prior to starting. The focal point of the interior cleaning should be the floorboard area, including lower compartments utilized for storage where most soil accumulates. Interior must be cleaned to USDA Standards.

4.4.2 Upon tender to the Contractor, the vehicle will be free from all contraband to include weapons, ammunition and classified material. Contractors may refuse to accept cargo from the government/shipper if cargo is not free of these materials.

4.4.3 Accessorial Rate includes costs to move cargo to the wash facility or to move the wash equipment to the cargo.

4.4.4 The Contractor may choose where to perform the washing service, unless the location is specifically directed by the Ordering Officer.

4.4.5 When washing services are ordered, the Contractor shall re-wash cargo at POD if rejected by customs/agriculture authorities, at no additional cost to the Government, if it is determined that rejection occurred at fault of Contractor.

#### **4.5 SECURITY (PHYSICAL, PERSONNEL, INFORMATION, ANTITERRORISM / FORCE PROTECTION AND INDUSTRIAL) General Security Information**

The majority of daily work associated with this PWS is at the unclassified level, but contractor personnel may be required to access classified information at the SECRET level; classified areas, or transport classified military equipment during performance of this contract / task order.

#### **4.6 Additional Security Requirements (Transportation Security)**

Contractors shall adhere to Defense Transportation Regulation, Part II, Chapter 205. Only carriers with a valid Facility Clearance Level (FCL) at the SECRET level are authorized to transport classified materials. The FCL can be an interim, but whether an interim or final FCL, it must be valid at the time of award and granted by the Defense Security Service.

#### **4.7 Citizenship and Clearance Requirements**

Only contractor employees that are U.S. citizens are able to have security clearances and access classified information, classified areas, and classified systems.

#### **4.8 Security Clearance Requirements**

Some positions on this task order (contract) require a minimum of a SECRET clearance as granted by the Vetting Risk Operations Center (VROC) or a completed adjudication of SECRET granted by the DoD Consolidated Adjudication Facility (CAF).

#### **4.9 Facilities Clearance (FCL)**

Only contractor employees with a personnel security clearance working for contractor companies with a facility clearance granted by the Defense Counterintelligence and Security Agency (DCSA) Facility Clearance Branch are eligible for access to classified information. The contractor must have a valid FCL at the SECRET level. Interim FCLs are acceptable provided they are not expired. FCL procedures and security guidelines for adjudicative requirements are outlined in DOD 5220.22-M

#### **4.10 Access to Scott Air Force Base or USTRANSCOM Facilities.**

Contractor employees visiting Scott AFB, IL and USTRANSCOM for periodic carrier or other meetings must send an electronic visit request in Defense Information System for Security (DISS). DISS visits can be forwarded to the Security Management Office (SMO) code USTC-SDDC. The visit request shall annotate the purpose of the visit; POCs by name and phone number; visit date(s) and the contract or task order number. Entrance into USTRANSCOM building 1900 will be via the breezeway between 1900E and 1900W. The contractor visitors must come to the Protection Services Center for validation of their clearance and visit request. Temporary badges or escort required badges will be issued based on access eligibility

#### **4.11 Classified Information at Contractor Headquarters**

No classified information obtained by contractor visitors at USTRANSCOM can be taken from USTRANSCOM back to the contractor company headquarters unless that specific CAGE code location has been granted safeguarding by DCSA. No contractor employee will hand-carry classified information from USTRANSCOM back to the contractor's location without written approval from USTRANSCOM/TCJ34. If authorized, the contractor courier must be briefed on responsibilities to safeguard the information and have a signed USTRANSCOM courier letter in his or her possession.

#### **4.12 Classified Meetings**

Visitors are required to follow the USTRANSCOM guidelines for attending classified meetings.

#### **4.13 Derogatory Information**

If USTRANSCOM notifies the contractor that the employment or the continued employment of any contractor personnel is prejudicial to the interests or endangers the security of the United States of America, that employee shall be removed and barred from performing on this contract. This includes security deviations/incidents and credible derogatory information on contractor personnel during the course of the contract period of performance. Personnel who have incident reports posted in DISS will be denied the ability to support the contract until the issues have been resolved and the incident has been removed in DISS. The contractor shall make any changes necessary in the appointment(s), at no additional cost to the Government. If any incident involves or may involve the mishandling of classified information or a potential Negligent Discharge of Classified Information, the USTRANSCOM Protection and Response office (618-220-6554) will be notified within 24 hours during the normal work week and within 72 hours if the incident occurs over the weekend.

#### **4.14 Security Regulation Guidance:**

**DoD:** (DoD issuances found at: <http://www.dtic.mil/whs/directives/corres/pub1.html>):

O-2000.16 (DODI Antiterrorism (AT) Standards), Vol 1, 17 November 2016

DoD 5200.02, Personnel Security Program, 17 April 2017

DoD 5200.08-R, Change-1, DoD Physical Security Program, May 27, 2009

DoDO 2000.16, DoD Antiterrorism (AT) Standards, Vol. 1, November 17, 2016

DoDI 5200.02 DODM Procedures for the DOD Personnel Security Program

DoDI 5220.22, National Industrial Security Program Operating Manual (NISPOM), 18 May 2016

DoDI 8500.01, Cybersecurity, March 13, 2014

DoDM 5200.01 VOL. 1, DoD Information Security Program: Overview, Classification, and Declassification, 24

February 2012

DoDM 5200.01 VOL. 2, DoD Information Security Program: Marking of Classified Information Summary of Changes, CH 2, 19 March 2013

DoDM 5200.01 VOL. 3, DoD Information Security Program: Protection of Classified Information Summary of Changes, CH 2, 19 March 2013

DoDM 5200.01 VOL. 4, 2/24/2012 DoD Information Security Program: Controlled Unclassified Information (CUI) Summary of Changes, 24 February 2012

DTM 08-027, Change-1, Security of Unclassified DoD Information on Non-DoD Information Systems, September 16, 2010

DoD 4500.9.R, Part II, Appendix E, Defense Transportation Regulations

**USTRANSCOM:**

USTRANSCOM Instruction 31-02 (USTRANSCOM Security Classification Guide)

USTRANSCOM Instruction 31-12 (Operations Security - OPSEC)

**FORMS:**

DD Form 254, DoD, Contract Security Classification Specification

**Contractor Facility Security Officer (FSO):**

The prime contractor will forward the name, address, email address and telephone number of the Company FSO and backup to USTRANSCOM Force Protection (Industrial Security) at time of award and if any changes occur.

**4.15 USTRANSCOM Force Protection (Industrial Security) Points of Contact:**

USTRANSCOM

Attn: TCCS-PR

508 Scott Drive

Scott AFB IL 62225

Email: [transcom.scott.tccs.mbx.industrial-security@mail.mil](mailto:transcom.scott.tccs.mbx.industrial-security@mail.mil)

**4.16 SDDC G2 Security Office (Industrial Security) Point of Contact:**

SDDC

Attn: G2 (Tony Cameron or Dave Stewart)

1 Soldier Way

Scott AFB IL 62225

Email at [standa.t.cameron.civ@army.mil](mailto:standa.t.cameron.civ@army.mil) or [david.l.stewart148.civ@army.mil](mailto:david.l.stewart148.civ@army.mil)

Group box: [usarmy.scot.sddc.mbx.g2-safb@army.mil](mailto:usarmy.scot.sddc.mbx.g2-safb@army.mil)

**4.17 Foreign Entity Vetting**

4.17.1 Subcontractor Suitability. Contractors shall complete and submit Attachment 10, Foreign Entity Vetting, to the Contracting Officer for each first tier foreign transportation service provider, operating as a separate legal entity, contracting directly with contractor or its commonly owned legal affiliate which has employees who may have physical contact with Government shipments in the ordinary course of contract performance. First tier foreign transportation service providers within scope include, but are not limited to: direct air and sea carriers, indirect air and sea carriers, freight forwarders, customs brokers, other brokers, stevedoring service providers, ramp personnel, ground handling services, railway operators, trucking companies, and courier services. The initial report is due 90 calendar days after contract award and every 6 months thereafter, no later than 15 January and 15 July each year. Each report shall include the service providers used during the previous 6 months.

4.17.1.1 The report shall include the following information:

4.17.1.1.1 Legal Company Name (in native language if known)

4.17.1.1.2 Complete Address including Country

4.17.1.1.3 Name, phone number and e-mail address of at least one point of contact at the company

4.17.1.2 The report shall include the following information if it is commercially available in the Contractor's system:

4.17.1.2.1 Any Previous or Alternate Company Names

4.17.1.2.2 Fax number

4.17.1.2.3 Website URL

4.17.1.2.4 International Civil Aviation Organization (ICAO) or equivalent designator

4.17.1.2.5 Owner(s)/Director(s) name(s) and e-mail address(es)

4.17.1.2.6 Manager(s) name(s) and e-mail address(es)

4.17.1.3 For all foreign air carriers that fall within the scope of the reporting requirement, Contractor shall provide a copy of the Air Operating Certificate. For foreign carriers that fall within the scope of the reporting requirement, Contractor shall provide a copy of business licenses required for the Contractor to legally operate in that country (e.g. Afghanistan Investment Support Agency (AISA) license when performance occurs in Afghanistan).

4.17.1.4 Contractor is not required to limit reporting solely to subcontractors used for services under the contract, but rather, may provide a complete list of subcontractors within scope in contractor's network. However, each report should only include information on the subcontractors used over the last 6 months.

4.17.1.5 The Contractor is responsible for appropriately marking sensitive information as proprietary/trade secret. The Government will handle proprietary/trade secret information within the applicable statutes, rules, and regulations regarding the handling and release of such information.

4.17.1.6 Periodically throughout contract performance, the Contracting Officer will make available to the Contractor the name of active or potential subcontractors determined to be unsuitable. The Contractor shall not allow named entities to perform any role in performance under this contract. If the Contractor chooses to terminate the unsuitable subcontractor, the Government shall not be liable for any costs incurred by the Contractor in establishing or terminating use of the unsuitable subcontractor. The Contractor may choose not to terminate the unsuitable subcontractor for use on its commercial contracts.

4.17.1.7 An unsuitable determination does not preclude the Contractor from nominating an unsuitable entity for reconsideration during the contract performance period. The Contractor is encouraged to provide the Contracting Officer additional relevant information that may affect the subcontractor's suitability. Any entity listed in the U.S. Government Consolidated Screening List ([http://export.gov/ecr/eg\\_main\\_023148.asp](http://export.gov/ecr/eg_main_023148.asp)) or otherwise prohibited per FAR Subpart 25.7, Prohibited Sources, will not be reconsidered.

#### **4.18 Electronic Systems Access**

The majority of business conducted under this contract requires the Contractor to access multiple modules within SDDC/TRANSCOM's Electronic Transportation Acquisition (ETA) System, such as the Integrated Booking System, and Business Support & Container Management Module. DODI 8520.02 and DODI 8520.03 shall govern Contractor's access to these systems; unless or until these DOD Instructions are amended to allow otherwise, the Contractor "shall use certificates issued by the DoD External Certification Authority (ECA) program or a DoD-approved PKI (Yubikey), when interacting with the DoD in unclassified domains." Contractors shall use ECA when possible and may use a DoD-approved external PKI (Yubikey) when ECA is not an option. Furthermore, contractors shall use multi-factor authentication as required by DODI 8520.03 which requires each user to have both a U.S. Government-provided user name and password as well as a non-PKI or PKI certificate/authenticator. Contractors must ensure compliance with system access standards as a requirement for doing business with the U.S. Government

and shall implement an identifying proofing/vetting process for ETA users in accordance with paragraphs 4.18.1 through 4.18.4, below. Any costs associated with meeting these access standards shall be borne by the Contractor.

4.18.1 The Contractor shall assign a US-citizen company official (acting as their Trusted Agent) to identify and authenticate all employees prior to receiving Yubikey credentials for ETA access. For the Yubikey options, the company official will assert the identity proofing has taken place and provide on company letterhead, a complete list of employees authenticated and authorized to receive PKI credentials. This assertion will be made to the Contracting Officer in accordance with format cited in Attachment 5 and updated letters provided if any information requires an update, employees leave the company, access is no longer required, or credentials are lost. Additionally, if requested by the Contracting Officer, the Contractor must provide a copy of all supporting the identity vetting/authentication documentation pertaining to an employee.

4.18.2 The company official must be able to recognize legitimate versions of identity documentation provided by the applicant in order to ensure only authorized personnel are granted ETA access.

4.18.3 The applicant must present two forms of Government-issued identification, at least one of which must be a proof of citizenship, in person, to the company official acting as the Trusted Agent. The following documents are examples of acceptable documents: Official Passport, Certified Birth Certificate issued by the city, county, state, or country in accordance with local laws, Naturalization Certificate, Certificate of Citizenship, FS-240 Consular Report, or DS-1350 Certification of Report of Birth. The authorized company official must exchange sufficient information to ensure the identity of the applicant is unambiguous and accurate.

4.18.4 All employees accessing ETA will successfully pass a commercial employment background check performed by the USC Contractor or a 3<sup>rd</sup> party or successfully pass a local government performed check for employment purposes. If requested by the Contracting Officer, the Contractor must provide a copy of the identification proofing documents used to perform the background checks of the employee.

#### **4.19 Aircraft Recovery Process**

4.19.1 Within 12 hours, the Contractor will provide an aircraft recovery plan identifying their process to repair and remove the aircraft. The Contractor will provide daily status information to the Senior Airfield Authority, AMD/ALCT, CDDOC, and Contracting Officer on the progress to repair/remove the aircraft.

4.19.2 The Government reserves the right to move the aircraft, at any time, off the active runway, taxiway or parking spot to another area as operational requirements dictate. The Contractor shall be charged associated costs for movement of the aircraft.

#### **4.20 Incident Reporting**

In the event of an air, surface, or ground safety incident in CENTCOM AOR, the Contractor shall immediately notify the CDDOC (Tel: +965-2202-7301, then dial 480-2778/2646 and centcom.arifjan.cddoc.list.cddoc-ops@army.mil), AMD/APCC (Tel: 011-974-458-9555, after prompt enter 436-4186), SDDC HQ COC (Tel 618-220-4262), the cognizant COR and the Contracting Office (Tel: 618-220-7127/7109). The Contractor shall state their name, whom they represent, incident type, incident location, aircraft or vehicle type, aircraft tail number, and incident time (Zulu). Additionally, the Contractor shall forward the CDDOC, AMD/APCC, SDDC HQ COC, cognizant COR and Contracting Office a completed Incident Report Form documenting the circumstances surrounding the incident within 12 hours (to include copies of the cargo manifest).

#### **4.21 General Cyber Security Requirements**

##### **4.21.1 Handling and Protection of Non-Public Information**

4.21.1.1 In performance of this contract, the Contractor may have access to DoD Transactional Information (DTI), which for the purposes of this section shall mean any information developed or received in the course of planning, ordering, shipping, tracking, and invoicing in support of the requirements of this contract. To adequately protect this

DTI, contractor information systems (IS) involved in the performance of this contract shall comply with the security requirements in the current version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations." Compliance with NIST SP 800-171 measures is required at the prime contractor level and does not apply to subcontractors and other entities that the prime contractor engages with in order to meet the requirements of this contract.

4.21.1.2 Additionally, the Contractor agrees to use such information only for the purposes of fulfilling the contracted requirements and to protect such information from unauthorized release or disclosure. Protection of the DTI does not abrogate any responsibilities of the Contractor to comply with or implement additional cyber security requirements as part of generally accepted system security principles or as required by other categories of information that may be co-resident with the DTI on the Contractor's IS.

#### 4.21.2 Operationally Critical Support

The services designated under this contract are "operationally critical support" as defined in DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

#### 4.21.3 Cyber Security Assessments and Mitigation Plans

4.21.3.1 The Contractor shall provide a Self-Assessment of its compliance with NIST SP 800-171 and present a Plan of Action that identifies any deviations, non-compliance, or proposed alternative means of compliance as well as plans for correcting non-compliant requirements to the Contracting officer within 60 days of contract award and then annually thereafter on 1 September each year. The Self-Assessment and Plan of Action shall address all of the requirements in NIST SP 800-171.

4.21.3.2 Table 5.17.3.5 provides modified requirements of CUI/CDI specific controls from NIST SP 800-171 that will be used to evaluate compliance in a non-CUI/CDI environment. Additionally, at any time during the period of performance, when a contractor determines it is non-compliant with a NIST SP 800-171 requirement or an approved alternate means of compliance resulting in a High or Moderate Potential Impact as defined in Federal Information Processing Standards Publication (FIPS PUB) 199, "Standards for Security Categorization of Federal Information and Information Systems," the Contractor shall submit a Plan of Action within 15 days of the determination of non-compliance.

4.21.3.3 Plans of Action and any requests to vary from NIST SP 800-171 shall be submitted to the Contracting Officer for consideration and approval by USTRANSCOM. The Contractor need not implement any security requirement determined by USTRANSCOM to be non-applicable or to have an equally effective alternative security measure implemented in its place. The Plan of Action shall follow the template provided in Attachment 7. Alternate formats for the Plan of Action may be proposed and must be approved by USTRANSCOM.

4.21.3.4 USTRANSCOM may conduct an on-site visit to a contractor's facility or request a third party assessment (U.S. Government agency or U.S. Government funded commercial entity) to review progress towards meeting their Plan of Action, evaluate any proposed variances to NIST SP 800-171 requirements, and to assess residual risk to the DTI resulting from the non-compliance. Date and time of on-site visits will be mutually agreed-upon by USTRANSCOM and the Contractor in advance.

| Table 5.17.3.5 – Modified NIST SP 800-171 Requirements |                                                                     |                                                                                                                                                              |
|--------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Req #                                                  | NIST SP 800-171 Requirement                                         | USTRANSCOM Modified Requirement                                                                                                                              |
| 3.1.3                                                  | Control the flow of CUI in accordance with approved authorizations. | Limit the flow of DoD information to organizations or individuals necessary for the performance of the operationally critical requirements of this contract. |

|        |                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.1.9  | Provide privacy and security notices consistent with applicable CUI rules.                                                                                                                                                                                                     | Provide privacy and security notices consistent with U.S. Government and/or local governmental regulations.                                                                                                                                                                                |
| 3.1.19 | Encrypt CUI on mobile devices and mobile computing platforms.                                                                                                                                                                                                                  | Provide adequate technical protections on mobile devices and computing platforms that process and/or store contractual information.                                                                                                                                                        |
| 3.1.22 | Control CUI posted or processed on publicly accessible systems.                                                                                                                                                                                                                | Control DoD information posted or processed on publicly accessible systems.                                                                                                                                                                                                                |
| 3.7.3  | Ensure equipment removed for off-site maintenance is sanitized of any CUI.                                                                                                                                                                                                     | Ensure equipment removed for off-site maintenance is sanitized of DoD information.                                                                                                                                                                                                         |
| 3.8.1  | Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.                                                                                                                                                                     | Protect (i.e., physically control and securely store) system media containing DoD information, both paper and digital.                                                                                                                                                                     |
| 3.8.2  | Limit access to CUI on system media to authorized users.                                                                                                                                                                                                                       | Limit access to DoD information on system media to authorized users.                                                                                                                                                                                                                       |
| 3.8.3  | Sanitize or destroy system media containing CUI before disposal or release for reuse.                                                                                                                                                                                          | Sanitize or destroy system media containing DoD information before disposal or release for reuse.                                                                                                                                                                                          |
| 3.8.4  | Mark media with necessary CUI markings and distribution limitations.                                                                                                                                                                                                           | Mark media with privacy and security notices consistent with U.S. Government and/or local government regulations.                                                                                                                                                                          |
| 3.8.5  | Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.                                                                                                                                                     | Control access to and maintain accountability for media containing DoD information.                                                                                                                                                                                                        |
| 3.8.9  | Protect the confidentiality of backup CUI at storage locations.                                                                                                                                                                                                                | Provide information backup procedures (frequency, timeframe for storage, etc.) for DoD data located on contractor systems. Protect the confidentiality of backup materials containing DoD information.                                                                                     |
| 3.9.1  | Screen individuals prior to authorizing access to organizational systems containing CUI.                                                                                                                                                                                       | Screen individuals prior to authorizing access to organizational systems containing DoD information.                                                                                                                                                                                       |
| 3.9.2  | Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.                                                                                                                                 | Ensure that DoD information and organizational systems containing DoD information are protected during and after personnel actions such as terminations and transfers.                                                                                                                     |
| 3.10.6 | Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).                                                                                                                                                                                          | Enforce safeguarding measures for DoD Information at alternate work sites (e.g., telework sites).                                                                                                                                                                                          |
| 3.11.1 | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI. | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of DoD information. |

|         |                                                                                                                                                                 |                                                                                                                                                                                            |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3.13.8  | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | Implement cryptographic mechanisms to prevent unauthorized disclosure of DoD information during transmission when possible unless otherwise protected by alternate physical safeguards.    |
| 3.13.11 | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.                                                                             | Employ FIPS-validated cryptography when used to protect the confidentiality of DoD information within the organization's systems and when possible when transmitting to external entities. |
| 3.13.16 | Protect the confidentiality of CUI at rest.                                                                                                                     | Protect the confidentiality of DoD information at rest.                                                                                                                                    |

#### 4.21.4 Cyber Incident Reporting

4.21.4.1 In addition to the DFARS 252.204-7012 reporting requirements for unclassified systems and DoD Manual (DoDM) 5220.22, National Industrial Security Program Operating Manual (NISPOM) for classified systems, reportable cyber-incidents include, but are not limited to, the following:

4.21.4.1.1 Cyber-incidents as defined in Table 1.

4.21.4.1.2 Notifications by a federal, state, or local law enforcement agency or cyber-center (i.e., National Cyber Investigative Joint Task Force (NCIJTF), National Cybersecurity & Communications Integration Center (NCCIC)) of being a victim of a successful or unsuccessful cyber-event, anomaly, incident, insider threat, breach, intrusion, or exfiltration.

Table 1.

| Incident Category    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Level Intrusion | Unauthorized privileged access to an IS. Privileged access, often referred to as administrative or root access, provides unrestricted access to the IS. This category includes unauthorized access to information or unauthorized access to account credentials that could be used to perform administrative functions (e.g., domain administrator). If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category.                                                                               |
| User Level Intrusion | Unauthorized non-privileged access to an IS. Non-privileged access, often referred to as user level access, provides restricted access to the IS based on the privileges granted to the user. This includes unauthorized access to information or unauthorized access to account credentials that could be used to perform user functions such as accessing Web applications, Web portals, or other similar information resources. If the IS is compromised with malicious code that provides remote interactive control, it will be reported in this category. |
| Denial of Service    | Denial of Service (Incident)—Activity that denies, degrades, or disrupts normal functionality of an IS or DoD information network.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Malicious Logic      | Installation of software designed and/or deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised IS. Malicious code that has allowed interactive access should be categorized as Root or User Level                                                                                                                                                 |



|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | Intrusion incidents. Interactive active access may include automated tools that establish an open channel of communications to and/or from an IS.                                                                                                                                                                                                                                                                                                               |
| Ransomware | Malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. Ransomware is a reportable incident that may be associated with multiple incident categories depending on the attack vector and execution. |

4.21.4.2 If the cyber-incident affects a classified system, vulnerabilities associated with the incident will be classified per the current version of USTRANSCOM Instruction 31-02, Security Classification Guide.

#### 4.21.5 Cybersecurity Incident Reporting Timelines

In addition to providing the notification required by DFARS 252.204-7012, the contractor is required to notify USTRANSCOM as soon as practicable, but no later than 72 hours after discovering a reportable cyber-incident. The reporting timeline begins when the incident is discovered or reported to the company, its employees, contractors, or cybersecurity firm responsible for providing cybersecurity and response for the company. The contractor shall contact the USTRANSCOM Cyber Operations Center (CyOC) via phone at 618-817-4222. If the contractor does not immediately reach the CyOC via phone, the contractor shall send an email notification to [transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil](mailto:transcom.scott.tcj6.mbx.cyoc-dodin-operations@mail.mil).

#### 4.21.6 Mandatory Reporting Data

4.21.6.1 The contractor shall work with the USTRANSCOM CyOC through resolution of the incident. Within 72 hours of becoming aware of a reportable cyber-incident, the contractor shall provide an initial notification of the incident, even if some details are not yet available, which includes, but is not limited to, the following information:

- (a) Company Name
- (b) Who will be the POC with contact information
- (c) Contracting Officer POC (name, telephone, email)
- (d) Overall Assessment –Description of incident, data at risk, mitigations applied
- (e) Indicators of compromise
- (f) Vector of attack (if known)
- (g) Estimated time of attack (if known)

4.21.6.2 The contractor shall provide a follow-on cyber-incident report to the USTRANSCOM CyOC within 5 days of becoming aware of a reportable cyber-incident, which includes, but is not limited to, the following information:

- (a) Contractor unique Commercial and Government Entity (CAGE) code
- (b) Contract numbers affected
- (c) Facility CAGE code where the incident occurred if different than the prime Contractor location
- (d) POC if different than the POC recorded in the System for Award Management (name, address, position, telephone, email)
- (e) Contracting Officer POC (name, telephone, email)
- (f) Contract clearance level
- (g) DoD programs, platforms, systems, or information involved
- (h) Location(s) of compromise
- (i) Date incident discovered
- (j) Type of compromise (e.g., unauthorized access, inadvertent release, other)
- (k) Description of technical information compromised

(l) Any additional information relevant to the information compromise

#### 4.21.7 Incident Reporting Coordination

4.21.7.1 In the event of a cyber-incident, USTRANSCOM may conduct an on-site review of network or information systems where DoD information is resident on or transiting to assist the contractor in evaluating the extent of the incident and to share information in an effort to minimize the impact to both parties. Date and time of on-site visits will be mutually agreed upon by USTRANSCOM and the contractor in advance.

4.21.7.2 The contractor agrees to allow follow-on actions by the Government (e.g., USTRANSCOM, Federal Bureau of Investigation, Department of Homeland Security, DC3, etc.) to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments might be necessary to ascertain an incident methodology and identify systems compromised as a result of the incident. Once an incident is identified, the contractor agrees to take all reasonable and appropriate steps to preserve any and all evidence, information, data, logs, electronic files and similar type information (reference NIST Special Publication 800-61: Computer Security Incident Handling Guide, (current version)) related to the incident for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government.

4.21.7.3 The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved (e.g., remove an affected system, while still powered on, from the network) and all actions documented until forensic analysis can be performed by the Government or, if the Government is unable to conduct the forensic analysis, a mutually agreed upon third party (e.g., Federally Funded Research and Development Center (FFRDC), commercial security contractor, etc.). Any follow-on actions shall be coordinated with the contractor via the Contracting Officer.

4.21.7.4 The contractor agrees to indemnify and hold the government harmless for following any recommendations to remedy or mitigate the cyber-incident following the actions under 4.21.7.1 and 4.21.7.2.

#### 4.21.8 Confidentiality and Non-Attribution Statement

The Government may use and disclose reported information as authorized by law and will only provide attribution information on a need-to-know basis to authorized persons for cybersecurity and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counter intelligence, threat reporting, and trend analysis). The Government may share threat information with other USTRANSCOM industry partners without attributing or identifying the affected contractor.

## SECTION 5 ELECTRONIC DATA INTERCHANGE (EDI) TRANSACTIONS AND DAILY ITV

### 5.1 EDI Transactions

5.1.1 The Contractor shall use EDI as the primary means for interfacing with SDDC for all contracted movements.

5.1.2 EDI is the computer-to-computer exchange of business data in machine-readable language using strictly defined public standards.

5.1.3 The Contractor shall use the Defense Transportation Electronic Business (DTEB) approved Implementation Convention (IC) for the ANSI X12 EDI 300, 301, 303, 304 and 315 transaction sets in compliance with their approved concepts of operations. Version 4010 or later is required. The Contractor shall implement changes to business processes contained in revisions to Transaction Set Implementation Conventions and their controlling concepts of operations as may be approved by the Defense Transportation Electronic Board. These changes shall be implemented in accordance with schedules approved by SDDC.

5.1.4 The Contractor shall receive or transmit, as appropriate, the following EDI transactions sets:

5.1.4.1 The Contractor receives EDI 300 Reservation (Booking Request) Ocean – the booking, including increases and decreases.

5.1.4.2 The Contractor transmits EDI 301 Confirmation (Ocean) - Confirmation of the booking or counter proposal (Contractor to Ordering Officer).

5.1.4.3 The Contractor receives EDI 303, Booking Cancellation (Ocean) - Ordering Officer Cancellation.

5.1.4.4 The Contractor receives EDI 304, Ocean Carrier Shipping Instructions

5.1.4.5 The Contractor transmits EDI 315, Status Detail (Ocean) – shipment status reporting data.

## 5.2 Shipment Status Reporting

5.2.1 The Contractor shall provide accurate shipment status reports using the 315 transaction sets. Transaction sets shall be submitted in accordance with the Department of Defense (DoD) Transportation Electronic Business (DTEB) Implementation Convention (IC) ANSI X – 12 EDI standard or via IBS OCI. Airport event locations will be submitted in accordance with the International Civil Aviation Organization (ICAO) with the following format for event location: ICAO XXX Location. Event location example for an air event is – ICAO OMNW AL MAKTOUM INTERNATIONAL. It is critical that all air events start with ICAO, followed by the four letter ICAO code.

5.2.2 Table 5.2.2 identifies specific events that require reporting. The Contractor shall submit all reports within 24 hours of accomplishment.

| <b>Table 5.2.2 Reportable Shipment Status Events</b> |                                                        |                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CODE                                                 | DEFINITION                                             | NOTES                                                                                                                                                                                                                                                                                                                                                                                                   |
| EE                                                   | Empty spotted                                          | Container pick up in lieu of actual spot is acceptable for shippers having container pools. Required for other than pool locations.<br><br>(NOT REQUIRED FOR BREAKBULK)                                                                                                                                                                                                                                 |
| W                                                    | Pickup of loaded<br><br>Container/Breakbulk            | This transaction is required at the time customer turns over possession to Contractor. Transaction only applicable upon Contractor pickup. There shall be exactly one W transaction per shipment. If erroneous W transactions are submitted, Contractor shall invalidate them via the Pipeline Asset Tool (PAT) EDI invalidator tool to ensure only one valid transaction is reflected per shipment.    |
| I                                                    | In-gate at Port of Embarkation (POE) (Vessel/Aircraft) | This transaction is required at the Seaport of Embarkation (SPOE) and Aerial Port of Embarkation (APOE). Transaction only applicable at POE. There shall be exactly two transactions per shipment. If erroneous I transactions are submitted, Contractor shall invalidate them via the Pipeline Asset Tool (PAT) EDI invalidator tool to ensure only two valid transactions are reflected per shipment. |
| AE                                                   | Loaded on Vessel                                       | This transaction is required at the SPOE and at all transshipment ports.                                                                                                                                                                                                                                                                                                                                |
| VD                                                   | Vessel/Aircraft Departure                              | This transaction is required at the SPOE and APOE and at all transshipment ports.                                                                                                                                                                                                                                                                                                                       |
| VA                                                   | Vessel/Aircraft                                        | This Transaction is required at the Seaport Port of Debarkation (SPOD) and Aerial Port of Debarkation (APOD), and at all                                                                                                                                                                                                                                                                                |

|    |                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Arrival                                                        | transshipment ports.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| UV | Vessel Discharge                                               | This transaction is required at the SPOD and at all transshipment ports                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| OA | Out-gate from POD (Vessel/Aircraft)                            | This transaction is required at the SPOD and APOD for all cargo, regardless of whether booked to port or to door. Transaction only applicable at the PODs. There shall be exactly two OA transactions per shipment. If erroneous OA transactions are submitted, Contractor shall invalidate them via the Pipeline Asset Tool (PAT) EDI invalidator tool to ensure only two valid transactions are reflected per shipment.                                                                                               |
| EC | Return of Empty Container to Contractor Prior to Delivery (X1) | This transaction is required for container shipments when the Contractor has regained possession of its asset prior to delivery (X1). An example of the proper use of an EC code would be when cargo is deconsolidated at a transship point. The container is returned to the Contractor prior to X1, and the cargo is moved as pallet loads to the final consignee. Each container shipment container return event should be documented with either an RD or an EC but never both.<br><br>(NOT REQUIRED FOR BREAKBULK) |
| X1 | Delivery to Consignee                                          | This transaction is required when shipment is delivered to the customer, or possession is turned over to the US Government. This transaction is only applicable upon actual physical delivery. There shall be exactly one X1 transaction per shipment. If erroneous X1 transactions are submitted, Contractor shall invalidate them via the Pipeline Asset Tool (PAT) EDI invalidator tool to ensure only one valid transaction is reflected per shipment.                                                              |
| RA | Carrier Notified Empty Container Available for Pick-up         | This transaction will be auto-generated via PAT to document USG notification to the Contractor that an empty container is available for pick-up. This transaction will be auto-generated based on the date of notification, if the Contractor does not dispute availability within seven (7) days of notification.<br><br>(NOT REQUIRED FOR BREAKBULK)                                                                                                                                                                  |
| RD | Return of Empty Container to Contractor After Delivery (X1)    | This transaction is required for every container shipment when the Contractor regains possession of its asset after delivery (X1). Each container shipment container return event should be documented with either an RD or an EC but never both.                                                                                                                                                                                                                                                                       |

## SECTION 6 Liability

### 6.1 Liability for Lost or Damaged Cargo

6.1.1 Lost or Damaged Cargo. The Contractor is required to deliver cargo to final destination in the same condition it was tendered by the shipper. The Contractor is liable for cargo that is lost, damaged, or in any way altered from the tendered condition. Should a shipper desire to declare the value of its booked cargo and receive greater liability coverage than that listed in paragraph 7.1.4., the shipper will order the “increased value” accessorial which obligates the Contractor to be liable for damage and loss up to the amount stated in the RFQ, or the actual

value of the lost cargo, whichever is less.

6.1.2 A “booking” covers all cargo booked under a single PCFN and the Contractor is liable to the shipper for lost or damaged cargo up to the amount declared in the booking, or the actual value of the lost cargo, whichever is less.

6.1.3 Notice. Pursuant to the Contract Disputes Act, the Government has 6 years from discovery of loss or damaged cargo, to file a claim with the Contractor. However, the Government will take all reasonable steps to provide notice of loss as soon as it is discovered.

6.1.4 Liability is governed by the applicable statute or multi-lateral international agreement based on the mode of cargo transportation (i.e. air, sea, or land) at the location where the loss or damage occurred. 49 U.S.C. §14706 also applies to all land cargo transportation including land cargo transportation outside the United States. However, the above referenced accessorial liability and notice requirements replace the following statutory and Convention provisions: Article 22(2) & (3) and Article 31, of the Convention for the Unification of Certain Rules for International Carriage by Air (Montreal Convention, (1999); 46 U.S.C.A. §30701, Section 4(5) & Section 3(6); and 49 U.S.C.A. §14706(e) & (f). For land cargo transportation under 49 U.S.C. §14706, including land cargo transportation outside the United States, liability is limited to \$50,000 per TCN, or the actual amount of the loss or damage to the cargo, whichever is less.

## **6.2 Contractor Bodily Injury and Property Damage Liability**

6.2.1 Contractors are required to maintain bodily injury and property damage liability insurance coverage in amounts equal to, or in excess of, those customarily used in the commercial marketplace in the areas where services will be performed and shall be commensurate with any legal requirements of the locality and sufficient to meet normal and customary claims. The insurance coverage shall provide for bodily injury and property damage liability covering the operation of all automobiles, trucks, aircraft, and ocean vessels used in connection with performing the contract.

## **SECTION 7 ACRONYMS AND DEFINITIONS**

### **7.1 Acronyms**

|         |                                                      |
|---------|------------------------------------------------------|
| AOR     | Area of Responsibility                               |
| APOD    | Aerial Port of Debarkation                           |
| APOE    | Aerial Port of Embarkation                           |
| CDDOC   | CENTCOM Deployment and Distribution Operation Center |
| CENTCOM | United States Central Command                        |
| CFS     | Container Freight Station                            |
| CO      | Contracting Officer                                  |
| CONUS   | Continental United States                            |
| COR     | Contracting Officer’s Representative                 |
| CPA     | Cargo Preference Act (1904)                          |

|        |                                                    |
|--------|----------------------------------------------------|
| CRAF   | Civil Reserve Air Fleet                            |
| CSC    | Convention of Safe Containers                      |
| DeCA   | Defense Commissary Agency                          |
| DFARS  | Defense Federal Acquisition Regulation Supplement  |
| DLA    | Defense Logistics Agency                           |
| DoD    | Department of Defense                              |
| DODAAC | Department Of Defense Activity Address Code        |
| D-RAP  | Delay Request and Authorization Portal             |
| DTEDI  | Defense Transportation Electronic Data Interchange |
| DTR    | Defense Transportation Regulation                  |
| DTS    | Defense Transportation System                      |
| EDI    | Electronic Data Interchange                        |
| EIPP   | Electronic Invoice Presentation and Payment        |
| FEU    | Forty Foot Equivalent Unit                         |
| FAR    | Federal Acquisition Regulation                     |
| FAK    | Freight All Kinds                                  |
| FIO    | Free In and Out                                    |
| GFC    | Government Furnished Containers                    |
| GLOC   | Ground Line of Communication                       |
| IMO    | International Maritime Organization                |
| ISO    | International Organization for Standardization     |
| IBS    | Integrated Booking System                          |
| ITGBL  | International Thru Government Bill of Lading       |

|          |                                               |
|----------|-----------------------------------------------|
| ITV      | Intransit Visibility                          |
| JOPES    | Joint Operation Planning and Execution System |
| MSC      | Military Sealift Command                      |
| OCBO     | Ocean Cargo Booking Office                    |
| OCCA     | Ocean Cargo Clearance Authority               |
| OCI      | Ocean Contractor Interface                    |
| OCONUS   | Outside Continental United States             |
| OO       | Ordering Officer                              |
| OTUMs    | Other Than Unit Moves                         |
| PCFN     | Port Call File Number                         |
| PCFN-NIB | Port Call File Number – Non-IBS Booking       |
| PIDs     | Plan Identifications                          |
| POD      | Port of Discharge                             |
| POE      | Port of Embarkation                           |
| POV      | Privately Owned Vehicle                       |
| PWS      | Performance Work Statement                    |
| QA       | Quality Assurance                             |
| QCP      | Quality Control Plan                          |
| RDD      | Required Delivery Date                        |
| Reefer   | Refrigerated Container                        |
| RFP      | Request for Proposals                         |
| RFQ      | Request for Quote                             |
| RLD      | Required Load Date                            |
| RORO     | Roll-On/Roll-Off                              |
| SCAC     | Standard Contractor Alpha Code                |
| SDDC     | Military Surface Deployment and               |

|            |                                            |
|------------|--------------------------------------------|
|            | Distribution Command                       |
| TCMD       | Transportation Control & Movement Document |
| TCN        | Transportation Control Number              |
| TEU        | Twenty Foot Equivalent Unit                |
| TREMCARD   | Transport Emergency Card                   |
| ULN        | Unit Line Numbers                          |
| US         | United States                              |
| USTRANSCOM | United States Transportation Command       |
| VETCOM     | US Army Veterinary Command                 |
| VISA       | Voluntary Intermodal Sealift Agreement     |

## 7.2 Definitions

The following terms have the meaning as set forth below:

Acceptable Space: Space with normal access thereto as would normally be used in liner service for the particular type of cargo declared at the time of booking, and shall be properly prepared, cleaned and ready to receive the cargo.

American National Standards Institute (ANSI ASC X12): Charters the Accredited Standards Committee (ASC) X12 to develop uniform standards for inter-industry electronic interchange of business transactions throughout North America.

Awarded Weight: Whichever is greater of the estimated scale weight of cargo provided by the shipper or the estimated dimensional weight of cargo based on the dimensions provided by the shipper. The dimensional weight is figured in the following manner: L X W X H (all measurements in inches) divided by 166.

Billable Weight: The weight of a shipment the Contractor may bill the Government. The billable weight is either the certified scale or dimensional weight, whichever is greater. For cargo that is unstuffed and reconfigured in accordance with section 1.5.3, only one method of determining billable weight (scale or dimensional) is allowed per PCFN. For all other cargo, the billable weight determination is allowed per TCN.

Booking: Offer by the Government and acceptance by the Contractor for the transportation of goods pursuant to the applicable rates, terms and conditions of the subject contract. A booking is an order.

Breakbulk/RORO Cargo: All cargo that is not containerized.

Bulk Cargo: Cargo consisting of unsegregated mass commodities. Examples of bulk cargo include sand, gravel, ready-mix concrete, coal, and agricultural products (e.g., seeds, grains, animal feeds).

Cargo Cleaning Service:

Wash Service: Cleaning required for cargo that has been tendered to the Contractor dirty and requires thorough washing.



Rinse Service: Cargo cleaning to remove road dirt and other contaminants accumulated while in transit or at the port. Service applies to cargo that was tendered to the Contractor clean.

Concealing Service: Covering and protecting of cargo using weather resistant, non-transparent, durable material.

Consignee: The person or entity named in the booking or shipping instructions to which goods have been shipped or turned over for care.

Contracting Officer (CO): A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the Contracting Officer acting within the limits of their authority as delegated by the Contracting Officer.

Contracting Officer's Representative (COR): Appointed in writing by the CO, responsible for, but not limited to, the following: monitoring the Contractor's performance in accordance with the terms of the contract; ensuring Contractor's compliance with reporting requirements; providing data for Government reports; verifying/ certifying invoices; and reviewing contractor claims.

Contractor: An entity in private industry, which enters into contracts with the Government to provide goods or services.

Constructive Staging: A delay in the final receipt of the cargo by the Government at the inland destination after release and commencement of on-carriage from the discharge port caused by the Government's refusal or inability to accept the containers at the inland destination. Requires cognizant COR approval.

CRAF Carrier: A US Flag commercial air carrier who is an active participant of the Civil Reserve Air Fleet (CRAF) Program. CRAF Participant is synonymous with CRAF Carrier.

Dimensional Weight: The weight computed on the basis of volume rather than actual weight. The dimensional weight of contractor-owned/provided containers shipments shall be determined by the dimensions of the contents within the container, established prior to airlift, unless the Government specifically requests in the booking remarks for the door to door movement of the contractor-owned/provided container. In the event the sum of the dimensional weight of the contents of a contractor-owned/provided container exceeds the dimensional weight of the container, the container dimensional weight shall apply.

Dimensional Weight is calculated as follows:  
 $L \times W \times H$  (all measurements in inches) divided by 166.

Driver free time: The time allowed for Government shippers and receivers to load and unload contractor equipment (i.e. containers) before driver wait time charges accrue.

Drop and Pick: See Spotting of Containers

Dry Cargo Container: A completely enclosed weatherproof container.

EDI Implementation Convention (IC): Defines the rules for filling in or "populating" an EDI transaction. Following the agreed upon convention, or version of the standard ensures that EDI partners will encounter fewer data quality problems during development and maintenance of their EDI systems.

Electronic Data Interchange (EDI): The computer-to –computer exchange of business data in machine-readable language using strictly defined public standards.

Flatrack (Platform) Container: A container without weatherproof sides and/or top to include platforms, which have no sides or ends and flatracks with rigid or collapsible ends.

Hazardous Cargo: A hazardous substance or material including a hazardous substance, which has been determined

by the Secretary of Transportation or International Maritime Organization (IMO) to be capable of posing an unreasonable risk to health, safety and property when transported in.

Heavy Lift Cargo (Breakbulk): Any piece of breakbulk cargo with a scale weight exceeding 60,000 lbs.

Heavy Lift Cargo (Container): Any container with a scale weight exceeding 44,000 lbs.

Heavy Vehicles: Breakbulk/RORO cargo – Wheeled or tracked vehicles (unboxed) exceeding 10,000 lbs per unit.

Light Vehicles: Breakbulk/RORO cargo – Wheeled or tracked vehicles (unboxed) up to and including 10,000 lbs per unit.

Liner In/Liner Out: Contractor is responsible for the loading and/or discharging of cargo at port of origin and/or destination and all costs associated thereto.

Liner Terms—Breakbulk: The Contractor provides all services from receipt of cargo at POE to load of cargo on the vessel (liner in) or from discharge of the vessel at POD to outgate (liner-out). Any costs for the loading and discharging of inland transport within the contractor's terminal are for the account of the Contractor.

Liner Terms – Container: The Contractor assumes all responsibility and cost for the transportation of the cargo from the port or point where the cargo is received for by the Contractor to the destination port or point where the Contractor makes the cargo available to the consignee. In the case of BB/RO-RO, the cargo is accepted and/or made available within the Contractor's terminal. Any costs for the loading or discharging of inland transport within the Contractor's terminal are for the account of the Contractor.

Live Unload: Contractor delivers a loaded container and the driver waits while the receiver unloads the container.

Multimodal Move: Being or involving more than one mode of transportation during a single journey that permits the Contractor to elect the most efficient type and/or mix of transportation methods (air, sea, rail, truck, barge, etc.) in order to meet a specified RDD. In a multimodal move, the prime Contractor maintains responsibility and liability for the cargo during the entire movement from origin to final destination.

Ocean Cargo Booking Office (OCBO): The SDDC activity that books DoD sponsored cargo for ocean movement, performs related contract administration, and accomplishes export/import ocean traffic management functions for DoD cargo moving within the DTS. May also perform authorized Customs Entries.

Ocean Cargo Clearance Authority (OCCA): See Ocean Cargo Booking Office (OCBO)

Ordering Activity: Includes the Commander, Surface Deployment and Distribution Command (SDDC), and authorized designees.

Ordering Officer (OO): An individual authorized to place orders against indefinite delivery indefinite quantity transportation or transportation-related services contracts awarded by USTRANSCOM, provided the contract terms and monetary limitations specified in the contract are met.

Over Dimensional Cargo - Container: Any individual piece of container booked cargo which cannot fit within the container because its dimensions are greater than that of the booked container.

Over Dimensional Cargo - Breakbulk: Breakbulk cargo that has any one dimension over 50 feet long, more than eleven (11) feet wide or over ten (10) feet in height, or as determined by the Ordering Officer, requires special handling equipment for loading aboard or discharging from a vessel or aircraft because of that cargo's atypical size.

PCFN (Port Call File Number): An identifier generated and assigned by the Integrated Booking System to uniquely identify a booking. A task order is issued at the PCFN level may consist of one or many TCNs.

QUADCON: Shipper Owned Container; four QUADCONs have the same external dimensions as a 20-foot shipping container.

Receiver: Individual or entity authorized by the consignee to receive and sign for delivered cargo.

Required Delivery Date (RDD): The date specified in the booking when cargo must be delivered.

Round Robin: See Spotting of Containers

Scale Weight: The weight of cargo determined by either a certified commercial weigh ticket or a joint weigh ticket. Weigh tickets shall represent the weight for the Government-owned or leased containers, contents of the contractor owned container, air pallet or breakbulk item only, independent of truck, chassis, or other conveyances. The weigh tickets shall represent the weight of the cargo only and not include any weight for dry ice, thermal sleeves, cargo netting, or other carrier augmented packaging materials. A Weigh ticket shall only contain the contents of a single TCN.

SEAVAN Service Codes: DTR codes which indicate the extent of service for which the Contractor is paid. Indicates where the Contractor's responsibility for movement begins or ends:

K – At the Contractor's terminal (Pier Service).

L – In the commercial zone of the US port city or, outside the US, within 10 miles of the port city limits. Certain port cities, which are divided into modified zones as listed in this Contract, are assigned codes 1-9 instead of L (Local Drayage).

1-9 – In a modified zone for certain port cities as defined in this Contract. The number codes used correspond with the zone number in the Contract.

M – At any point not covered by codes K, L, or 1-9.

P – Same as Code M, except that one or more scheduled stop-offs in route to final destination have been booked with the ocean contractor. Does not apply to local deliveries performed at the expense of the Government.

S – Same as Code T, except that one or more stop-offs in route to final destinations have been booked with the contractor. Does not apply to local deliveries performed at the expense of the Government.

T – Same as Code L, 1-9, or M except cargo is booked as a "Through Shipment" under Single Factor Rates.

Shipper Owned 20/40 ft Containers: Breakbulk/RORO – Government owned/leased container cargo carried by break bulk and/or RORO operators under the Breakbulk/RORO section.

Spotting containers: Positioning empty containers at shipper's facility for loading by the shipper:

Drop and Pick: Contractor delivers an empty container on chassis and later picks it up after it has been loaded.

Live Load: Contractor delivers an empty container and the driver waits while the shipper loads the container.

Round Robin Drop and Pick: The Contractor would position one empty container at the shipper's facility. All other deliveries of empty containers would be scheduled with the pickup of loaded containers.

Staging: Delay in commencement of drayage, line-haul or on-carriage transit requested by the Government. Containers may be staged at the contractor's terminal, port facility, or at any other location chosen by the Contractor, such as a railhead or barge terminal.

Transportation Control Number (TCN): A 17-character data element assigned to control and manage every shipment unit throughout the transportation pipeline.

TRICON: Shipper Owned Container; three TRICONs have the same external dimensions as a 20-foot shipping container

Vessel Status Code: The first position of the code describes the type of contract. The second indicates whether Government or Contractor is responsible for vessel load and delivery of cargo to/from port. Codes 5-9 are only used

for breakbulk cargoes 2nd Position codes are as follows:

| Code | POE           | POD            |
|------|---------------|----------------|
| 1.   | Free-in       | Free-out       |
| 2.   | Liner-in      | Liner-out      |
| 3.   | Free-in       | Liner-out      |
| 4.   | Liner-in      | Free-out       |
| 5.   | Door/Liner-in | Free-out       |
| 6.   | Door/Liner-in | Liner-out      |
| 7.   | Free-in       | Liner-out/Door |
| 8.   | Liner-in      | Liner-out/Door |
| 9.   | Door/Liner-in | Liner-out/Door |

Weight Conversion Factor: 1 Kilogram = 2.20462 pounds

Wheeled or Tracked Vehicles: (Unboxed) - Includes all types of unboxed, land or amphibious vehicles, set up on wheels or tracks, whether or not self-propelled.

## SECTION 8 DELIVERABLES

| PWS Reference       | Deliverable                              | Task Delivery Date                                                                             | Distribution                                                  | Format                                       |
|---------------------|------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------|----------------------------------------------|
| PWS 1.15            | Delivery Receipt                         | When cargo is delivered and when POD is requested                                              | Consignee/agent (upon delivery)<br>SDDC/TCAQ (when requested) | Paper<br>Electronic                          |
| 1.A.1.1.1.1. WS 3.4 | 1.A.1.1.1.2. Broken/Replacement of Seals | 1.A.1.1.1.3. Within 24 hours of discovery                                                      | 1.A.1.1.1.4. OR                                               | 1.A.1.1.1.5. Electronic                      |
| PWS – 4.17          | Foreign Entity Vetting                   | The initial report is due 90 calendar days after contract award and every 6 months thereafter. | Contracting Officer and Specialist                            | Attachment 10 – FEV Template                 |
| PWS 4.20            | Incident Reporting                       | As required                                                                                    | As described in PWS 4.20                                      | Electronic                                   |
| PWS 4.21.4          | Cyber Incident Reporting                 | Provide timely cyber-incident reporting as required.                                           | As required by 4.21.5                                         | As required by 4.21.5                        |
| PWS – 1.17          | Manual Operational Reports               | As required                                                                                    | As described in Attachment 4                                  | Electronic                                   |
| PWS – 4.21          | Cyber Security Self Assessment           | 60 days after award then annually on 1 September                                               | Contracting Officer and Specialist                            | Attachment 7- NIST.SP.800-171- POAM Template |
| PWS - 4.21.3        | Cyber Security Plan of Action            | 60 days after award then annually on 1 September                                               | Contracting Officer and Specialist                            |                                              |
| PWS – 1.12.7        | Prime Vendor Carrier Agreements          | Prior to receiving an award of Prime Vendor Cargo or upon any changes to the agreement         | Contracting Officer and Specialist                            | Electronic (Attachment 6)                    |

## **Invoicing and Payment**

### **A. General Information**

A.1. All invoices and supporting documentation shall be in English and on prime contractor company letterhead. All invoices shall be submitted promptly within the timeframes described in this Attachment. Descriptions of services rendered must match the terms used in the contract. When carrier terminology differs from the contract, the latter shall be used.

A.2. There are three distinct invoicing categories for this contract as follows:

- 1) Invoices for Services Ordered via IBS or Services Ordered via Contracting Action
- 2) Invoices for Services Not Ordered
- 3) Invoices associated with Requests for Equitable Adjustments

Invoices shall be submitted only after services included on the invoice have been satisfactorily performed (Ref FAR 32.905) and shall be submitted within the timeframe requested under the established billing procedure. Commercial interim financing payments may be billed as described below, unless the Contracting Officer determines after award that adequate security is lacking or financing payments are no longer in the best interest of the Government. (See FAR 52.232-29)

A.3. The Government has the right to request additional information in support of the charges in the invoice. In addition, all charges for services not ordered in the Integrated Booking System (IBS) booking (Driver Wait Time) will require COR review and certification via the SDDC Pipeline Asset Tool Invoice Processing Portal (PAT IPP) tool and REA invoices will require review and approval by the Contracting Officer.

A.4. Invoices for IBS Booked Services will be created via the Treasury Invoice Processing Portal (T-IPP) using the online purchase order flip capability. TFMS will pass purchase order data to Treasury IPP for use in the invoice creation process. Once invoice data is successfully input to Treasury IPP, it will pass from Treasury IPP to TFMS for entitlement processing. TFMS will match obligation data from the booking, manifest data provided by GATES and invoice data provided from Treasury IPP and create a payable record. TFMS will also return invoice status data to Treasury IPP to include invoice payment notification.

A.5. The provisions of cash management will not apply to this contract. A pay immediate payment term will be applied to all invoices processed in conjunction with this contract. Once a payable invoice is received by the government, entitlement action will be completed and funds will be disbursed to the contractor. The standard entitlement processing cycle for these invoices will include disbursement of funds to the carrier financial institution within two business days of payable transaction certification within the Transportation Financial Management System (TFMS). The provisions of prompt payment will apply to this contract and any invoice not paid within 30 days will incur interest penalty. The provisions of prompt payment applies to final invoices, but not to requests for financing payments. Financing Payments will be made as soon as possible upon receipt of the invoice identified as "First Invoice", target date will be within 10 business days of receipt of a proper interim financing invoice.

A.6. Interim financing payment in the amount of 25% of the booked costs based on the booked dimensional weight will be authorized once the vessel leaves the sea port of embarkation (SPOE) (VD EDI transaction code) for shipments where the sea leg is the first leg of a shipment requiring both a sea and an air leg. The remaining balance due for work completed in accordance with the contract will be invoiced upon delivery. Interim financing payment in the amount of 60% of the booked costs based on the booked dimensional weight will be authorized once the vessel leaves the sea port of embarkation (SPOE) (VD EDI transaction code) for shipments where the air leg is the first leg of a shipment requiring both a sea and an air leg. The remaining balance due for work completed in accordance with the contract will be invoiced upon delivery. No interim financing payments are authorized for shipments where only one mode of transport is used (air only or ocean only moves).

A.7. All final invoices must be accompanied by documented cargo weights. The final invoice presented should bear the same invoice number as the interim financing payment invoice for that shipment with the first three positions of the invoice number being "FIN". Final invoices shall not be submitted prior to delivery of cargo to consignee.

A.8. All first and final or final invoices must be presented for the complete door to door shipment cost. The certified weigh ticket and Airway Bill are required, for moves encompassing both an air and ocean leg or moves including an air leg only, to pay the entire shipment and must be attached to the invoice transaction in Treasury IPP. For moves encompassing an ocean leg only, the ocean manifest is required and must be attached to the invoice transaction in Treasury IPP.

**B. Invoicing Procedures for Services Ordered via IBS or Services Ordered via Contracting Action:**

B.1 The following procedures applicable to invoicing and payment for services ordered or modified thereafter within the SDDC Integrated Booking System (IBS) or for services ordered or modified thereafter within USTRANSCOM contracting.

B.2 All invoices for these charges shall be submitted electronically via the Treasury IPP. Invoices along with any required supporting documentation will be submitted via this portal. Once invoices are successfully uploaded to the portal, they will be interfaced into the Transportation Financial Management System (TFMS) for entitlement processing.

B.3 A Treasury IPP invoice will contain the following information:

Header:

Contractor Name and Address (\*)

Invoice Date and Invoice Number

Invoice Total Amount (\*)

Contract Number (\*) *TFMS PO Number (\*) (Combination of contract number + Port Call File Number (PCFN) + PCFN fiscal year + sequence number) – no more than one (1) per invoice.*

Sail Date

Line Item Detail:

Line Item Description (\*)

Quantity

Unit of Measure (\*)

Unit Price (\*)

Extended price of services performed (\*<sup>1</sup>)

TFMS PO Line Number (\*)

TFMS PO Schedule Number (\*)

Transportation Control Number (TCN) (\*)

B.4 The contractor or the contractor's designated representative will weigh and document all cargo in accordance with one of two options below:

- i. Prior to delivery, the contractor will weigh each Government owned container, the contents of each carrier owned container, air pallet or piece of breakbulk cargo at a certified commercial scale. A weigh ticket shall only contain the contents of a single TCN. All final invoices will be accompanied by legible and certified weigh tickets. Hand-written, or pen-and-ink weigh tickets will be rejected, unless completed in accordance with para ii below. Weigh tickets shall represent the weight for the government owned container, contents of the contractor owned container, air pallet or breakbulk item only, independent of truck, chassis, or other conveyances. The Government reserves the right to send a Government representative to observe and verify commercial weighs. The contractor will accommodate Government requests for joint weigh at a commercial facility.

<sup>1</sup> \* Denotes the fields are prepopulated from the order or computed within the Treasury IPP for services ordered via IBS

ii. If the contractor does not have access to a certified commercial scale, the contractor must document cargo weights on a joint certified document. A contractor representative and an authorized Government representative must sign the document. The joint weigh may be conducted at a sea or air terminal, or at the shipment point of origin (installation, depot, or other shipper location) upon coordination with the shipper/unit. The contractor may request a joint weigh for any multimodal movement, subject to availability of a Government representative.

B.5 Weigh tickets and joint certified documents must include, at minimum, the following information:

- TCN
- Weight (stated in Pounds or with Pound conversion when kilograms are used)
- Cargo dimensions (length x width x height)
- Date/time of weigh
- Name and signature of authorized contractor or Government representatives conducting the weigh (for joint certified documents)

\* Note 1: When kilograms are converted to U.S. pounds, round to the next whole number

\*\*Note 2: Weigh tickets should reflect manifested dimensional weight of cargo

B.6 The Contractor shall submit the executed task order and any associated modifications for services ordered via Contracting Action with each invoice.

#### **C. Invoicing Procedures for Services Not Ordered:**

C.1 These procedures are applicable to invoicing and payment for priced charges or Contracting Officer pre-approved charges that are not ordered are provided below. All applicable EDI 315 transactions as outlined in Attachment 1 are required for submission of these invoices. Failure to submit required EDI 315 transactions will result in an invoice rejection until EDI 315 requirements are performed accordingly.

C.2 All invoices for non-booked charges shall be submitted electronically via upload to the SDDC Pipeline Asset Tool (PAT). Invoices containing such charges will be assigned to appropriate COR personnel within SDDC for validation/certification. Once these invoices are certified, they will be passed to the G8 accounts payable section for entitlement processing.

C.3 Invoices for driver wait time charges are included in this category. Upon completion of invoice validation, the Government and contractor will resolve any differences between the invoice driver wait time amount and the COR validated driver wait time amount. Upon completion of the reconciliation, the Government will make payment on the invoice.

#### **D. Invoicing Procedures for Request for Equitable Adjustment (REA)**

D.1. The amount of any request for equitable adjustment (REA) to contract terms shall accurately reflect the contract adjustment for which the Contractor believes the Government is liable. The request shall include only costs for performing the change and shall not include any costs that already have been reimbursed or that have been separately claimed.

D.2. REA's shall be submitted in accordance with DFARS clause 252.243-7 02 and must be accompanied with an invoice. Invoices for equitable adjustment requests may be submitted through the REA portal within the SDDC Invoice Processing Portal.



**ORDERING PROCEDURES  
CONTRACTOR SELECTION  
“FAIR OPPORTUNITY PROCESS”**

**1. Fair Opportunity to Compete.**

1.1. Fair Opportunity to Compete for Task Order (booking) Awards: Under the Multimodal multiple award contracts, fair opportunity for booking awards is provided through a “best value” RFQ process detailed below. The Government is responsible for evaluating shipment requirements and for making independent best value booking decisions.

1.2. Ordering: IAW FAR 16.505(b), Ordering, all multiple award contractors shall be provided a fair opportunity to be considered for each order in excess of \$3,500 pursuant to the procedures established in this section, unless the contracting officer (or ordering officer/booker) determines that:

- A. The agency’s need for the services or supplies is of such urgency that providing such opportunity would result in unacceptable delays.
- B. Only one awardee is capable of providing the services or supplies at the level of quality required because the supplies or services ordered are unique or highly specialized.
- C. The order must be issued on a sole-source basis in the interest of economy and efficiency because it is a logical follow-on to an order already issued under the contract, provided that all awardees were given a fair opportunity to be considered for the original order.
- D. It is necessary to place an order to satisfy a minimum guarantee.

**2. RFQ Process**

2.1. The task order awards will be based on the Government’s “best value” analysis.

2.2. The following RFQ process/analysis will be used in determining task order awards:

- A. Only the Surface Deployment Distribution Command (SDDC) Ordering Office and the Contracting Officer are authorized to order services under this contract.
- B. The requirements will be sent electronically to the multimodal contractors.
- C. All multimodal contractors will be provided an equal opportunity to submit prices electronically for the specific cargo booking within the timeframe specified in the RFQ. (The Government intends for contractors to respond to RFQs within 24-72 hours; however, this time could be shorter during a national emergency). All multimodal contractors will be given the same information and time to respond.
- D. The multimodal contractors have the option to review their existing capacity and respond with a price per pound within the specified response time, unless otherwise directed by TCAQ. Offered prices must be firm for 14 calendar days, unless specified on the RFQ. The price per pound rate shall include any Government ordered accessories.
- E. Quotes received after the cutoff may be considered; however, quotes received late for requirements that have already been awarded will not be considered.
- F. The Government will do a best value analysis as presented in Para 2.4.

- G. Once the Government accepts offered rates and proposals, offerors are obligated to accept the subsequent booking by submission of a booking number through EDI, Ocean Carrier Interface (OCI), or email memorializing the agreement. Offeror shall accept bookings on the same business day if received prior to 1430 Central Time. For a booking received after 1430 Central Time, the offeror shall accept no later than 1200 Central Time of the next business day. The accepted booking constitutes the task order under the contract.
  - H. The Government reserves the right to issue task orders when SDDC Integrated Booking System (IBS) cannot support the booking. Task orders may be for one movement or may include multiple movements for ongoing task orders.
  - I. The Government may make awards at either the PCFN level or to an aggregation of PCFNs. The RFQ bid sheet will identify if the award will be made at the PCFN or aggregation level.
  - J. Special Instructions may be provided for a PCFN on any RFQ. The special instructions will describe any additional conditions associated with the PCFN(s). In the event the special instructions conflict with any PWS paragraph, the special instructions take precedence.
  - K. If the Government requires transportation of cargo through a particular SPOE, SPOD, APOE, and/or APOD, this requirement will be specifically communicated to carriers on the Request for Quotes (RFQ) bid sheet. The term “carrier choice” indicates that the carrier may choose the seaport and/or airport.
  - L. Task orders are awarded on a point to point basis. Rates will be priced on a per pound basis and shall include all services necessary to transport the cargo to/from the door and any accessories ordered, as applicable. In the event cargo is booked to/from a seaport with no provisions for onward movement, the port shall be considered the door.
  - M. All proposed price per pound rates shall be rounded to the nearest whole cent.
- 2.3. The following process will be used in determining task order awards for excepted cargo (as defined in the PWS), for requirements that do not have an established rate, and for special operational circumstances:
- A. The Government will provide all multimodal contractors an equal opportunity to submit a rate electronically for the specific cargo booking. All multimodal contractors will be given the same information and time to respond.
  - B. The contractors have the option to review their existing capacity and respond with a price per pound by the date and time as indicated in the request. The price must be an all-inclusive price per pound.
  - C. The Government will do a best value analysis as presented in Para 2.4.
  - D. Task Order Award is constituted by the Government accepting a quote, which is then definitized by an IBS booking or the issuance of a task order.
- 2.4. The Government’s best value analysis will consider the following factors and sub-factors:
- A. Technical—the Government first evaluates potential contractors on an acceptable (quote clearly meets the minimum requirements of the RFQ)/unacceptable (proposal does not clearly meet the minimum requirements of the RFQ) basis. In order to be considered technically acceptable, offerors must provide the following that clearly meet the requirements:
    - (1) Required Delivery Date
    - (2) All required services
    - (3) Required equipment
    - (4) Meets international, national, local and DoD statutory and regulatory requirements for the

commodity, hazard and security classification, category or threat  
(5) CONOPS report (upon request for Government review)

B. In accordance with the Cargo Preference Act of 1904, the order of priority for cargo moving via ocean is as follows: U.S. Flag vessels (P1), the combination of U.S. Flag and foreign flag vessels (P2), and foreign flag vessels (P3).

C. VISA/CRAF Preference – VISA and CRAF participants receive an equal preference. The VISA and CRAF participation status of the prime and its proposed first tier subcontractor participants will be used in the application of the VISA and CRAF preferences. Multimodal contractors can receive at most one VISA preference and one CRAF preference. VISA participation at the prime and first tier subcontractor level shall result in only one VISA preference. Likewise, CRAF participation at the prime and first tier subcontractor level shall result in only one CRAF preference.

D. Best Value Determination – The following evaluation process will be accomplished for each individual booking:

(1) Contractors meeting the technical requirements above, who are identified as offering the highest identified order of priority for cargo (if moving via ocean) and who are identified as falling within the highest identified VISA/CRAF preference will then be evaluated based upon the factors below.

(2) Evaluation Factors: Past Performance Rating and Price evaluation factors are of approximately equal importance.

(i) Past Performance Rating

(ii) Price

(a) Total all-inclusive rate of all services applicable to the booking. The following formula will be used to determine the price per pound rate on all bookings: Price per pound X estimated dimensional weight or scale weight (whichever is greater)

(iii) If the (i) Past Performance Rating and (ii) Price are equal between two carriers, award will be made to the carrier with the higher past performance score.

E. Contractors who fail to perform proposed carriage using proposed CRAF/VISA carriers/subcontractors will be subject to contract remedies/adverse past performance ratings.

2.5. Variance. Services Ordered via IBS or Contracting Action: If the total billable weight varies more than 25 percent above or below the total booked weight for the Task Order (e.g. total of all PCFN's awarded together), the contractor may request an equitable adjustment to the Government for additional costs incurred by the carrier due to the weight variance in excess of 25%. Supporting documents confirming the additional costs that were incurred by the carrier due to the weight variance in excess of 25% between the booked weight and the billable weight must be submitted to the Contracting Officer no later than 15 calendar days after delivery of the cargo. In addition, the contractor shall submit, to the best of their ability, all appropriate documents requested by the Contracting Officer.

2.6. Competition. Competition among all awarded IDIQ holders on all requirements, for all cargo, and on all routes, is important to the Government on this contract. Accordingly, awardees are highly encouraged, but not required, to submit a quote for all requirements.

## Reports and Formats

Operational Reports to be provided by Contractor:

1. Lift Reports
  - 1.A Sealift (IBS) – Containers/Breakbulk
    - 1.A.1 Required by: PWS Paragraph 1.17
    - 1.A.2 Reports due: Next business day after vessel sail
    - 1.A.3 Medium: Excel attachment uploaded into Pipeline Asset Tool (PAT) per POE
    - 1.A.4 Distribution: Authorized users of ETA/PAT
    - 1.A.5 Required elements:

Mandatory header fields (Populates these fields for all records)

1. SCAC
2. VOYDOC (Select from dropdown)
3. Sail Date
4. POE (Select from dropdown – based on vessel schedule and VOYDOC selection)
5. Vessel Name (select from dropdown – based on vessel schedule and VOYDOC selection)

Excel Columns heading (One row per shipment)

1. Van Type – 35 characters
2. TCN - 17 characters
3. Container # - 11 characters with dash
4. Consignor DODAAC – 6 characters
5. Commercial VOYDOC – 10 characters
6. POD – 3 characters
7. Commercial Booking Number – 25 characters
8. PCFN – 6 characters
9. Vessel Status – 2 characters
10. Consignee DODAAC – 6 characters
11. Cargo Description
12. Cube – Numeric
13. Length – Numeric
14. Width – Numeric
15. Height - Numeric
16. Weight – Numeric
17. Measurement Tons - Numeric
18. Is Booked (Y/N) – Based on if the contractor thinks the item has been booked
19. Has SI (Y/N) – Based on whether contractor has VSI
20. Comment One – free form text field for any contractor comment on the item (250 characters max)
21. Comment Two – free form text field for any contractor comment on the item (250 characters max)

- 1.B Non-IBS Lift
  - 1.B.1 Required by: PWS Paragraph 1.17
  - 1.B.2 Reports due: Within 24hrs of lift
  - 1.B.3 Medium: Excel attachment uploaded into Pipeline Asset Tool (PAT) per POE
  - 1.B.4 Distribution: Authorized users of ETA/PAT
  - 1.B.5 Required elements:

Mandatory header fields (Populates these fields for all records)

1. SCAC
2. TCN

3. Consignee DODAAC
4. Shipper DODAAC
5. Shipper POC
6. POE
7. Sail Date
8. RDD
9. Booking Number
10. Air POE (Select from dropdown – based on vessel schedule and VOYDOC selection)
11. Tail Number

Excel Columns heading (One row per shipment)

1. SCAC – 4 characters
2. TCN - 17 characters
3. DTR Commodity Code - 3 characters
4. Consignor DODAAC – 6 characters
5. Shipper DODAAC – 6 characters
6. Shipper POC – Up to 50 characters
7. POE – 3 characters (AIR)
8. Sail Date – 10 characters (MM/DD/YYYY) (Date of lift)
9. Vessel Name – Leave Blank
10. Flag – Leave Blank
11. POD – 3 characters (AIR)
12. POD Arrival Date – 10 characters (MM/DD/YYYY)
13. VoyDoc – Leave Blank
14. Van Type – Up to 35 characters usually BREAKBULK/CONTAINER
15. Report Type – Up to 20 characters (ex. New, Rolled, Cancelled)
16. Booking Date – 10 characters (MM/DD/YYYY)
17. RDD – 10 characters (MM/DD/YYYY)
18. Version Number
19. Is Active - (Database Flag that indicates whether this is the active version of the uploaded report)
20. Create Date – 10 characters (MM/DD/YYYY) created by database
21. Uploaded by – System Generated
22. Booking Number – Up to 25 characters (RFQ number ex. MM0XXX)
23. Air POE – 3 to 4 characters (IATA or ICAO code)
24. Air POD – 3 to 4 characters (IATA or ICAO code)
25. Tail Number – Up to 4 characters

2. Pre-Arrival Notice

2.1 Required by: PWS Paragraph 1.17

2.2 Reports due: Seven (7) days prior to the scheduled arrival of the delivering vessel or day after sail if less than three (3) days sail time to POD

2.3 Medium: Excel attachment to email

2.4 Distribution: Cognizant SDDC terminal as advised by COR

2.5 Required elements:

TCN

Consignee DODAAC

Container number (when applicable) with alpha prefix, estimated date and time of vessel arrival, and any variation from information previously furnished

Contractor Name

PCFN/Contractor booking number

Vessel name and voyage

VOYDOC

Seal number (when applicable on container shipments)

Date cargo is to arrive  
POD  
Name and voyage number of mother vessel if transshipped

- 3 Contractor Containerization:
- 3.1 Required by: PWS Paragraph 1.17
- 3.2 Reports due: Next business day after Contractor responsible for containerizing cargo at their convenience
- 3.3 Medium: Excel attachment to email
- 3.4 Distribution: Cognizant SDDC terminal as advised by COR
- 3.5 Required elements:

Booked container TCN  
POE  
Cargo TCN, pieces, weight, cube  
Container number and prefix  
Seal number  
Date stuffed  
POD  
Consignee if for inland delivery by the Contractor  
Booking reference  
Booked / scheduled vessel  
Location stuffed

#### 4. Freight Reporting [REMOVED effective Rev 3]

- 5. Cargo not lifted as booked / booked and not lifted:
- 5.1 Required by: PWS Paragraph 1.17
- 5.2 Reports due: Next business day after vessels departs the POE.
- 5.3 Distribution: Cognizant Ordering Officer for the POE
- 5.4 Required elements:

Contractor Name  
POE  
Vessel Name  
Sail date  
TCN  
Container number with prefix  
Reason cargo/container was not lifted as booked

Operational Reports to be provided by the US Government:

#### Cargo Lift – Containers/Breakbulk

- 1.1 Required by: PWS Paragraph 1.17
- 1.2 Reports due: Daily within 4 hours of completion of daily vessel operations
- 1.3 Medium: Excel attachment to email
- 1.4 Distribution: Local Contractor Representative as advised by cognizant COR
- 1.5 Required elements:

Mandatory header fields (Populates these fields for all records)

- 1. SCAC
- 2. VOYDOC
- 3. Sail Date
- 4. Port of Embarkation

## 5. Vessel Name

Excel Columns heading (One row per shipment)

Van Type – 35 characters  
TCN - 17 characters  
Container # - 11 characters with dash (if applicable)  
PCFN – 6 characters  
Consignee DODAAC – 6 characters  
Cargo Description  
Cube – Numeric  
Length – Numeric  
Width – Numeric  
Height - Numeric  
Weight – Numeric  
Measurement Tons - Numeric  
Is Booked in IBS (Y/N) – Based on if the US Government thinks the item has been booked  
Comment One – free form text field for any US Government comment on the item

Cargo Discharge:

- 2.1 Required by: PWS Paragraph 1.17
- 2.2 Reports due: Daily within 4 hours of completion of daily vessel operations
- 2.3 Medium: Excel attachment to email
- 2.4 Distribution: Local Contractor Representative as advised by cognizant COR
- 2.5 Required elements:
  - IBS booked TCN
  - Container number with prefix (if applicable)
  - Port of Debarkation
  - Name and voyage number of vessel discharging cargo
  - Port Call File Number
  - Seal number (if applicable)
  - Date and time the cargo was discharged from the vessel,
  - Seal and/or keyless lock number

(Contractor's Company Letterhead)

Month DD, YYYY

From: (Commercial Carrier)  
To: SDDC G3 (POC)

Subj: (COMPANY NAME) INITIAL/UPDATED YUBIKEY ISSUED LIST

Ref: (a) Multimodal 3 Performance Work Statement

1. As requested by Ref (a) I (Name) (Company Representative) identified and authenticated the following personnel in accordance with Attachment 1 paragraph 5.9.

| Name/ ETA User ID | Authentication |            | Date       |         | Yubikey<br>Number |
|-------------------|----------------|------------|------------|---------|-------------------|
|                   | Document 1     | Document 2 | Authorized | Removed |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |
|                   |                |            |            |         |                   |

(Signature)  
(Name)  
(Company Title)



Month DD, YYYY

From: (Commercial Carrier)

To: SDDC G3 (POC)

Subj: (COMPANY NAME) AUTHORIZED YUBIKEY APPROVER LIST

Ref: (a) Multimodal 3 Performance Work Statement

| Name | Company Position | Signature |
|------|------------------|-----------|
|      |                  |           |
|      |                  |           |
|      |                  |           |
|      |                  |           |

(Signature)

(Name)

(Company Title)

## SHIPMENTS OF DLA PRIME VENDOR CARGO

### 1. Special Provisions for Defense Logistics Agency (DLA) Prime Vendor Program

**1.1 Contractual Intent.** Generally, the terms, conditions and prices of this contract shall apply equally to the transportation of both Government owned and non-Government owned cargo. For example, the standard of liability of a Multimodal (MM) Contractor for loss/damage to cargo is the same in both situations. Also, compensation due the MM Contractor for detention of carrier containers, for port storage, for reefer maintenance, and other matters is the same in both situations. However, experience has demonstrated to the Government that certain matters are properly handled directly between a Prime Vendor and a MM Contractor (the real parties in interest) where non-Government cargo is involved. These matters include, but are not limited to:

- a) Claims procedures and claims dispute resolution procedures related to Prime Vendor cargo and Prime Vendor claims against a MM Contractor for loss/damage to Prime Vendor cargo;
- b) MM Contractor claims against a Prime Vendor for loss/damage to MM Contractor equipment;
- c) MM Contractor claims against a Prime Vendor for detention of MM Contractor equipment;
- d) MM Contractor claims against a Prime Vendor for port storage charges (e.g. while cargo delayed through fault of Prime Vendor or request of Prime Vendor);
- e) MM Contractor claims against a Prime Vendor for trucker wait time (e.g. while cargo delayed through fault of Prime Vendor or request of Prime Vendor);
- f) MM Contractor claims against a Prime Vendor for reefer maintenance (e.g. while reefer in custody of Prime Vendor, or cargo delayed through fault of Prime Vendor or request of Prime Vendor); and,
- g) Claims between the Prime Vendor and MM Contractor for services not ordered by the Government

This stands to reason because the Prime Vendor owns the cargo and because only the Prime Vendor and a MM Contractor have specific, factual knowledge and evidence related to such matters and the delivery location, DLA's Prime Vendor contracts involving the cargo movements outside of the Continental United States (OCONUS) require the Prime Vendor to sign an agreement (which the MM Contractor may accept and seek to supplement) establishing a minimum level of claims processing and dispute resolution procedures. This contract requires the carrier to accept a minimum level agreement to be eligible for the carriage of Prime Vendor cargo OCONUS. The contractual intent is for the Prime Vendor and the MM Contractor to address/resolve such matters directly with each other. The Government customer can be harmed when procedures for resolving such matters between the Prime Vendor and a MM Contractor are not established and problems are not resolved directly between the Prime Vendor and the MM Contractor. However, the MM Contractor may submit claims for issues arising out of the control of both the Prime Vendor and the MM Contractor.

**1.1.1** The following are the responsibility of the MM Contractor and any costs incurred by the Prime Vendor as a result of the MM Contractor's failure to properly perform these services, in accordance with this PWS, shall be borne by the MM Contractor, as shall any other failure of the MM Contractor to perform in accordance with the requirements of this PWS that results in a loss by the Prime Vendor:

- a. Spotting equipment at the date and time agreed upon by the Vendor and the Carrier
- b. Picking-up cargo at the date and time agreed upon by the Vendor and the Carrier
- c. Allowing 2 business days to schedule delivery appointments.
- d. Providing an accurate Bill of Lading (B/L)
- e. Notifying the Government within 24 hours of discovering a seal on any unit of cargo has been broken and/or replaced.
- f. Ensuring refrigerated containers maintain a temperature within three degrees Fahrenheit for chilled cargo, or five degrees Fahrenheit for frozen cargo, of the temperature requested in the booking.

The Prime Vendor will submit any claims related to the above directly to the MM Carrier. The U.S. Government shall not be liable for loss or damage to Prime Vendor cargo. Any discrepancy report or notice of claim for such loss

or damage shall be submitted by the DLA Prime Vendor directly to the MM Contractor for resolution, not to DLA or USTRANSCOM. The MM Contractor shall accept such discrepancy report or notice of claim for such loss or damage from the DLA Prime Vendor, as well as any other communications regarding such loss or damage.

**1.1.2** The following are the responsibility of the Prime Vendor Contractor and any costs incurred by the MM Contractor resulting from the Prime Vendor's failure to properly perform these services, in accordance with the Prime Vendor Contract, shall be borne by the Prime Vendor:

- a. Loading containers at the date and time agreed upon by the Vendor and the Carrier
- b. Providing accurate and timely Health Certificates and Commercial Invoices and Packing Lists
- c. Receiving and unloading of cargo at the date and time agreed upon by the Vendor and the Carrier

The Carrier shall submit any claims related to the above directly to the Prime Vendor. The U.S Government shall not be liable for MM Contractor claims against a Prime Vendor for loss/damage to MM Contractor equipment; MM Contractor claims against a Prime Vendor for detention of MM Contractor equipment; MM Contractor claims against a Prime Vendor for port storage charges (e.g. while cargo delayed through fault of Prime Vendor or request of Prime Vendor); MM Contractor claims against a Prime Vendor for trucker wait time (e.g. while cargo delayed through fault of Prime Vendor or request of Prime Vendor); MM Contractor claims against a Prime Vendor for reefer maintenance (e.g. while reefer in custody of Prime Vendor, or cargo delayed through fault of Prime Vendor or request of Prime Vendor); and claims between the Prime Vendor and MM Contractor for services not ordered by the Government).

**1.1.3** The Government may be responsible for the following and any costs incurred by the MM Contractor resulting from the Government's failure to properly perform these services:

- a. Clearing Customs
- b. Providing accurate and timely shipping instructions

The carrier shall submit claims related to the above directly to the Government.

**1.1.4** The Contractor and the Prime Vendor should include any common issues not delineated above in their Prime Vendor/MM Carrier Agreements for resolution in accordance with the Agreements.

**1.2 Prime Vendor and MM Contractor Agreements for OCONUS:** The MM Contractor is required, after notification of an award of any route for Prime Vendor cargo movement, to enter into a written agreement with the Prime Vendor which shall, at a minimum, include the content in the sample Prime Vendor/MM Carrier Agreement in 2 below. The agreement provides procedures to submit and process claims and resolve disputes arising in connection with U.S. Government ordered transportation services for non-Government owned cargo. The sample Prime Vendor/MM Carrier Agreement is the minimum instrument required to address the matters described in 1.1.1 and 1.1.2. A copy of the agreement and any negotiated supplemental language in respect thereof or changes thereto, shall be furnished to the MM Contracting Officer.

**1.3 Supplementation Encouraged.** The MM Contractor is encouraged, but not required, to supplement the terms of the sample agreement located in paragraph 2 with each Prime Vendor by providing additional details, more specific procedures, or other terms that will facilitate claims processing and dispute resolution. Supplementary language must be consistent with this Attachment. A copy of any supplemental terms must be provided to the MM Contracting Officer. In negotiating any agreement, the MM Contractor should consider that the Prime Vendor may exercise a right of setoff, if any exists, involving a commercial contract or other remedial action against the MM Contractor. Similarly, the MM Contractor may take remedial action or other actions to protect its interests against the Prime Vendor, including the assertion of a lien, if any exists, on Prime Vendor cargo.

## 2. Sample Prime Vendor Carrier Agreement

### **PRIME VENDOR/MM CARRIER AGREEMENT**

WHEREAS, components of the Defense Logistics Agency (DLA) have entered into contracts with various suppliers and distributors under a “Prime Vendor” (PV) program to supply various commodities to U.S. Government agencies and under this program the PVs retain title to such commodities until final delivery;

WHEREAS, DLA’s PV contracts permit components of DLA to order transportation services from commercial carriers under a contract with the United States Transportation Command (USTRANSCOM) known as the Multimodal(MM);

WHEREAS, MM carriers transport PV commodities and return them to PVs at a different location prior to delivery of same by the PV to U.S. Government agencies;

WHEREAS, past experience has demonstrated that PVs and carriers may disagree about claims procedures and claims dispute resolution procedures related to PV cargo, including PV claims against a MM Contractor for loss/damage to PV cargo; MM Contractor claims against a PV for loss/damage to MM Contractor equipment; MM Contractor claims against a PV for detention of MM Contractor equipment; MM Contractor claims against a PV for port storage charges (e.g. while cargo delayed through fault of PV or request of PV); MM Contractor claims against a PV for trucker wait time (e.g. while cargo delayed through fault of PV or request of PV); MM Contractor claims against a PV for reefer maintenance (e.g. while reefer in custody of PV, or cargo delayed through fault of PV or request of PV); and claims between the PV and MM Contractor for services not ordered by the Government;

WHEREAS, \_\_\_\_\_ (hereinafter referred to as The PV) has been awarded contract number \_\_\_\_\_ by \_\_\_\_\_ for the supply of PV cargo;

WHEREAS, one or more carriers under the MM may serve the geographical area covered by said contract and transport PV commodities intended for performance of said contract;

NOW, THEREFORE, in consideration of the mutual promises herein and for the purpose of facilitating minimum standards for the processing of claims and the resolution of disputes between the PV and applicable MM carriers, the PV and any MM carrier accepting the terms of this Agreement (hereinafter referred to as Accepting MM Carrier) agree as follows:

1. The PV and Accepting MM Carrier agree to adhere to the booking requirements of the transportation services ordered. Cargo ordered for delivery to a PV location shall be accepted by the PV upon delivery by the MM carrier. If the cargo is suspected to be in an unacceptable condition for delivery, the PV and MM carrier will abide by the destination services requirements for delivery and receipt notifications. If the cargo is determined to be in an unacceptable condition, the PV and MM Carrier agree to resolve these claims after delivery and subsequent destruction of the cargo.

2. The PV will submit directly to the Accepting MM Carrier (not to DLA or USTRANSCOM) for resolution any discrepancy report or notice of claim for loss/damage to PV cargo, for services not ordered by DLA/USTRANSCOM, or for ending container detention charges or other matters. The Accepting MM Carrier shall accept such report/notice and both parties agree to communicate with each other regarding the processing of claims. The parties may (but are not required to) supplement this minimum level of agreement with additional or more specific terms and conditions consistent with this Agreement and Attachment of the MM contract.

3. The Accepting MM Carrier will submit to the PV (not to DLA or USTRANSCOM) for resolution any notice of claim for equipment loss/damage, container detention, maintenance of refrigerated containers, port storage, services not ordered by DLA/USTRANSCOM, procedures for ending container detention charges, or other matters. The PV shall accept such notice of claims and both parties agree to communicate with each other regarding the processing of

claims. The parties may (but are not required to) supplement this minimum level of agreement with additional or more specific terms and conditions consistent with this Agreement and Attachment 1, PWS in the MM contract.

4. When the claims process does not lead to resolution of the claim, the parties agree to initiate some form of dispute resolution process (such as, but not limited to, direct negotiation, alternative dispute resolution, binding arbitration, and/or court action) that does not involve the U.S. Government as a party (including DLA/USTRANSCOM.) The parties may (but are not required to) supplement this minimum level of agreement with additional or more specific terms and conditions consistent with this Agreement and Attachment 1, PWS in the MM contract.

5. The PV and the Accepting MM Carrier will notify their respective Contracting Officers of any refusal to communicate regarding the processing of a claim and of any failure to attempt to resolve a dispute.

6. The PV and the Accepting MM Carrier acknowledge that the terms of their contracts with the U.S. Government (DLA and USTRANSCOM respectively) generally preclude liability of the Government for the following: PV claims against a MM Contractor for loss/damage to PV cargo; MM Contractor claims against a PV for loss/damage to MM Contractor equipment; MM Contractor claims against a PV for detention of MM Contractor equipment; MM Contractor claims against a PV for port storage charges (e.g. while cargo delayed through fault of PV or request of PV); MM Contractor claims against a PV for trucker wait time (e.g. while cargo delayed through fault of PV or request of PV); MM Contractor claims against a PV for reefer maintenance (e.g. while reefer in custody of PV, or cargo delayed through fault of PV or request of PV); and claims between the PV and MM Contractor for services not ordered by the Government.

7. The parties acknowledge that the terms of the MM contract are applicable to this Agreement and incorporate by reference into this Agreement the MM contract in force at the time PV cargo is booked. For example, the standard of liability of an Accepting MM Carrier for loss/damage to PV cargo is the same as the standard of liability of a MM carrier for loss/damage to government-owned cargo under MM. Similarly, the compensation due an Accepting MM Carrier for damage to its equipment, detention of its containers, port storage of its equipment, and maintenance of its refrigerated containers is the same as the compensation due to a MM Carrier for such matters under MM. Attachment 7 to the MM contract describes specific provisions of the MM contract that are modified to acknowledge that the transportation described herein involves PV cargo, not government-owned cargo; that MM carriers deliver cargo back to the PV, not to the Government; and that the real parties in interest for PV cargo movements are generally the PV and the MM carrier, not the Government.

XXXXXXXX XXXXXXXXXX, INC.  
"The Prime Vendor"

Date:

By:  
Title:

The undersigned, an authorized representative of YYYYYYYYYYYYYY YYYYYYYYYY, INC., hereby accepts and agrees to the terms and provisions above of this Agreement.

YYYYYYYYYYYYYYYYY YYYYYYYYYY, INC.  
"Accepting MM Carrier"

Date:

By:  
Title:

#### SUPPLEMENTAL TERMS AND CONDITIONS

(If the parties agree to supplement this minimum level of agreement with additional or more specific terms and conditions consistent with this Agreement and Attachment of the MM contract, the parties may record their supplemental agreement below OR may record it elsewhere.)



## USTRANSCOM NIST 800-171 Plan of Actions & Milestones POAM



### INSTRUCTIONS

The FARS 52.204-21 tab highlights FAR Clause 52.204-21 the Basic Safeguarding of Covered Contractor Information Systems (DODI 8582.01)

The Carrier Info tab summarizes the NIST 800-171 controls from the control family tabs across the bottom of this workbook.

Please complete

Company name:

Contract number:

Cage code:

Date completed:

Submission Type (Annual or update?)

Point of contact (POC):

POC phone number:

POC e-mail address:

The remainder of tabs across the bottom of this workbook contains a NIST 800-171 control family.

Note: Certain areas of each sheet are not editable. These include "control compliance", "control/objective number", "control family", "DIBCAC score", "control/objective text" and "control type" (columns A through F). These are all locked out.

Overarching control compliance status is controlled by the subobjectives under each control number. Example: 3.1.1 can only be compliant ("yes") if objectives 3.1.1[a] through [f] are all compliant ("yes"). A noncompliant ("no") in any subobjective will automatically render the objective as noncompliant ("no"). Thus, when all subobjectives are in compliance ("yes"), the objective automatically is compliant ("yes").

Noncompliance Detection Date: self explanatory

Scheduled Completion Date: please provide an estimated time the noncompliant control/objective will be corrected.

Actual Completion Date: please annotate the date the noncompliant control/objective was corrected.

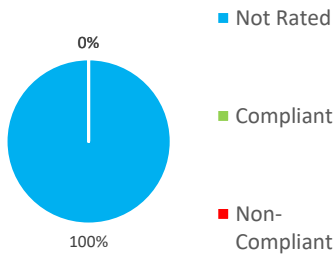
Supporting Documentation/System Controls: briefly describe those technology controls and/or process documents that will be used to achieve compliance with the control/objective requirement. Include details of the implementation/deployment plans and associated milestones. Description should be complete enough so assessors can clearly see a pathway to compliance.

Status/Comments: additional amplifying information regarding the control, objective, documentation, and/or the POAM itself.

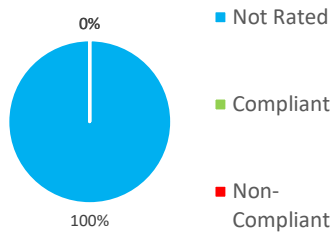
Company name:  
Contract number:  
Cage code:  
Date completed:  
Submission Type (Annual or update?)  
Point of contact (POC):  
POC phone number:  
POC e-mail address:

## Annual Submission

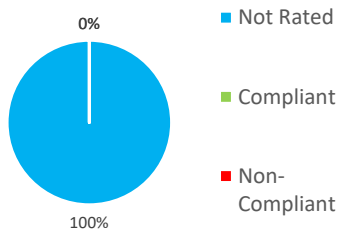
800-171 Controls



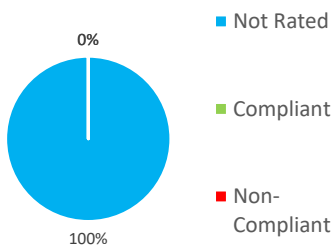
800-171 Objectives



FAR 52.204-21 Controls



FAR 52.204-21 Objectives

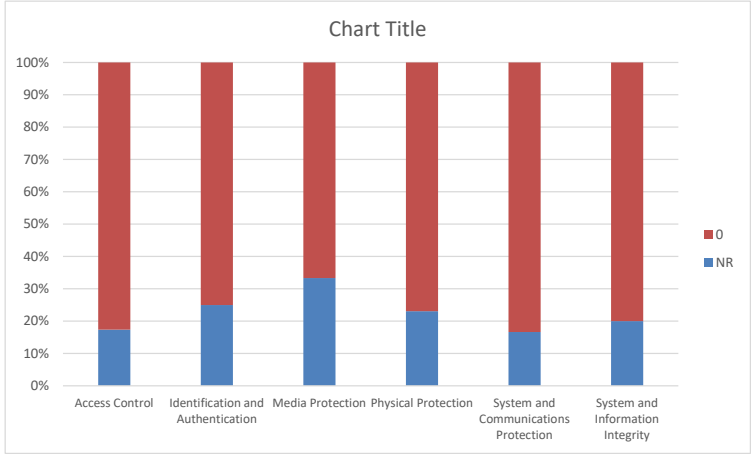
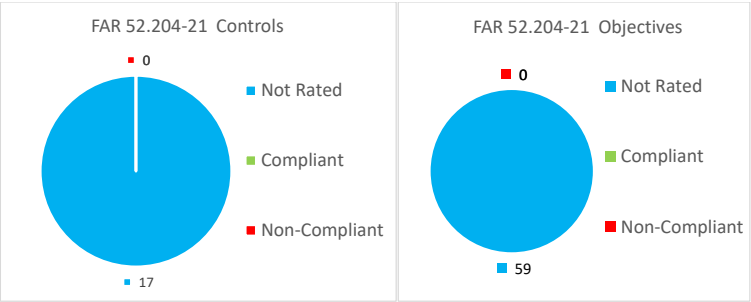


Controls marked requiring Plan of Action and Milestones

no

Controls

Scheduled Completion Date



|                                                              |       |
|--------------------------------------------------------------|-------|
| Basic Safeguarding of Covered Contractor Information Systems | 1     |
| NIST 800-171 Control/Objective Number                        | (All) |

| Count of Compliant                   |    | Column Labels |   |
|--------------------------------------|----|---------------|---|
| Row Labels                           |    | NR            | 0 |
| Access Control                       | 4  | 19            |   |
| Identification and Authentication    | 2  | 6             |   |
| Media Protection                     | 1  | 2             |   |
| Physical Protection                  | 3  | 10            |   |
| System and Communications Protection | 2  | 10            |   |
| System and Information Integrity     | 3  | 12            |   |
| Grand Total                          | 15 | 59            |   |

|                                                                       |    |
|-----------------------------------------------------------------------|----|
| Basic Safeguarding of Covered Contractor Information Systems          | 1  |
| FAR 52.204-21 Controls marked requiring Plan of Action and Milestones | no |

|          |                           |
|----------|---------------------------|
| Controls | Scheduled Completion Date |
|----------|---------------------------|



| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family | Control/Objective Text                                                                                                                                       | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.1.1                                       | Access Control | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).       |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[a]                                    | Access Control | authorized users are identified.                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[b]                                    | Access Control | processes acting on behalf of authorized users are identified.                                                                                               |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[c]                                    | Access Control | devices (and other systems) authorized to connect to the system are identified.                                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[d]                                    | Access Control | system access is limited to authorized users.                                                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[e]                                    | Access Control | system access is limited to processes acting on behalf of authorized users.                                                                                  |                                  |                              |                           |                                            |                   |
|                       | 3.1.1[f]                                    | Access Control | system access is limited to authorized devices (including other systems).                                                                                    |                                  |                              |                           |                                            |                   |
| NR                    | 3.1.2                                       | Access Control | Limit information system access to the types of transactions and functions that authorized users are permitted to execute.                                   |                                  |                              |                           |                                            |                   |
|                       | 3.1.2[a]                                    | Access Control | the types of transactions and functions that authorized users are permitted to execute are defined.                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.1.2[b]                                    | Access Control | system access is limited to the defined types of transactions and functions for authorized users.                                                            |                                  |                              |                           |                                            |                   |
| NR                    | 3.1.3                                       | Access Control | Limit the flow of DoD information to organizations or individuals necessary for the performance of the operationally critical requirements of this contract. |                                  |                              |                           |                                            |                   |
|                       | 3.1.3[a]                                    | Access Control | information flow control policies are defined.                                                                                                               |                                  |                              |                           |                                            |                   |

|    |          |                |                                                                                                                                                             |  |  |  |  |  |
|----|----------|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.1.3[b] | Access Control | methods and enforcement mechanisms for controlling the flow of CUI are defined.                                                                             |  |  |  |  |  |
|    | 3.1.3[c] | Access Control | designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified. |  |  |  |  |  |
|    | 3.1.3[d] | Access Control | authorizations for controlling the flow of CUI are defined.                                                                                                 |  |  |  |  |  |
|    | 3.1.3[e] | Access Control | approved authorizations for controlling the flow of CUI are enforced.                                                                                       |  |  |  |  |  |
| NR | 3.1.4    | Access Control | Separate the duties of individuals to reduce the risk of malevolent activity without collusion.                                                             |  |  |  |  |  |
|    | 3.1.4[a] | Access Control | the duties of individuals requiring separation are defined.                                                                                                 |  |  |  |  |  |
|    | 3.1.4[b] | Access Control | responsibilities for duties that require separation are assigned to separate individuals.                                                                   |  |  |  |  |  |
|    | 3.1.4[c] | Access Control | access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.                               |  |  |  |  |  |
| NR | 3.1.5    | Access Control | Employ the principle of least privilege, including for specific security functions and privileged accounts.                                                 |  |  |  |  |  |
|    | 3.1.5[a] | Access Control | privileged accounts are identified.                                                                                                                         |  |  |  |  |  |
|    | 3.1.5[b] | Access Control | access to privileged accounts is authorized in accordance with the principle of least privilege.                                                            |  |  |  |  |  |
|    | 3.1.5[c] | Access Control | security functions are identified.                                                                                                                          |  |  |  |  |  |
|    | 3.1.5[d] | Access Control | access to security functions is authorized in accordance with the principle of least privilege.                                                             |  |  |  |  |  |

|    |          |                |                                                                                                                                         |  |  |  |  |  |
|----|----------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| NR | 3.1.6    | Access Control | Use non-privileged accounts or roles when accessing nonsecurity functions.                                                              |  |  |  |  |  |
|    | 3.1.6[a] | Access Control | nonsecurity functions are identified.                                                                                                   |  |  |  |  |  |
|    | 3.1.6[b] | Access Control | users are required to use non-privileged accounts or roles when accessing nonsecurity functions.                                        |  |  |  |  |  |
| NR | 3.1.7    | Access Control | Prevent non-privileged users from executing privileged functions and audit the execution of such functions.                             |  |  |  |  |  |
|    | 3.1.7[a] | Access Control | privileged functions are defined.                                                                                                       |  |  |  |  |  |
|    | 3.1.7[b] | Access Control | non-privileged users are defined.                                                                                                       |  |  |  |  |  |
|    | 3.1.7[c] | Access Control | non-privileged users are prevented from executing privileged functions.                                                                 |  |  |  |  |  |
|    | 3.1.7[d] | Access Control | the execution of privileged functions is captured in audit logs.                                                                        |  |  |  |  |  |
| NR | 3.1.8    | Access Control | Limit unsuccessful logon attempts.                                                                                                      |  |  |  |  |  |
|    | 3.1.8[a] | Access Control | the means of limiting unsuccessful logon attempts is defined.                                                                           |  |  |  |  |  |
|    | 3.1.8[b] | Access Control | the defined means of limiting unsuccessful logon attempts is implemented.                                                               |  |  |  |  |  |
| NR | 3.1.9    | Access Control | Provide privacy and security notices consistent with U.S. Government and/or local governmental regulations.                             |  |  |  |  |  |
|    | 3.1.9[a] | Access Control | privacy and security notices required by CUI-specified rules are identified, consistent, and associated with the specific CUI category. |  |  |  |  |  |

|    |           |                |                                                                                                                            |  |  |  |  |  |
|----|-----------|----------------|----------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.1.9[b]  | Access Control | privacy and security notices are displayed.                                                                                |  |  |  |  |  |
| NR | 3.1.10    | Access Control | Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.                |  |  |  |  |  |
|    | 3.1.10[a] | Access Control | the period of inactivity after which the system initiates a session lock is defined.                                       |  |  |  |  |  |
|    | 3.1.10[b] | Access Control | access to the system and viewing of data is prevented by initiating a session lock after the defined period of inactivity. |  |  |  |  |  |
|    | 3.1.10[c] | Access Control | previously visible information is concealed via a pattern-hiding display after the defined period of inactivity.           |  |  |  |  |  |
| NR | 3.1.11    | Access Control | Terminate (automatically) a user session after a defined condition.                                                        |  |  |  |  |  |
|    | 3.1.11[a] | Access Control | conditions requiring a user session to terminate are defined.                                                              |  |  |  |  |  |
|    | 3.1.11[b] | Access Control | a user session is automatically terminated after any of the defined conditions occur.                                      |  |  |  |  |  |
| NR | 3.1.12    | Access Control | Monitor and control remote access sessions.                                                                                |  |  |  |  |  |
|    | 3.1.12[a] | Access Control | remote access sessions are permitted.                                                                                      |  |  |  |  |  |
|    | 3.1.12[b] | Access Control | the types of permitted remote access are identified.                                                                       |  |  |  |  |  |
|    | 3.1.12[c] | Access Control | remote access sessions are controlled.                                                                                     |  |  |  |  |  |
|    | 3.1.12[d] | Access Control | remote access sessions are monitored.                                                                                      |  |  |  |  |  |

|    |           |                |                                                                                                       |  |  |  |  |  |
|----|-----------|----------------|-------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| NR | 3.1.13    | Access Control | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.             |  |  |  |  |  |
|    | 3.1.13[a] | Access Control | cryptographic mechanisms to protect the confidentiality of remote access sessions are identified.     |  |  |  |  |  |
|    | 3.1.13[b] | Access Control | cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented.    |  |  |  |  |  |
| NR | 3.1.14    | Access Control | Route remote access via managed access control points.                                                |  |  |  |  |  |
|    | 3.1.14[a] | Access Control | managed access control points are identified and implemented.                                         |  |  |  |  |  |
|    | 3.1.14[b] | Access Control | remote access is routed through managed network access control points.                                |  |  |  |  |  |
| NR | 3.1.15    | Access Control | Authorize remote execution of privileged commands and remote access to security-relevant information. |  |  |  |  |  |
|    | 3.1.15[a] | Access Control | privileged commands authorized for remote execution are identified.                                   |  |  |  |  |  |
|    | 3.1.15[b] | Access Control | security-relevant information authorized to be accessed remotely is identified.                       |  |  |  |  |  |
|    | 3.1.15[c] | Access Control | the execution of the identified privileged commands via remote access is authorized.                  |  |  |  |  |  |
|    | 3.1.15[d] | Access Control | access to the identified security-relevant information via remote access is authorized.               |  |  |  |  |  |
| NR | 3.1.16    | Access Control | Authorize wireless access prior to allowing such connections.                                         |  |  |  |  |  |
|    | 3.1.16[a] | Access Control | wireless access points are identified.                                                                |  |  |  |  |  |

|    |           |                |                                                                                                                                     |  |  |  |  |  |
|----|-----------|----------------|-------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.1.16[b] | Access Control | wireless access is authorized prior to allowing such connections.                                                                   |  |  |  |  |  |
| NR | 3.1.17    | Access Control | Protect wireless access using authentication and encryption.                                                                        |  |  |  |  |  |
|    | 3.1.17[a] | Access Control | wireless access to the system is protected using authentication.                                                                    |  |  |  |  |  |
|    | 3.1.17[b] | Access Control | wireless access to the system is protected using encryption.                                                                        |  |  |  |  |  |
| NR | 3.1.18    | Access Control | Control connection of mobile devices.                                                                                               |  |  |  |  |  |
|    | 3.1.18[a] | Access Control | mobile devices that process, store, or transmit CUI are identified.                                                                 |  |  |  |  |  |
|    | 3.1.18[b] | Access Control | mobile device connections are authorized.                                                                                           |  |  |  |  |  |
|    | 3.1.18[c] | Access Control | mobile device connections are monitored and logged.                                                                                 |  |  |  |  |  |
| NR | 3.1.19    | Access Control | Provide adequate technical protections on mobile devices and computing platforms that process and/or store contractual information. |  |  |  |  |  |
|    | 3.1.19[a] | Access Control | mobile devices and mobile computing platforms that process, store, or transmit CUI are identified.                                  |  |  |  |  |  |
|    | 3.1.19[b] | Access Control | encryption is employed to protect CUI on identified mobile devices and mobile computing platforms.                                  |  |  |  |  |  |
| NR | 3.1.20    | Access Control | Verify and control/limit connections to and use of external information systems.                                                    |  |  |  |  |  |
|    | 3.1.20[a] | Access Control | connections to external systems are identified.                                                                                     |  |  |  |  |  |

|    |           |                |                                                                                                      |  |  |  |  |  |
|----|-----------|----------------|------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.1.20[b] | Access Control | the use of external systems is identified.                                                           |  |  |  |  |  |
|    | 3.1.20[c] | Access Control | connections to external systems are verified.                                                        |  |  |  |  |  |
|    | 3.1.20[d] | Access Control | the use of external systems is verified.                                                             |  |  |  |  |  |
|    | 3.1.20[e] | Access Control | connections to external systems are controlled/limited.                                              |  |  |  |  |  |
|    | 3.1.20[f] | Access Control | the use of external systems is controlled/limited.                                                   |  |  |  |  |  |
| NR | 3.1.21    | Access Control | Limit use of organizational portable storage devices on external information systems.                |  |  |  |  |  |
|    | 3.1.21[a] | Access Control | the use of portable storage devices containing CUI on external systems is identified and documented. |  |  |  |  |  |
|    | 3.1.21[b] | Access Control | limits on the use of portable storage devices containing CUI on external systems are defined.        |  |  |  |  |  |
|    | 3.1.21[c] | Access Control | the use of portable storage devices containing CUI on external systems is limited as defined.        |  |  |  |  |  |
| NR | 3.1.22    | Access Control | Control DoD information posted or processed on publically accessible systems.                        |  |  |  |  |  |
|    | 3.1.22[a] | Access Control | individuals authorized to post or process information on publicly accessible systems are identified. |  |  |  |  |  |
|    | 3.1.22[b] | Access Control | procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.   |  |  |  |  |  |
|    | 3.1.22[c] | Access Control | a review process is in place prior to posting of any content to publicly accessible systems.         |  |  |  |  |  |

|  |           |                |                                                                                            |  |  |  |  |  |
|--|-----------|----------------|--------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | 3.1.22[d] | Access Control | content on publicly accessible systems is reviewed to ensure that it does not include CUI. |  |  |  |  |  |
|  | 3.1.22[e] | Access Control | mechanisms are in place to remove and address improper posting of CUI.                     |  |  |  |  |  |



| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family            | Control/Objective Text                                                                                                                                                                                                                                                                       | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.2.1                                       | Awareness and<br>Training | Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. |                                  |                              |                           |                                            |                   |
|                       | 3.2.1[a]                                    | Awareness and<br>Training | security risks associated with organizational activities involving CUI are identified.                                                                                                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.2.1[b]                                    | Awareness and<br>Training | policies, standards, and procedures related to the security of the system are identified.                                                                                                                                                                                                    |                                  |                              |                           |                                            |                   |
|                       | 3.2.1[c]                                    | Awareness and<br>Training | managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.                                                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.2.1[d]                                    | Awareness and<br>Training | managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.                                                                                                                        |                                  |                              |                           |                                            |                   |
| NR                    | 3.2.2                                       | Awareness and<br>Training | Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.                                                                                                                                            |                                  |                              |                           |                                            |                   |
|                       | 3.2.2[a]                                    | Awareness and<br>Training | information security-related duties, roles, and responsibilities are defined.                                                                                                                                                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.2.2[b]                                    | Awareness and<br>Training | information security-related duties, roles, and responsibilities are assigned to designated personnel.                                                                                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.2.2[c]                                    | Awareness and<br>Training | personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.                                                                                                                                                               |                                  |                              |                           |                                            |                   |
| NR                    | 3.2.3                                       | Awareness and<br>Training | Provide security awareness training on recognizing and reporting potential indicators of insider threat.                                                                                                                                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.2.3[a]                                    | Awareness and<br>Training | potential indicators associated with insider threats are identified.                                                                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.2.3[b]                                    | Awareness and<br>Training | security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.                                                                                                                                                       |                                  |                              |                           |                                            |                   |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family           | Control/Objective Text                                                                                                                                                                                                      | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.3.1                                       | Audit and Accountability | Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[a]                                    | Audit and Accountability | audit logs needed (i.e., event types to be logged) to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity are specified.                                              |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[b]                                    | Audit and Accountability | the content of audit records needed to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is defined.                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[c]                                    | Audit and Accountability | audit records are created (generated).                                                                                                                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[d]                                    | Audit and Accountability | audit records, once created, contain the defined content.                                                                                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[e]                                    | Audit and Accountability | retention requirements for audit records are defined.                                                                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.3.1[f]                                    | Audit and Accountability | audit records are retained as defined.                                                                                                                                                                                      |                                  |                              |                           |                                            |                   |
| NR                    | 3.3.2                                       | Audit and Accountability | Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.3.2[a]                                    | Audit and Accountability | the content of the audit records needed to support the ability to uniquely trace users to their actions is defined.                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.3.2[b]                                    | Audit and Accountability | audit records, once created, contain the defined content.                                                                                                                                                                   |                                  |                              |                           |                                            |                   |
| NR                    | 3.3.3                                       | Audit and Accountability | Review and update audited events.                                                                                                                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.3.3[a]                                    | Audit and Accountability | a process for determining when to review logged events is defined.                                                                                                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.3.3[b]                                    | Audit and Accountability | event types being logged are reviewed in accordance with the defined review process.                                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.3.3[c]                                    | Audit and Accountability | event types being logged are updated based on the review.                                                                                                                                                                   |                                  |                              |                           |                                            |                   |
| NR                    | 3.3.4                                       | Audit and Accountability | Alert in the event of an audit process failure.                                                                                                                                                                             |                                  |                              |                           |                                            |                   |

|    |          |                          |                                                                                                                                                                                                      |  |  |  |  |  |
|----|----------|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.3.4[a] | Audit and Accountability | personnel or roles to be alerted in the event of an audit logging process failure are identified.                                                                                                    |  |  |  |  |  |
|    | 3.3.4[b] | Audit and Accountability | types of audit logging process failures for which alert will be generated are defined.                                                                                                               |  |  |  |  |  |
|    | 3.3.4[c] | Audit and Accountability | identified personnel or roles are alerted in the event of an audit logging process failure.                                                                                                          |  |  |  |  |  |
| NR | 3.3.5    | Audit and Accountability | Use automated mechanisms to integrate and correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity. |  |  |  |  |  |
|    | 3.3.5[a] | Audit and Accountability | audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity are defined.                         |  |  |  |  |  |
|    | 3.3.5[b] | Audit and Accountability | defined audit record review, analysis, and reporting processes are correlated.                                                                                                                       |  |  |  |  |  |
| NR | 3.3.6    | Audit and Accountability | Provide audit reduction and report generation to support on-demand analysis and reporting.                                                                                                           |  |  |  |  |  |
|    | 3.3.6[a] | Audit and Accountability | an audit record reduction capability that supports on-demand analysis is provided.                                                                                                                   |  |  |  |  |  |
|    | 3.3.6[b] | Audit and Accountability | a report generation capability that supports on-demand reporting is provided.                                                                                                                        |  |  |  |  |  |
| NR | 3.3.7    | Audit and Accountability | Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.                               |  |  |  |  |  |
|    | 3.3.7[a] | Audit and Accountability | internal system clocks are used to generate time stamps for audit records.                                                                                                                           |  |  |  |  |  |
|    | 3.3.7[b] | Audit and Accountability | an authoritative source with which to compare and synchronize internal system clocks is specified.                                                                                                   |  |  |  |  |  |
|    | 3.3.7[c] | Audit and Accountability | internal system clocks used to generate time stamps for audit records are compared to and synchronized with the specified authoritative time source.                                                 |  |  |  |  |  |
| NR | 3.3.8    | Audit and Accountability | Protect audit information and audit tools from unauthorized access, modification, and deletion.                                                                                                      |  |  |  |  |  |
|    | 3.3.8[a] | Audit and Accountability | audit information is protected from unauthorized access.                                                                                                                                             |  |  |  |  |  |
|    | 3.3.8[b] | Audit and Accountability | audit information is protected from unauthorized modification.                                                                                                                                       |  |  |  |  |  |

|    |          |                          |                                                                                                 |  |  |  |  |  |
|----|----------|--------------------------|-------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.3.8[c] | Audit and Accountability | audit information is protected from unauthorized deletion.                                      |  |  |  |  |  |
|    | 3.3.8[d] | Audit and Accountability | audit logging tools are protected from unauthorized access.                                     |  |  |  |  |  |
|    | 3.3.8[e] | Audit and Accountability | audit logging tools are protected from unauthorized modification.                               |  |  |  |  |  |
|    | 3.3.8[f] | Audit and Accountability | audit logging tools are protected from unauthorized deletion.                                   |  |  |  |  |  |
| NR | 3.3.9    | Audit and Accountability | Limit management of audit functionality to a subset of privileged users.                        |  |  |  |  |  |
|    | 3.3.9[a] | Audit and Accountability | a subset of privileged users granted access to manage audit logging functionality is defined.   |  |  |  |  |  |
|    | 3.3.9[b] | Audit and Accountability | management of audit logging functionality is limited to the defined subset of privileged users. |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family              | Control/Objective Text                                                                                                                                                                                                     | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.4.1                                       | Configuration<br>Management | Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[a]                                    | Configuration<br>Management | a baseline configuration is established.                                                                                                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[b]                                    | Configuration<br>Management | the baseline configuration includes hardware, software, firmware, and documentation.                                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[c]                                    | Configuration<br>Management | the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.                                                                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[d]                                    | Configuration<br>Management | a system inventory is established.                                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[e]                                    | Configuration<br>Management | the system inventory includes hardware, software, firmware, and documentation.                                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.4.1[f]                                    | Configuration<br>Management | the inventory is maintained (reviewed and updated) throughout the system development life cycle.                                                                                                                           |                                  |                              |                           |                                            |                   |
| NR                    | 3.4.2                                       | Configuration<br>Management | Establish and enforce security configuration settings for information technology products employed in organizational information systems.                                                                                  |                                  |                              |                           |                                            |                   |
|                       | 3.4.2[a]                                    | Configuration<br>Management | security configuration settings for information technology products employed in the system are established and included in the baseline configuration.                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.4.2[b]                                    | Configuration<br>Management | security configuration settings for information technology products employed in the system are enforced.                                                                                                                   |                                  |                              |                           |                                            |                   |
| NR                    | 3.4.3                                       | Configuration<br>Management | Track, review, approve/disapprove, and audit changes to information systems.                                                                                                                                               |                                  |                              |                           |                                            |                   |
|                       | 3.4.3[a]                                    | Configuration<br>Management | changes to the system are tracked.                                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.4.3[b]                                    | Configuration<br>Management | changes to the system are reviewed.                                                                                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.4.3[c]                                    | Configuration<br>Management | changes to the system are approved or disapproved.                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.4.3[d]                                    | Configuration<br>Management | changes to the system are logged.                                                                                                                                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.4.4                                       | Configuration<br>Management | Analyze the security impact of changes prior to implementation.                                                                                                                                                            |                                  |                              |                           |                                            |                   |
| NR                    | 3.4.5                                       | Configuration<br>Management | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.                                                                                         |                                  |                              |                           |                                            |                   |

|    |          |                          |                                                                                                                           |  |  |  |  |  |
|----|----------|--------------------------|---------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.4.5[a] | Configuration Management | physical access restrictions associated with changes to the system are defined.                                           |  |  |  |  |  |
|    | 3.4.5[b] | Configuration Management | physical access restrictions associated with changes to the system are documented.                                        |  |  |  |  |  |
|    | 3.4.5[c] | Configuration Management | physical access restrictions associated with changes to the system are approved.                                          |  |  |  |  |  |
|    | 3.4.5[d] | Configuration Management | physical access restrictions associated with changes to the system are enforced.                                          |  |  |  |  |  |
|    | 3.4.5[e] | Configuration Management | logical access restrictions associated with changes to the system are defined.                                            |  |  |  |  |  |
|    | 3.4.5[f] | Configuration Management | logical access restrictions associated with changes to the system are documented.                                         |  |  |  |  |  |
|    | 3.4.5[g] | Configuration Management | logical access restrictions associated with changes to the system are approved.                                           |  |  |  |  |  |
|    | 3.4.5[h] | Configuration Management | logical access restrictions associated with changes to the system are enforced.                                           |  |  |  |  |  |
| NR | 3.4.6    | Configuration Management | Employ the principle of least functionality by configuring the information system to provide only essential capabilities. |  |  |  |  |  |
|    | 3.4.6[a] | Configuration Management | essential system capabilities are defined based on the principle of least functionality.                                  |  |  |  |  |  |
|    | 3.4.6[b] | Configuration Management | the system is configured to provide only the defined essential capabilities.                                              |  |  |  |  |  |
| NR | 3.4.7    | Configuration Management | Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.               |  |  |  |  |  |
|    | 3.4.7[a] | Configuration Management | essential programs are defined.                                                                                           |  |  |  |  |  |
|    | 3.4.7[b] | Configuration Management | the use of nonessential programs is defined.                                                                              |  |  |  |  |  |
|    | 3.4.7[c] | Configuration Management | the use of nonessential programs is restricted, disabled, or prevented as defined.                                        |  |  |  |  |  |
|    | 3.4.7[d] | Configuration Management | essential functions are defined.                                                                                          |  |  |  |  |  |
|    | 3.4.7[e] | Configuration Management | the use of nonessential functions is defined.                                                                             |  |  |  |  |  |
|    | 3.4.7[f] | Configuration Management | the use of nonessential functions is restricted, disabled, or prevented as defined.                                       |  |  |  |  |  |

|    |          |                          |                                                                                                                                                                                              |  |  |  |  |  |
|----|----------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.4.7[g] | Configuration Management | essential ports are defined.                                                                                                                                                                 |  |  |  |  |  |
|    | 3.4.7[h] | Configuration Management | the use of nonessential ports is defined.                                                                                                                                                    |  |  |  |  |  |
|    | 3.4.7[i] | Configuration Management | the use of nonessential ports is restricted, disabled, or prevented as defined.                                                                                                              |  |  |  |  |  |
|    | 3.4.7[j] | Configuration Management | essential protocols are defined.                                                                                                                                                             |  |  |  |  |  |
|    | 3.4.7[k] | Configuration Management | the use of nonessential protocols is defined.                                                                                                                                                |  |  |  |  |  |
|    | 3.4.7[l] | Configuration Management | the use of nonessential protocols is restricted, disabled, or prevented as defined.                                                                                                          |  |  |  |  |  |
|    | 3.4.7[m] | Configuration Management | essential services are defined.                                                                                                                                                              |  |  |  |  |  |
|    | 3.4.7[n] | Configuration Management | the use of nonessential services is defined.                                                                                                                                                 |  |  |  |  |  |
|    | 3.4.7[o] | Configuration Management | the use of nonessential services is restricted, disabled, or prevented as defined.                                                                                                           |  |  |  |  |  |
| NR | 3.4.8    | Configuration Management | Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software. |  |  |  |  |  |
|    | 3.4.8[a] | Configuration Management | a policy specifying whether whitelisting or blacklisting is to be implemented is specified.                                                                                                  |  |  |  |  |  |
|    | 3.4.8[b] | Configuration Management | the software allowed to execute under whitelisting or denied use under blacklisting is specified.                                                                                            |  |  |  |  |  |
|    | 3.4.8[c] | Configuration Management | whitelisting to allow the execution of authorized software or blacklisting to prevent the use of unauthorized software is implemented as specified.                                          |  |  |  |  |  |
| NR | 3.4.9    | Configuration Management | Control and monitor user-installed software.                                                                                                                                                 |  |  |  |  |  |
|    | 3.4.9[a] | Configuration Management | a policy for controlling the installation of software by users is established.                                                                                                               |  |  |  |  |  |
|    | 3.4.9[b] | Configuration Management | installation of software by users is controlled based on the established policy.                                                                                                             |  |  |  |  |  |
|    | 3.4.9[c] | Configuration Management | installation of software by users is monitored.                                                                                                                                              |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family                    | Control/Objective Text                                                                                                                                     | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.5.1                                       | Identification and Authentication | Identify information system users, processes acting on behalf of users, or devices.                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.5.1[a]                                    | Identification and Authentication | system users are identified.                                                                                                                               |                                  |                              |                           |                                            |                   |
|                       | 3.5.1[b]                                    | Identification and Authentication | processes acting on behalf of users are identified.                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.5.1[c]                                    | Identification and Authentication | devices accessing the system are identified.                                                                                                               |                                  |                              |                           |                                            |                   |
| NR                    | 3.5.2                                       | Identification and Authentication | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |                                  |                              |                           |                                            |                   |
|                       | 3.5.2[a]                                    | Identification and Authentication | the identity of each user is authenticated or verified as a prerequisite to system access.                                                                 |                                  |                              |                           |                                            |                   |
|                       | 3.5.2[b]                                    | Identification and Authentication | the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.                                   |                                  |                              |                           |                                            |                   |
|                       | 3.5.2[c]                                    | Identification and Authentication | the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.                         |                                  |                              |                           |                                            |                   |
| NR                    | 3.5.3                                       | Identification and Authentication | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.                      |                                  |                              |                           |                                            |                   |
|                       | 3.5.3[a]                                    | Identification and Authentication | privileged accounts are identified.                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.5.3[b]                                    | Identification and Authentication | multifactor authentication is implemented for local access to privileged accounts.                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.5.3[c]                                    | Identification and Authentication | multifactor authentication is implemented for network access to privileged accounts.                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.5.3[d]                                    | Identification and Authentication | multifactor authentication is implemented for network access to non-privileged accounts.                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.5.4                                       | Identification and Authentication | Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.                                            |                                  |                              |                           |                                            |                   |



|    |          |                                   |                                                                                                           |  |  |  |  |  |
|----|----------|-----------------------------------|-----------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| NR | 3.5.5    | Identification and Authentication | Prevent reuse of identifiers for a defined period.                                                        |  |  |  |  |  |
|    | 3.5.5[a] | Identification and Authentication | a period within which identifiers cannot be reused is defined.                                            |  |  |  |  |  |
|    | 3.5.5[b] | Identification and Authentication | reuse of identifiers is prevented within the defined period.                                              |  |  |  |  |  |
| NR | 3.5.6    | Identification and Authentication | Disable identifiers after a defined period of inactivity.                                                 |  |  |  |  |  |
|    | 3.5.6[a] | Identification and Authentication | a period of inactivity after which an identifier is disabled is defined.                                  |  |  |  |  |  |
|    | 3.5.6[b] | Identification and Authentication | identifiers are disabled after the defined period of inactivity.                                          |  |  |  |  |  |
| NR | 3.5.7    | Identification and Authentication | Enforce a minimum password complexity and change of characters when new passwords are created.            |  |  |  |  |  |
|    | 3.5.7[a] | Identification and Authentication | password complexity requirements are defined.                                                             |  |  |  |  |  |
|    | 3.5.7[b] | Identification and Authentication | password change of character requirements are defined.                                                    |  |  |  |  |  |
|    | 3.5.7[c] | Identification and Authentication | minimum password complexity requirements as defined are enforced when new passwords are created.          |  |  |  |  |  |
|    | 3.5.7[d] | Identification and Authentication | minimum password change of character requirements as defined are enforced when new passwords are created. |  |  |  |  |  |
| NR | 3.5.8    | Identification and Authentication | Prohibit password reuse for a specified number of generations.                                            |  |  |  |  |  |
|    | 3.5.8[a] | Identification and Authentication | the number of generations during which a password cannot be reused is specified.                          |  |  |  |  |  |
|    | 3.5.8[b] | Identification and Authentication | reuse of passwords is prohibited during the specified number of generations.                              |  |  |  |  |  |

|    |           |                                   |                                                                                                  |  |  |  |  |  |
|----|-----------|-----------------------------------|--------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.5.9     | Identification and Authentication | Allow temporary password use for system logons with an immediate change to a permanent password. |  |  |  |  |  |
| NR | 3.5.10    | Identification and Authentication | Store and transmit only encrypted representation of passwords.                                   |  |  |  |  |  |
|    | 3.5.10[a] | Identification and Authentication | passwords are cryptographically protected in storage.                                            |  |  |  |  |  |
|    | 3.5.10[b] | Identification and Authentication | passwords are cryptographically protected in transit.                                            |  |  |  |  |  |
|    | 3.5.11    | Identification and Authentication | Obscure feedback of authentication information.                                                  |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family    | Control/Objective Text                                                                                                                                                                                     | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.6.1                                       | Incident Response | Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities. |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[a]                                    | Incident Response | an operational incident-handling capability is established.                                                                                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[b]                                    | Incident Response | the operational incident-handling capability includes preparation.                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[c]                                    | Incident Response | the operational incident-handling capability includes detection.                                                                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[d]                                    | Incident Response | the operational incident-handling capability includes analysis.                                                                                                                                            |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[e]                                    | Incident Response | the operational incident-handling capability includes containment.                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[f]                                    | Incident Response | the operational incident-handling capability includes recovery.                                                                                                                                            |                                  |                              |                           |                                            |                   |
|                       | 3.6.1[g]                                    | Incident Response | the operational incident-handling capability includes user response activities.                                                                                                                            |                                  |                              |                           |                                            |                   |
| NR                    | 3.6.2                                       | Incident Response | Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[a]                                    | Incident Response | incidents are tracked.                                                                                                                                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[b]                                    | Incident Response | incidents are documented.                                                                                                                                                                                  |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[c]                                    | Incident Response | authorities to whom incidents are to be reported are identified.                                                                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[d]                                    | Incident Response | organizational officials to whom incidents are to be reported are identified.                                                                                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[e]                                    | Incident Response | identified authorities are notified of incidents.                                                                                                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.6.2[f]                                    | Incident Response | identified organizational officials are notified of incidents.                                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.6.3                                       | Incident Response | Test the organizational incident response capability.                                                                                                                                                      |                                  |                              |                           |                                            |                   |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family | Control/Objective Text                                                                                                                                                               | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
|                       | 3.7.1                                       | Maintenance    | Perform maintenance on organizational information systems.                                                                                                                           |                                  |                              |                           |                                            |                   |
| NR                    | 3.7.2                                       | Maintenance    | Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.7.2[a]                                    | Maintenance    | tools used to conduct system maintenance are controlled.                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.7.2[b]                                    | Maintenance    | techniques used to conduct system maintenance are controlled.                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.7.2[c]                                    | Maintenance    | mechanisms used to conduct system maintenance are controlled.                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.7.2[d]                                    | Maintenance    | personnel used to conduct system maintenance are controlled.                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.7.3                                       | Maintenance    | Ensure equipment removed for off-site maintenance is sanitized of DoD information.                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.7.4                                       | Maintenance    | Check media containing diagnostic and test programs for malicious code before the media are used in the information system.                                                          |                                  |                              |                           |                                            |                   |
| NR                    | 3.7.5                                       | Maintenance    | Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. |                                  |                              |                           |                                            |                   |
|                       | 3.7.5[a]                                    | Maintenance    | multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.7.5[b]                                    | Maintenance    | nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.7.6                                       | Maintenance    | Supervise the maintenance activities of maintenance personnel without required access authorization.                                                                                 |                                  |                              |                           |                                            |                   |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family   | Control/Objective Text                                                                                                                                                           | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.8.1                                       | Media Protection | Protect (i.e., physically control and securely store) system media containing DoD information, both paper and digital.                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.8.1[a]                                    | Media Protection | paper media containing CUI is physically controlled.                                                                                                                             |                                  |                              |                           |                                            |                   |
|                       | 3.8.1[b]                                    | Media Protection | digital media containing CUI is physically controlled.                                                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.8.1[c]                                    | Media Protection | paper media containing CUI is securely stored.                                                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.8.1[d]                                    | Media Protection | digital media containing CUI is securely stored.                                                                                                                                 |                                  |                              |                           |                                            |                   |
|                       | 3.8.2                                       | Media Protection | Limit access to DoD information on system media to authorized users.                                                                                                             |                                  |                              |                           |                                            |                   |
| NR                    | 3.8.3                                       | Media Protection | Sanitize or destroy system media containing DoD information before disposal or release for reuse.                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.8.3[a]                                    | Media Protection | system media containing CUI is sanitized or destroyed before disposal.                                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.8.3[b]                                    | Media Protection | system media containing CUI is sanitized before it is released for reuse.                                                                                                        |                                  |                              |                           |                                            |                   |
| NR                    | 3.8.4                                       | Media Protection | Mark media with privacy and security notices consistent with U.S. Government and/or local government regulations.                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.8.4[a]                                    | Media Protection | media containing CUI is marked with applicable CUI markings.                                                                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.8.4[b]                                    | Media Protection | media containing CUI is marked with distribution limitations.                                                                                                                    |                                  |                              |                           |                                            |                   |
| NR                    | 3.8.5                                       | Media Protection | Control access to and maintain accountability for media containing DoD information.                                                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.8.5[a]                                    | Media Protection | access to media containing CUI is controlled.                                                                                                                                    |                                  |                              |                           |                                            |                   |
|                       | 3.8.5[b]                                    | Media Protection | accountability for media containing CUI is maintained during transport outside of controlled areas.                                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.8.6                                       | Media Protection | Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. |                                  |                              |                           |                                            |                   |

|  |       |                  |                                                                                                                                                                                                        |  |  |  |  |  |
|--|-------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | 3.8.7 | Media Protection | Control the use of removable media on information system components.                                                                                                                                   |  |  |  |  |  |
|  | 3.8.8 | Media Protection | Prohibit the use of portable storage devices when such devices have no identifiable owner.                                                                                                             |  |  |  |  |  |
|  | 3.8.9 | Media Protection | Provide information backup procedures (frequency, timeframe for storage, etc.) for DoD data located on contractor systems. Protect the confidentiality of backup materials containing DoD information. |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family     | Control/Objective Text                                                                                                                                                 | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual Completion<br>Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
|                       | 3.9.1                                       | Personnel Security | Screen individuals prior to authorizing access to organizational systems containing DoD information.                                                                   |                                  |                              |                           |                                            |                   |
| NR                    | 3.9.2                                       | Personnel Security | Ensure that DoD information and organizational systems containing DoD information are protected during and after personnel actions such as terminations and transfers. |                                  |                              |                           |                                            |                   |
|                       | 3.9.2[a]                                    | Personnel Security | a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.                                            |                                  |                              |                           |                                            |                   |
|                       | 3.9.2[b]                                    | Personnel Security | system access and credentials are terminated consistent with personnel actions such as termination or transfer.                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.9.2[c]                                    | Personnel Security | the system is protected during and after personnel transfer actions.                                                                                                   |                                  |                              |                           |                                            |                   |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family      | Control/Objective Text                                                                                                                       | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.10.1                                      | Physical Protection | Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. |                                  |                              |                           |                                            |                   |
|                       | 3.10.1[a]                                   | Physical Protection | authorized individuals allowed physical access are identified.                                                                               |                                  |                              |                           |                                            |                   |
|                       | 3.10.1[b]                                   | Physical Protection | physical access to organizational systems is limited to authorized individuals.                                                              |                                  |                              |                           |                                            |                   |
|                       | 3.10.1[c]                                   | Physical Protection | physical access to equipment is limited to authorized individuals.                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.10.1[d]                                   | Physical Protection | physical access to operating environments is limited to authorized individuals.                                                              |                                  |                              |                           |                                            |                   |
| NR                    | 3.10.2                                      | Physical Protection | Protect and monitor the physical facility and support infrastructure for those information systems.                                          |                                  |                              |                           |                                            |                   |
|                       | 3.10.2[a]                                   | Physical Protection | the physical facility where organizational systems reside is protected.                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.10.2[b]                                   | Physical Protection | the support infrastructure for organizational systems is protected.                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.10.2[c]                                   | Physical Protection | the physical facility where organizational systems reside is monitored.                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.10.2[d]                                   | Physical Protection | the support infrastructure for organizational systems is monitored.                                                                          |                                  |                              |                           |                                            |                   |
| NR                    | 3.10.3                                      | Physical Protection | Escort visitors and monitor visitor activity.                                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.10.3[a]                                   | Physical Protection | visitors are escorted.                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.10.3[b]                                   | Physical Protection | visitor activity is monitored.                                                                                                               |                                  |                              |                           |                                            |                   |
|                       | 3.10.4                                      | Physical Protection | Maintain audit logs of physical access.                                                                                                      |                                  |                              |                           |                                            |                   |
| NR                    | 3.10.5                                      | Physical Protection | Control and manage physical access devices.                                                                                                  |                                  |                              |                           |                                            |                   |
|                       | 3.10.5[a]                                   | Physical Protection | physical access devices are identified.                                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.10.5[b]                                   | Physical Protection | physical access devices are controlled.                                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.10.5[c]                                   | Physical Protection | physical access devices are managed.                                                                                                         |                                  |                              |                           |                                            |                   |
| NR                    | 3.10.6                                      | Physical Protection | Enforce safeguarding measures for DoD Information at alternate work sites (e.g., telework sites).                                            |                                  |                              |                           |                                            |                   |
|                       | 3.10.6[a]                                   | Physical Protection | safeguarding measures for CUI are defined for alternate work sites.                                                                          |                                  |                              |                           |                                            |                   |
|                       | 3.10.6[b]                                   | Physical Protection | safeguarding measures for CUI are enforced for alternate work sites.                                                                         |                                  |                              |                           |                                            |                   |



| Compliant (Yes/No) | NIST 800-171 Control/Objective Number | Control Family  | Control/Objective Text                                                                                                                                                                                                                                                                     | Non-Compliance Detection Date | Scheduled Completion Date | Actual Completion Date | Supporting Documentation / System Controls | Status / Comments |
|--------------------|---------------------------------------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|---------------------------|------------------------|--------------------------------------------|-------------------|
| NR                 | 3.11.1                                | Risk Assessment | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of DoD information. |                               |                           |                        |                                            |                   |
|                    | 3.11.1[a]                             | Risk Assessment | the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.                                                                                                                                                                              |                               |                           |                        |                                            |                   |
|                    | 3.11.1[b]                             | Risk Assessment | risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.                                                                        |                               |                           |                        |                                            |                   |
| NR                 | 3.11.2                                | Risk Assessment | Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.                                                                                                                                         |                               |                           |                        |                                            |                   |
|                    | 3.11.2[a]                             | Risk Assessment | the frequency to scan for vulnerabilities in organizational systems and applications is defined.                                                                                                                                                                                           |                               |                           |                        |                                            |                   |
|                    | 3.11.2[b]                             | Risk Assessment | vulnerability scans are performed on organizational systems with the defined frequency.                                                                                                                                                                                                    |                               |                           |                        |                                            |                   |
|                    | 3.11.2[c]                             | Risk Assessment | vulnerability scans are performed on applications with the defined frequency.                                                                                                                                                                                                              |                               |                           |                        |                                            |                   |
|                    | 3.11.2[d]                             | Risk Assessment | vulnerability scans are performed on organizational systems when new vulnerabilities are identified.                                                                                                                                                                                       |                               |                           |                        |                                            |                   |
|                    | 3.11.2[e]                             | Risk Assessment | vulnerability scans are performed on applications when new vulnerabilities are identified.                                                                                                                                                                                                 |                               |                           |                        |                                            |                   |
| NR                 | 3.11.3                                | Risk Assessment | Remediate vulnerabilities in accordance with assessments of risk.                                                                                                                                                                                                                          |                               |                           |                        |                                            |                   |
|                    | 3.11.3[a]                             | Risk Assessment | vulnerabilities are identified.                                                                                                                                                                                                                                                            |                               |                           |                        |                                            |                   |
|                    | 3.11.3[b]                             | Risk Assessment | vulnerabilities are remediated in accordance with risk assessments.                                                                                                                                                                                                                        |                               |                           |                        |                                            |                   |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family      | Control/Objective Text                                                                                                                                                                                                                     | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.12.1                                      | Security Assessment | Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.                                                                                           |                                  |                              |                           |                                            |                   |
|                       | 3.12.1[a]                                   | Security Assessment | the frequency of security control assessments is defined.                                                                                                                                                                                  |                                  |                              |                           |                                            |                   |
|                       | 3.12.1[b]                                   | Security Assessment | security controls are assessed with the defined frequency to determine if the controls are effective in their application.                                                                                                                 |                                  |                              |                           |                                            |                   |
| NR                    | 3.12.2                                      | Security Assessment | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.12.2[a]                                   | Security Assessment | deficiencies and vulnerabilities to be addressed by the plan of action are identified.                                                                                                                                                     |                                  |                              |                           |                                            |                   |
|                       | 3.12.2[b]                                   | Security Assessment | a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.                                                                                                                       |                                  |                              |                           |                                            |                   |
|                       | 3.12.2[c]                                   | Security Assessment | the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.                                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.12.3                                      | Security Assessment | Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.                                                                                                                    |                                  |                              |                           |                                            |                   |
| NR                    | 3.12.4                                      | Security Assessment | Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. |                                  |                              |                           |                                            |                   |

|  |           |                     |                                                                                                                 |  |  |  |  |  |
|--|-----------|---------------------|-----------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|  | 3.12.4[a] | Security Assessment | a system security plan is developed.                                                                            |  |  |  |  |  |
|  | 3.12.4[b] | Security Assessment | the system boundary is described and documented in the system security plan.                                    |  |  |  |  |  |
|  | 3.12.4[c] | Security Assessment | the system environment of operation is described and documented in the system security plan.                    |  |  |  |  |  |
|  | 3.12.4[d] | Security Assessment | the security requirements identified and approved by the designated authority as non-applicable are identified. |  |  |  |  |  |
|  | 3.12.4[e] | Security Assessment | the method of security requirement implementation is described and documented in the system security plan.      |  |  |  |  |  |
|  | 3.12.4[f] | Security Assessment | the relationship with or connection to other systems is described and documented in the system security plan.   |  |  |  |  |  |
|  | 3.12.4[g] | Security Assessment | the frequency to update the system security plan is defined.                                                    |  |  |  |  |  |
|  | 3.12.4[h] | Security Assessment | system security plan is updated with the defined frequency.                                                     |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family                             | Control/Objective Text                                                                                                                                                                                                           | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.13.1                                      | System and<br>Communications<br>Protection | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[a]                                   | System and<br>Communications<br>Protection | the external system boundary is defined.                                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[b]                                   | System and<br>Communications<br>Protection | key internal system boundaries are defined.                                                                                                                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[c]                                   | System and<br>Communications<br>Protection | communications are monitored at the external system boundary.                                                                                                                                                                    |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[d]                                   | System and<br>Communications<br>Protection | communications are monitored at key internal boundaries.                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[e]                                   | System and<br>Communications<br>Protection | communications are controlled at the external system boundary.                                                                                                                                                                   |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[f]                                   | System and<br>Communications<br>Protection | communications are controlled at key internal boundaries.                                                                                                                                                                        |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[g]                                   | System and<br>Communications<br>Protection | communications are protected at the external system boundary.                                                                                                                                                                    |                                  |                              |                           |                                            |                   |
|                       | 3.13.1[h]                                   | System and<br>Communications<br>Protection | communications are protected at key internal boundaries.                                                                                                                                                                         |                                  |                              |                           |                                            |                   |
| NR                    | 3.13.2                                      | System and<br>Communications<br>Protection | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.                                         |                                  |                              |                           |                                            |                   |
|                       | 3.13.2[a]                                   | System and<br>Communications<br>Protection | architectural designs that promote effective information security are identified.                                                                                                                                                |                                  |                              |                           |                                            |                   |
|                       | 3.13.2[b]                                   | System and<br>Communications<br>Protection | software development techniques that promote effective information security are identified.                                                                                                                                      |                                  |                              |                           |                                            |                   |
|                       | 3.13.2[c]                                   | System and<br>Communications<br>Protection | systems engineering principles that promote effective information security are identified.                                                                                                                                       |                                  |                              |                           |                                            |                   |

|    |           |                                      |                                                                                                                                             |  |  |  |  |  |
|----|-----------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.13.2[d] | System and Communications Protection | identified architectural designs that promote effective information security are employed.                                                  |  |  |  |  |  |
|    | 3.13.2[e] | System and Communications Protection | identified software development techniques that promote effective information security are employed.                                        |  |  |  |  |  |
|    | 3.13.2[f] | System and Communications Protection | identified systems engineering principles that promote effective information security are employed.                                         |  |  |  |  |  |
| NR | 3.13.3    | System and Communications Protection | Separate user functionality from information system management functionality.                                                               |  |  |  |  |  |
|    | 3.13.3[a] | System and Communications Protection | user functionality is identified.                                                                                                           |  |  |  |  |  |
|    | 3.13.3[b] | System and Communications Protection | system management functionality is identified.                                                                                              |  |  |  |  |  |
|    | 3.13.3[c] | System and Communications Protection | user functionality is separated from system management functionality.                                                                       |  |  |  |  |  |
|    | 3.13.4    | System and Communications Protection | Prevent unauthorized and unintended information transfer via shared system resources.                                                       |  |  |  |  |  |
| NR | 3.13.5    | System and Communications Protection | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.          |  |  |  |  |  |
|    | 3.13.5[a] | System and Communications Protection | publicly accessible system components are identified.                                                                                       |  |  |  |  |  |
|    | 3.13.5[b] | System and Communications Protection | subnetworks for publicly accessible system components are physically or logically separated from internal networks.                         |  |  |  |  |  |
| NR | 3.13.6    | System and Communications Protection | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). |  |  |  |  |  |
|    | 3.13.6[a] | System and Communications Protection | network communications traffic is denied by default.                                                                                        |  |  |  |  |  |
|    | 3.13.6[b] | System and Communications Protection | network communications traffic is allowed by exception.                                                                                     |  |  |  |  |  |

|    |            |                                      |                                                                                                                                                                                            |  |  |  |  |  |
|----|------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.13.7     | System and Communications Protection | Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.  |  |  |  |  |  |
| NR | 3.13.8     | System and Communications Protection | Implement cryptographic mechanisms to prevent unauthorized disclosure of DoD information during transmission when possible unless otherwise protected by alternate physical safeguards.    |  |  |  |  |  |
|    | 3.13.8[a]  | System and Communications Protection | cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.                                                                                                |  |  |  |  |  |
|    | 3.13.8[b]  | System and Communications Protection | alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.                                                                                         |  |  |  |  |  |
|    | 3.13.8[c]  | System and Communications Protection | either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.                                          |  |  |  |  |  |
| NR | 3.13.9     | System and Communications Protection | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.                                                  |  |  |  |  |  |
|    | 3.13.9[a]  | System and Communications Protection | a period of inactivity to terminate network connections associated with communications sessions is defined.                                                                                |  |  |  |  |  |
|    | 3.13.9[b]  | System and Communications Protection | network connections associated with communications sessions are terminated at the end of the sessions.                                                                                     |  |  |  |  |  |
|    | 3.13.9[c]  | System and Communications Protection | network connections associated with communications sessions are terminated after the defined period of inactivity.                                                                         |  |  |  |  |  |
| NR | 3.13.10    | System and Communications Protection | Establish and manage cryptographic keys for cryptography employed in the information system;                                                                                               |  |  |  |  |  |
|    | 3.13.10[a] | System and Communications Protection | cryptographic keys are established whenever cryptography is employed.                                                                                                                      |  |  |  |  |  |
|    | 3.13.10[b] | System and Communications Protection | cryptographic keys are managed whenever cryptography is employed.                                                                                                                          |  |  |  |  |  |
|    | 3.13.11    | System and Communications Protection | Employ FIPS-validated cryptography when used to protect the confidentiality of DoD information within the organization's systems and when possible when transmitting to external entities. |  |  |  |  |  |
| NR | 3.13.12    | System and Communications Protection | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.                                                     |  |  |  |  |  |

|           |            |                                      |                                                                                  |  |  |  |  |  |
|-----------|------------|--------------------------------------|----------------------------------------------------------------------------------|--|--|--|--|--|
|           | 3.13.12[a] | System and Communications Protection | collaborative computing devices are identified.                                  |  |  |  |  |  |
|           | 3.13.12[b] | System and Communications Protection | collaborative computing devices provide indication to users of devices in use.   |  |  |  |  |  |
|           | 3.13.12[c] | System and Communications Protection | remote activation of collaborative computing devices is prohibited.              |  |  |  |  |  |
| <b>NR</b> | 3.13.13    | System and Communications Protection | Control and monitor the use of mobile code.                                      |  |  |  |  |  |
|           | 3.13.13[a] | System and Communications Protection | use of mobile code is controlled.                                                |  |  |  |  |  |
|           | 3.13.13[b] | System and Communications Protection | use of mobile code is monitored.                                                 |  |  |  |  |  |
| <b>NR</b> | 3.13.14    | System and Communications Protection | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. |  |  |  |  |  |
|           | 3.13.14[a] | System and Communications Protection | use of Voice over Internet Protocol (VoIP) technologies is controlled.           |  |  |  |  |  |
|           | 3.13.14[b] | System and Communications Protection | use of Voice over Internet Protocol (VoIP) technologies is monitored.            |  |  |  |  |  |
|           | 3.13.15    | System and Communications Protection | Protect the authenticity of communications sessions.                             |  |  |  |  |  |
|           | 3.13.16    | System and Communications Protection | Protect the confidentiality of DoD information at rest.                          |  |  |  |  |  |

| Compliant<br>(Yes/No) | NIST 800-171<br>Control/Objective<br>Number | Control Family                         | Control/Objective Text                                                                                        | Non-Compliance<br>Detection Date | Scheduled<br>Completion Date | Actual<br>Completion Date | Supporting Documentation / System Controls | Status / Comments |
|-----------------------|---------------------------------------------|----------------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------|------------------------------|---------------------------|--------------------------------------------|-------------------|
| NR                    | 3.14.1                                      | System and<br>Information<br>Integrity | Identify, report, and correct information and<br>information system flaws in a timely manner.                 |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[a]                                   | System and<br>Information<br>Integrity | the time within which to identify system flaws is<br>specified.                                               |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[b]                                   | System and<br>Information<br>Integrity | system flaws are identified within the specified time<br>frame.                                               |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[c]                                   | System and<br>Information<br>Integrity | the time within which to report system flaws is<br>specified.                                                 |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[d]                                   | System and<br>Information<br>Integrity | system flaws are reported within the specified time<br>frame.                                                 |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[e]                                   | System and<br>Information<br>Integrity | the time within which to correct system flaws is<br>specified.                                                |                                  |                              |                           |                                            |                   |
|                       | 3.14.1[f]                                   | System and<br>Information<br>Integrity | system flaws are corrected within the specified time<br>frame.                                                |                                  |                              |                           |                                            |                   |
| NR                    | 3.14.2                                      | System and<br>Information<br>Integrity | Provide protection from malicious code at appropriate<br>locations within organizational information systems. |                                  |                              |                           |                                            |                   |
|                       | 3.14.2[a]                                   | System and<br>Information<br>Integrity | designated locations for malicious code protection are<br>identified.                                         |                                  |                              |                           |                                            |                   |



|    |           |                                  |                                                                                                                                                   |  |  |  |  |  |
|----|-----------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
|    | 3.14.2[b] | System and Information Integrity | protection from malicious code at designated locations is provided.                                                                               |  |  |  |  |  |
| NR | 3.14.3    | System and Information Integrity | Monitor information system security alerts and advisories and take appropriate actions in response.                                               |  |  |  |  |  |
|    | 3.14.3[a] | System and Information Integrity | response actions to system security alerts and advisories are identified.                                                                         |  |  |  |  |  |
|    | 3.14.3[b] | System and Information Integrity | system security alerts and advisories are monitored.                                                                                              |  |  |  |  |  |
|    | 3.14.3[c] | System and Information Integrity | actions in response to system security alerts and advisories are taken.                                                                           |  |  |  |  |  |
|    | 3.14.4    | System and Information Integrity | Update malicious code protection mechanisms when new releases are available.                                                                      |  |  |  |  |  |
| NR | 3.14.5    | System and Information Integrity | Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. |  |  |  |  |  |
|    | 3.14.5[a] | System and Information Integrity | the frequency for malicious code scans is defined.                                                                                                |  |  |  |  |  |
|    | 3.14.5[b] | System and Information Integrity | malicious code scans are performed with the defined frequency.                                                                                    |  |  |  |  |  |
|    | 3.14.5[c] | System and Information Integrity | real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.                         |  |  |  |  |  |

|    |           |                                  |                                                                                                                                              |  |  |  |  |  |
|----|-----------|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| NR | 3.14.6    | System and Information Integrity | Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. |  |  |  |  |  |
|    | 3.14.6[a] | System and Information Integrity | the system is monitored to detect attacks and indicators of potential attacks.                                                               |  |  |  |  |  |
|    | 3.14.6[b] | System and Information Integrity | inbound communications traffic is monitored to detect attacks and indicators of potential attacks.                                           |  |  |  |  |  |
|    | 3.14.6[c] | System and Information Integrity | outbound communications traffic is monitored to detect attacks and indicators of potential attacks.                                          |  |  |  |  |  |
| NR | 3.14.7    | System and Information Integrity | Identify unauthorized use of the information system.                                                                                         |  |  |  |  |  |
|    | 3.14.7[a] | System and Information Integrity | authorized use of the system is defined.                                                                                                     |  |  |  |  |  |
|    | 3.14.7[b] | System and Information Integrity | unauthorized use of the system is identified.                                                                                                |  |  |  |  |  |

REGISTER OF WAGE DETERMINATIONS UNDER THE  
SERVICE CONTRACT ACT

By direction of the Secretary of Labor

Daniel W. Simms Director      Division of Wage  
Determinations

U.S. DEPARTMENT OF LABOR  
EMPLOYMENT STANDARDS ADMINISTRATION  
WAGE AND HOUR DIVISION  
WASHINGTON, D.C. 20210

Wage Determination No.: 2015-0213

Revision No.: 32

Date of Last Revision: 7/7/2023

Note: Contracts subject to the Service Contract Act are generally required to pay at least the applicable minimum wage rate required under Executive Order 14026 or Executive Order 13658.

|                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| If the contract is entered into <u>on or after January 30, 2022</u> , or the contract is renewed or extended (e.g., an option is exercised) on or after January 30, 2022: | <ul style="list-style-type: none"><li>• Executive Order 14026 generally applies to contract.</li><li>• The contractor must pay all covered workers <b>at least \$16.20 per hour</b> (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in 2023.</li></ul> |
| If the contract was awarded <u>on or between January 1, 2015 and January 29, 2022</u> , and the contract is <u>not</u> renewed or extended on or after January 30, 2022:  | <ul style="list-style-type: none"><li>• Executive Order 13658 generally applies to the contract.</li><li>• The contractor must pay all covered workers at least \$12.15 per hour (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in 2023.</li></ul>    |

The applicable Executive Order minimum wage rate will be adjusted annually. Additional information on contractor requirements and worker protections under the Executive Orders is available at [www.dol.gov/whd/govcontracts](http://www.dol.gov/whd/govcontracts).

Nationwide applicable in: Alaska, Alabama, American Samoa, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Guam, Hawaii, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, New Hampshire, New Jersey, New Mexico, New York, North Carolina, Oregon, Puerto Rico, Rhode Island, South Carolina, Texas, Virginia, Washington, Wisconsin

**\*\*Fringe Benefits Required Follow the Occupational Listing\*\***

Employed on contract for tugboats and other coastal vessels.

| OCCUPATION CODE - TITLE          | FOOTNOTE | RATE          |
|----------------------------------|----------|---------------|
| 47080 - General Vessel Assistant |          | 327 .75 Daily |
| (not set) - Captain, Harbor Tug  |          | 495 .97 Daily |
| (not set) - Deckhand, Harbor Tug |          | 312 .16 Daily |
| (not set) - Engineer, Harbor Tug |          | 417 .17 Daily |

\*\*\*Workers in this classification may be entitled to a higher minimum wage under Executive Order 14026 (\$16.20 per hour) or 13658 (\$12.15 per hour). Please see the Note at the top of the wage determination for more information. Please also note that the minimum wage requirements of Executive Order 14026 and 13658 are not currently being enforced as to contracts or contract-like instruments entered into with the federal government in connection with seasonal recreational services or seasonal recreational equipment rental for the general public on federal lands.

---

Note: Executive Order (EO) 13706, Establishing Paid Sick Leave for Federal Contractors, applies to all contracts subject to the Service Contract Act for which the contract is awarded (and any solicitation was issued) on or after January 1, 2017. If this contract is covered by the EO, the contractor must provide employees with 1 hour of paid sick leave for every 30 hours they work, up to 56 hours of paid sick leave each year. Employees must be permitted to use paid sick leave for their own illness, injury or other health-related needs, including preventive care; to assist a family member (or person who is like family to the employee) who is ill, injured, or has other health-related needs, including preventive care; or for reasons resulting from, or to assist a family member (or person who is like family to the employee) who is the victim of, domestic violence, sexual assault, or stalking. Additional information on contractor requirements and worker protections under the EO is available at [www.dol.gov/whd/govcontracts](http://www.dol.gov/whd/govcontracts).

ALL OCCUPATIONS LISTED ABOVE RECEIVE THE FOLLOWING BENEFITS:

HEALTH & WELFARE: \$4.98 per hour, up to 40 hours per week, or \$199.20 per week or \$863.20 per month

HEALTH & WELFARE EO 13706: \$4.57 per hour, up to 40 hours per week, or \$182.80 per week, or \$792.13 per month

(Hawaii): \$2.15 per hour, up to 40 hours per week, or \$86.00 per week, or \$372.67 per month for all employees on whose behalf the contractor provides health care benefits pursuant to the Hawaii prepaid Health Care Act. For those employees who are not receiving health care benefits mandated by the Hawaii prepaid Health Care Act, the new health and welfare benefit rate will be \$4.80 per hour, up to 40 hours per week.

HEALTH & WELFARE (Hawaii) EO 13706: \$1.74 per hour, up to 40 hours per week, or \$69.60 per week, or \$301.60 per month for all employees on whose behalf the contractor provides health care benefits pursuant to the Hawaii prepaid Health Care Act. For those employees who are not receiving health care benefits mandated by the Hawaii prepaid Health Care Act, the new health and welfare benefit rate will be \$4.57 per hour, up to 40 hours per week.\*

\*This rate is to be used only when compensating employees for performance on an SCA-covered contract also covered by EO 13706, Establishing Paid Sick Leave for Federal Contractors. A contractor may not receive credit toward its SCA obligations for any paid sick leave provided pursuant to EO 13706.

VACATION: 2 weeks paid vacation after 1 year of service with a contractor or successor, 3 weeks after 5 years, and 4 weeks after 15 years. Length of service includes the whole span of continuous service with the present contractor or successor, wherever employed, and with the predecessor contractors in the performance of similar work at the same Federal facility. (Reg. 29 CFR 4.173)

HOLIDAYS: A minimum of eleven paid holidays per year: New Year's Day, Martin Luther King Jr.'s Birthday, Washington's Birthday, Memorial Day, Juneteenth National Independence Day, Independence Day, Labor Day, Columbus Day, Veterans' Day, Thanksgiving Day, and Christmas Day. (A contractor may substitute for any of the named holidays another day off with pay in accordance with a plan communicated to the employees involved.) (See 29 CFR 4.174)

**\*\* UNIFORM ALLOWANCE \*\***

If employees are required to wear uniforms in the performance of this contract (either by the terms of the Government contract, by the employer, by the state or local law, etc.), the cost of furnishing such uniforms and maintaining (by laundering or dry cleaning) such uniforms is an expense that may not be borne by an employee where such cost reduces the hourly rate below that required by the wage determination. The Department of Labor will accept payment in accordance with the following standards as compliance:

The contractor or subcontractor is required to furnish all employees with an adequate number of uniforms without cost or to reimburse employees for the actual cost of the uniforms. In addition, where uniform cleaning and maintenance is made the responsibility of the employee, all contractors and subcontractors subject to this wage determination shall (in the absence of a bona fide collective bargaining agreement providing for a different amount, or the furnishing of contrary affirmative proof as to the actual cost), reimburse all employees for such cleaning and maintenance at a rate of \$3.35 per week (or \$.67 cents per day). However, in those instances where the uniforms furnished are made of "wash and wear" materials, may be routinely washed and dried with other personal garments, and do not require any special treatment such as dry cleaning, daily washing, or commercial laundering in order to meet the cleanliness or appearance standards set by the terms of the Government contract, by the contractor, by law, or by the nature of the work, there is no requirement that employees be reimbursed for uniform maintenance costs.

**\*\* SERVICE CONTRACT ACT DIRECTORY OF OCCUPATIONS \*\***

The duties of employees under job titles listed are those described in the "Service Contract Act Directory of Occupations", Fifth Edition (Revision 1), dated September 2015, unless otherwise indicated.

**\*\* REQUEST FOR AUTHORIZATION OF ADDITIONAL CLASSIFICATION AND WAGE RATE, Standard Form 1444 (SF-1444) \*\***

**Conformance Process:**

The contracting officer shall require that any class of service employee which is not listed herein and which is to be employed under the contract (i.e., the work to be performed is not performed by any classification listed in the wage determination), be classified by the contractor so as to provide a reasonable relationship (i.e., appropriate level of skill comparison) between such unlisted classifications and the classifications listed in the wage determination (See 29 CFR 4.6(b)(2)(i)). Such conforming procedures shall be initiated by the contractor prior to the performance of contract work by such unlisted class(es) of employees (See 29 CFR 4.6(b)(2)(ii)). The Wage and Hour Division shall make a final determination of conformed classification, wage rate, and/or fringe benefits which shall be paid to all employees performing in the classification from the first day of work on which contract work is performed by them in the classification. Failure to pay such unlisted employees the compensation agreed upon by the interested parties and/or fully determined by the Wage and Hour Division retroactive to the date such class of employees commenced contract work shall be a violation of the Act and this contract. (See 29 CFR 4.6(b)(2)(v)). When multiple wage determinations are included in a contract, a separate SF-1444 should be prepared for each wage determination to which a class(es) is to be conformed.

The process for preparing a conformance request is as follows:

- 1) When preparing the bid, the contractor identifies the need for a conformed occupation(s) and computes a proposed rate(s).
- 2) After contract award, the contractor prepares a written report listing in order the proposed classification title(s), a Federal grade equivalency (FGE) for each proposed classification(s), job description(s), and rationale for proposed wage rate(s), including information regarding the agreement or disagreement of the authorized representative of the employees involved, or where there is no authorized representative, the employees themselves. This report should be submitted to the contracting officer no later than 30 days after such unlisted class(es) of employees performs any contract work.
- 3) The contracting officer reviews the proposed action and promptly submits a report of the action, together with the agency's recommendations and pertinent information including the position of the contractor and the employees, to the U.S. Department of Labor, Wage and Hour Division, for review (See 29 CFR 4.6(b)(2)(ii)).
- 4) Within 30 days of receipt, the Wage and Hour Division approves, modifies, or disapproves the action via transmittal to the agency contracting officer, or notifies the contracting officer that additional time will be required to process the request.
- 5) The contracting officer transmits the Wage and Hour Division's decision to the contractor.
- 6) Each affected employee shall be furnished by the contractor with a written copy of such determination or it shall be posted as a part of the wage determination (See 29 CFR 4.6(b)(2)(iii)).

Information required by the Regulations must be submitted on SF-1444 or bond paper.

When preparing a conformance request, the "Service Contract Act Directory of Occupations" should be used to compare job definitions to ensure that duties requested are not performed by a classification already listed in the wage determination. Remember, it is not the job title, but the required tasks that determine whether a class is included in an established wage determination. Conformances may not be used to artificially split, combine, or subdivide classifications listed in the wage determination (See 29 CFR 4.152(c)(1)).

**\*\* OCCUPATIONS NOT INCLUDED IN THE SCA DIRECTORY OF OCCUPATIONS \*\***

**Captain, Harbor Tug**

Qualified tug master and operator in charge of the tugboat, its personnel, its operation and maintenance. The Captain is a radio operator, understands and operates radar and other navigational aids used in conjunction with tug-ship operations and tug-barge operations both harbor and ocean. This person must also be qualified in administrative ship business and overall charge of maintenance of the vessel. Must hold appropriate Coast Guard documentation/license.

**Deckhand, Harbor Tug**

Qualified seaman capable of performing all duties related to tugboat servicing ships and barges both in the harbor and at sea. Must hold appropriate Coast Guard documentation/license.

**Engineer, Harbor Tug**

Qualified engineer in the operation, the maintenance, both corrective and preventative, and overall supervisor in the proper operation and maintenance of all machinery, both main and auxiliary and electrical and other mechanical gear aboard the tugboat. Also must have administrative ability to keep records and maintain the inventory of parts, tools, fuel, etc. Must hold appropriate Coast Guard documentation/license.

## Sexual Harassment/Assault Response & Prevention (SHARP)

### 1. Definitions. As used in this policy

1.A. "Sexual Assault" means - A crime defined as intentional sexual contact, characterized by use of force, physical threat or abuse of authority or when the victim does not or cannot consent. Sexual assault includes rape, nonconsensual sodomy (oral or anal sex), indecent assault (unwanted, inappropriate sexual contact or fondling), or attempts to commit these acts. Sexual assault can occur without regard to gender or spousal relationship or age of victim. "Consent" will not be deemed or construed to mean the failure by the victim to offer physical resistance. Consent is not given when a person uses force, threat of force, or coercion or when the victim is asleep, incapacitated, or unconscious.

1.B. "Sexual Harassment" is a form of sex discrimination that involves unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when:

1.B.1. Submission to such conduct is made either explicitly or implicitly a term or condition of a person's job, pay, or career, or

1.B.2. Submission to or rejection of such conduct by a person is used as a basis for career or employment decisions affecting that person, or

1.B.3. Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creates an intimidating, hostile, or offensive working environment. This definition emphasizes that workplace conduct, to be actionable as "abusive work environment" harassment, need not result in concrete psychological harm to the victim, but rather need only be so severe or pervasive that a reasonable person would perceive, and the victim does perceive, the work environment as hostile or offensive. Any person in a supervisory or command position who uses or condones any form of sexual behavior to control, influence, or affect the career, pay, or job of an employee is engaging in sexual harassment. Similarly, any employee who makes deliberate or repeated unwelcome verbal comments, gestures, or physical contact of a sexual nature in the workplace is also engaging in sexual harassment.

1.C. Categories of sexual harassment are:

1.C.1. Verbal - Examples include telling sexual jokes; using sexually explicit profanity, threats, sexually oriented cadences, or sexual comments; whistling in a sexually suggestive manner; and describing certain attributes of one's physical appearance in a sexual manner.

1.C.2. Nonverbal - Examples include staring at someone, blowing kisses, winking, or licking one's lips in a suggestive manner. The term may also include printed material (for example, displaying sexually oriented pictures or cartoons); using sexually oriented screen savers on one's computer; or sending sexually oriented notes, letters, faxes or email.

1.C.3. Physical Contact - Examples include touching, patting, pinching, bumping, grabbing, cornering, or blocking a passageway; kissing; and providing unsolicited back or neck rubs.

### 2. Policy

- 2.A. The Department of Defense has adopted a policy to prevent sexual assault and sexual harassment.
- 2.B. Contractors and contractor employees working in Afghanistan shall not:
  - 2.B.1. Commit acts of sexual assault against any person on any camp, post, installation, or other United States enclave; or
  - 2.B.2. Sexually harass any person on any camp, post, installation, or other United States enclave.
- 3. Contractor Requirements.
  - 3.A. The Contractor shall have a written Sexual Assault/Sexual Harassment Policy
    - 3.A.1. The contractor shall have a written sexual assault/sexual harassment policy published to all employees performing work in Afghanistan that addresses, at a minimum, the following: (i) the definitions of sexual assault and sexual harassment as defined above in paragraph 1a; (ii) a description of sexual harassment (iii) the Company's internal complaint process and the company's internal process for adjudication; (iv) the available channels through which an employee can report a sexual assault; and (v) protection against retaliation, coercion, and reprisal.
    - 3.A.2. The policy shall address that victims of sexual assault shall be protected, treated with dignity and respect, and shall receive timely access to comprehensive healthcare (medical and mental health) treatment, including emergency care treatment and services. Emergency care consists of emergency healthcare and the offer of a sexual assault forensic examination (SAFE) consistent with the Department of Justice protocol. The victim shall be advised that even if a SAFE is declined, the victim is encouraged (but not mandated) to seek medical care. Contractor employees are only eligible to file an Unrestricted Report. Contractor employees will also be offered LIMITED Sexual Assault Prevention and Response or SAPR services, meaning the assistance of a Sexual Assault Response Coordinator (SARC) and a SAPR Victim Advocate (VA) while undergoing emergency care OCONUS. These limited emergency medical services (at a Military Treatment Facility) and SAPR services shall be provided at no cost by the USG to all DoD contractor personnel. Limited medical services are: a SAFE exam and consultation regarding further care in accordance with DoDI 6495.02.
    - 3.A.3. The contractor shall designate an employee credentialed in Victim Advocacy as the company POC (for more information regarding credentialing as a Victim Advocate visit the National Advocate Credentialing Program (NACP): <https://www.thenacp.org/>).
    - 3.A.4. The Contractor shall provide a Sexual Assault/Sexual Harassment and Awareness Training Plan that includes a schedule for all training. The Plan shall identify the methods of training (e.g. classroom, on-line, etc), as well as intervals (e.g. quarterly) for refresher training, as applicable. The plan shall address (but not be limited to) such things as: procedures for training each employee, training record retention, method/mode of instruction, instructor accreditation, on-line/web-based resources/training aids. The Contractor's Training shall address, at a minimum, the following:
      - 3.A.4.1. Defining what constitutes sexual assault and sexual harassment.
      - 3.A.4.2. Explaining sexual assault is a crime.



3.A.4.3. Defining the meaning of “consent” as defined in DoDD 6495.01 (Sexual Assault Prevention and Response Program, SAPR).

3.A.4.4. Addressing individual accountability and the potential for Uniformed Code of Military Justice (UCMJ) violations.

3.A.4.5. Explaining victims rights under the UCMJ (to include consideration of the victim's preference whether the office should be prosecuted by court-martial or in a civilian court).

3.A.4.6. Explaining the distinction between sexual harassment and sexual assault and that both are unacceptable forms of behavior even though they may have different penalties. Emphasizing the distinction between civil and criminal actions.

3.A.4.7. Explaining Unrestricted Reporting

3.A.4.8. Providing an awareness of the SAPR program, as well as the roles and responsibilities of company managers, including all available resources for victims.

3.B. The Contractor shall notify its employees of:

3.B.1. The Department of Defense's policies regarding Sexual Assault/Sexual Harassment; and

3.B.2. The actions that will be taken against employees for violations of this policy. Such actions may include, but are not limited to, removal from the contract, reduction in benefits, or termination of employment;

3.C. The Contractor shall take appropriate action, up to and including termination, against employees or Subcontractors that violate the policy in paragraph (b).

3.D. The Contractor shall inform the Contracting Officer immediately of

3.D.1. Any information it receives from any source (including host country law enforcement) that alleges a Contractor employee, Subcontractor, or Subcontractor employee has engaged in conduct that violates this policy; and

3.D.2. Any actions taken against Contractor employees, Subcontractors, or Subcontractor employees pursuant to this policy.

4. Remedies.

4.A. In addition to other remedies available to the Government, the Contractor's failure to comply with the requirements of paragraphs (c), (d), or (f) of this policy may result in:

4.A.1. Requiring the Contractor to remove a Contractor employee or employees from the performance of the contract;

4.A.2. Requiring the Contractor to terminate a subcontract;

4.A.3. Suspension of contract payments;

- 4.A.4. Loss of award fee, consistent with the award fee plan, for the performance period in which the Government determined Contractor non-compliance;
  - 4.A.5. Termination of the contract for default or cause, in accordance with the termination clause of this contract; or
  - 4.A.6. Suspension or debarment.
5. Subcontracts

The Contractor shall include the substance of this policy, including this paragraph (f), in all subcontracts.

6. Mitigating Factor.

The Contracting Officer may consider whether the Contractor had a Sexual Assault Prevention and Response training program at the time of the violation as a mitigating factor when determining remedies. Additional information about Sexual Assault Prevention and Response training programs can be found at the Department of Defense Sexual Assault Prevention and Response Home Page, <http://www.sapr.mil>."

|                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Foreign Subcontractor Air Carriers (Airlines) must submit the AOC along with the data provided in this spreadsheet.                                                                                                                                              |
| 2. Foreign Subcontractor Air Carrier data previously submitted must be resubmitted if the provided AOC has expired and an update is required for continued use. Update the Air Carrier Submission Tab and place a "Y" in the Update AOC space provided in column O. |
| 3. Foreign Subcontractor Business Licenses shall be provided for the Contractor to legally operate in each country they service.                                                                                                                                    |
| 4. Ensure you populate the appropriate tab(s) below to ensure Acquisitions can determine what type of service the foreign subcontractor provides.                                                                                                                   |
| 5. For any columns that aren't applicable, please enter N/A.                                                                                                                                                                                                        |
| 6. Submissions shall include all foreign subcontractors utilized in the six (6) months preceeding the report date. For example, the report due 15 January would report foreign subcontractors utilized between 1 July - 31 December.                                |
| 7. The tabs/service providers listed are not all inclusive. Please use the 'other' tab for any other type of service provider category.                                                                                                                             |

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owner(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and<br>e-mail address(es) | Air Operations<br>Certificate (AOC)<br>Provided? | New<br>AOC? | Updated<br>AOC? | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------|--------------------------------------------------|-------------|-----------------|-----------------------------------------------|
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------|--------------------------------------------------|-------------|-----------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

|                              |                                                |                                     |          |                  |           |                                         |            |             |                                                                           |                                                       | Required Business Licenses Provided?      |
|------------------------------|------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------|------------|-------------|---------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|
| Legal Company Name (English) | Legal Company Name (Native Language, if known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or Alternate Company Names | Fax Number | Website URL | International Civil Aviation Organization (ICAO) or equivalent designator | Owners(s)/ Director(s) name(s) and e-mail address(es) | Manager(s) name(s) and e-mail address(es) |

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-<br>mail address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or Alternate Company Names | Fax Number | Website URL | International Civil Aviation Organization (ICAO) or equivalent designator | Owners(s)/ Director(s) name(s) and e-mail address(es) | Manager(s) name(s) and e-mail address(es) | Required Business Licenses Provided? |
|---------------------------------|------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------|------------|-------------|---------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|--------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-mail<br>address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|-----------------------------------------------|



Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or Alternate Company Names | Fax Number | Website URL | International Civil Aviation Organization (ICAO) or equivalent designator | Owners(s)/ Director(s) name(s) and e-mail address(es) | Manager(s) name(s) and e-mail address(es) | Required Business Licenses Provided? |
|---------------------------------|------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------|------------|-------------|---------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|--------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-mail<br>address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or Alternate Company Names | Fax Number | Website URL | International Civil Aviation Organization (ICAO) or equivalent designator | Owners(s)/ Director(s) name(s) and e-mail address(es) | Manager(s) name(s) and e-mail address(es) | Required Business Licenses Provided? |
|---------------------------------|------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------|------------|-------------|---------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------------|--------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-mail<br>address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-mail<br>address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-mail<br>address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------|-----------------------------------------------|

Industry Partner Name  
Contract No.  
Date:

| Legal Company Name<br>(English) | Legal Company Name (Native Language, if<br>known) | Company Address (including Country) | POC Name | POC Phone Number | POC Email | Any Previous or<br>Alternate Company<br>Names | Fax Number | Website URL | International Civil Aviation<br>Organization (ICAO) or<br>equivalent designator | Owners(s)/ Director(s) name(s)<br>and e-mail address(es) | Manager(s) name(s) and e-<br>mail address(es) | Required<br>Business<br>Licenses<br>Provided? |
|---------------------------------|---------------------------------------------------|-------------------------------------|----------|------------------|-----------|-----------------------------------------------|------------|-------------|---------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------|-----------------------------------------------|