UNITED STATES TRANSPORTATION COMMAND (USTRANSCOM)

Contract GS-06F-0626Z
Order No. HTC711-11-F-D051
1 October 2011
(Solicitation: HTC711-11-R-003)

Corporate Services Support

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

1. REQUISITION NUMBER	PAGE 1 OF 70

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS-06F-0626Z	01-Oct-2011	HTC711-11-F-D051		

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

9. ISSUED BY CODE HTC711

USTRANSCOM-AQ - HTC711
508 SCOTT DR
SCOTT AFB IL 62225-5357

TEL: CONTACT BUYER
FAX: CONTACT BUYER

10. THIS ACQUISITION IS
- [ ] UNRESTRICTED
- [X] SET ASIDE: 100 % FOR
  - [X] SB
  - [ ] HUBZONE SB
  - [ ] 8(A)
  - [ ] SVC-DISABLED VET-OWNED SB
  - [ ] EMERGING SB

SIZE STD: 25M NAICS: 541513

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
- [ ] SEE SCHEDULE

12. DISCOUNT TERMS
Net 30 Days

- [ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
- [ ] RFQ
- [ ] IFB
- [ ] RFP

15. DELIVER TO CODE F3ST95

USTC/J8 - F3ST95
TERRANCE THREAT
508 SCOTT DR
SCOTT AFB IL 62225-5357

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/OFFEROR CODE 1HXK0

WEBSTER DATA COMMUNICATION, INC.
JAY LEE
11250 WAPLES MILL RD STE 430
FAIRFAX VA 22030-7400

TEL. 571-748-4455 FACILITY CODE

18a. PAYMENT WILL BE MADE BY CODE F87700

DFAS-LIMESTONE DEAMS - F87700
ACCTG DISB STA NR 387700
DFAS DEAMS
27 ARKANSAS RD
LIMESTONE ME 04751-6216

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

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

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

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)
$8,790,021.52

- [ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED
- [X] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [X] ARE [ ] ARE NOT ATTACHED

28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES
- [X] 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 HEREIN.

REF: Offer dated 14 July 2011

29. AWARD OF CONTRACT: REFERENCE
- [ ] OFFER DATED 14-Jul-2011 . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: SEE SCHEDULE

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)	31c. DATE SIGNED
	(b)(6)	08-Sep-2011

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)
		TERESA M. FRANCOEUR / CONTRACTING OFFICER TEL: 618-220-7053 EMAIL: terri.francoeur@ustranscom.mil

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV 3/2005)
Prescribed by GSA
FAR (48 CFR) 53.212

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS (CONTINUED)		PAGE 2 OF 70

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

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 ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

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	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	CSS:SS Task Area 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 1, Contract Level and Task Order Management, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	(b)(4)
			NET AMT		(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0002	CSS:SS Task Area 2, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 1: SDDC Helpdesk and Desktop Customer Support, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	(b)(4)
			NET AMT		(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003	CSS:SS Task Area 2, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 2: USTRANSCOM Service Desk Support, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	(b)(4)

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004 OPTION	CSS:SS Task Area 2, Subtask 3 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task 2, Subtask 3: USTRANSCOM Service Desk Extended Support, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4)

TOT ESTIMATED PRICE (b)(4)

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005		12	Months	(b)(4)	(b)(4)

CSS:SS Task Area 3 Support
FFP
Corporate Services Support: Service Support - Labor for Task Area 3, Computer System Maintenance and Logistics Support, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0006		12	Months	(b)(4)	(b)(4)

CSS:SS Task Area 4, Subtask 1 Support
FFP
Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 1: PC Maintenance, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0007		12	Months	(b)(4)	(b)(4)

CSS:SS Task Area 4, Subtask 2 Support
FFP
Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 2: Software Management, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0008		1	Lot	(b)(4)	(b)(4) NTE

CSS:SS Task Area 5 Support
LH
Corporate Services Support: Service Support - Labor for Task Area 5, Special C4 Support Function, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012

Task 5, Subtask 1: Senior Management Support - (b)(4)
Task 5, Subtask 1, para 1.3.5.1.2: SDDC Senior Management Support - (b)(4)
Task 5, Subtask 2, Portable Electronic Device (PED) Support Services - (b)(4)
Task 5, Subtask 3: Telephone Support Services - (b)(4)
FOB: Destination
SIGNAL CODE: A

TOT ESTIMATED PRICE (b)(4) NTE
CEILING PRICE $0.00

ITEM(S) 0008 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0009		1	Lot	(b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 5, Subtask 4 Support				
	LH				
	(OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 5, Subtask 4: Telephone Implementation and Integration Support, in accordance with the attached PWS.				
	Period of Performance: 1 October 2011 through 30 September 2012				
	FOB: Destination				
	SIGNAL CODE: A				
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0010		12	Months	(b)(4)	(b)(4)
	CSS:SS Task Area 6 Support				
	FFP				
	Corporate Services Support: Service Support - Labor for Task Area 6, Training/Lab Function (includes Subtasks 1 through 3 only), in accordance with the attached PWS.				
	Period of Performance: 1 October 2011 through 30 September 2012				
	FOB: Destination				
	SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0011 OPTION	CSS:SS Task Area 6, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 6, Subtask 4: Training Videos and Computer Based Training, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	$ (b)(4) NTE
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0012	CSS:SS Task Area 7 Support LH Corporate Services Support: Service Support - Labor for Task Area 7, USTRANSCOM Information Assurance and Information Protection (IA/IP), in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 Task 7, Subtask 1: Engineering Support - $ (b)(4) Task 7, Subtask 2: Communications Security (COMSEC) Manager - $ (b)(4) Task 7, Subtask 3: Certification & Accreditation (C&A) Support - $ (b)(4) Task 7, Subtask 4: IA/IP for USTRANSCOM Component Commands - $ (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 0012 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0013		1	Lot	$ (b)(4)	$ (b)(4) NTE

CSS:SS Task Area 8 Support

LH

Corporate Services Support: Service Support - Labor for Task Area 8, Project and Program Management, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012

Task 8, Subtask 1: Technical Project Management - (b)(4)

Task 8, Subtask 2: Enterprise Infrastructure Management Support - $ (b)(4)

FOB: Destination

SIGNAL CODE: A

TOT ESTIMATED PRICE	$ (b)(4) NTE
CEILING PRICE	$0.00

ITEM(S) 0013 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0014		12	Months	(b)(4)	$ (b)(4)

CSS:SS Task Area 9 Support
FFP
Corporate Services Support: Service Support - Labor for Task Area 9, Audiovisual and Video Teleconferencing Support (includes Subtasks 1 through 6 only), in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0015		12	Months	(b)(4)	(b)(4)

CSS:SS Task Area 9, Subtask 7 Support
FFP
Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 7: Briefing and Display Systems Support for the Fusion Center, in accordance with the attached PWS.

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
0016	CSS:SS Task Area 9, Subtask 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE

TOT ESTIMATED PRICE (b)(4) NTE

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0017 OPTION	CSS:SS Cyber Security Requirements FFP (OPTIONAL) Corporate Services Support: Service Support - Cyber Security Requirements, in accordance with PWS paragraphs 5.4 through 5.8 and paragraphs 5.10 through 5.16 Period of Performance: 1 October 2011 through 30 September 2012 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	(b)(4)

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0018			Lot		$55,000.00

Travel
COST
Travel, in accordance with PWS paragraph 4.3

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

ESTIMATED COST $55,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0019			Lot		$22,500.00

Other Direct Costs (ODCs)
COST
Other Direct Costs (ODCs) in accordance with PWS paragraph 4.4

Period of Performance: 1 October 2011 through 30 September 2012
FOB: Destination
SIGNAL CODE: A

ESTIMATED COST $22,500.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 1, Contract Level and Task Order Management, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1002		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 1: SDDC Helpdesk and Desktop Customer Support, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1003		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 2: USTRANSCOM Service Desk Support, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT	
1004		1	Lot	(b)(4)	(b)(4)	NTE
OPTION	CSS:SS Task Area 2, Subtask 3 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task 2, Subtask 3: USTRANSCOM Service Desk Extended Support, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A					
				TOT ESTIMATED PRICE	(b)(4)	NTE
				CEILING PRICE		$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1005		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 3 Support FFP Corporate Services Support: Service Support - Labor for Task Area 3, Computer System Maintenance and Logistics Support, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1006		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 4, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 1: PC Maintenance, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1007		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 4, Subtask 2 Support				
	FFP				
	Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 2: Software Management, in accordance with the attached PWS.				
	Period of Performance: 1 October 2012 through 30 September 2013				
	FOB: Destination				
	SIGNAL CODE: A				

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
1008		1	Lot	(b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 5 Support				
	LH				
	Corporate Services Support: Service Support - Labor for Task Area 5, Special C4 Support Function, in accordance with the attached PWS.				
	Period of Performance: 1 October 2012 through 30 September 2013				
	Task 5, Subtask 1: Senior Management Support - $ (b)(4)				
	Task 5, Subtask 1, para 1.3.5.1.2: SDDC Senior Management Support - (b)(4)				
	Task 5, Subtask 2, Portable Electronic Device (PED) Support Services - $ (b)(4)				
	Task 5, Subtask 3: Telephone Support Services - (b)(4)				
	FOB: Destination				
	SIGNAL CODE: A				

TOT ESTIMATED PRICE (b)(4) NTE

CEILING PRICE $0.00

ITEM(S) 1008 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT (b)(4) NTE
1009 OPTION	CSS:SS Task Area 5, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 5, Subtask 4: Telephone Implementation and Integration Support, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	

TOT ESTIMATED PRICE (b)(4) NTE

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT (b)(4)
1010 OPTION	CSS:SS Task Area 6 Support FFP Corporate Services Support: Service Support - Labor for Task Area 6, Training/Lab Function (includes Subtasks 1 through 3 only), in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
1011 OPTION	CSS:SS Task Area 6, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 6, Subtask 4: Training Videos and Computer Based Training, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
1012 OPTION	CSS:SS Task Area 7 Support LH Corporate Services Support: Service Support - Labor for Task Area 7, USTRANSCOM Information Assurance and Information Protection (IA/IP), in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 Task 7, Subtask 1: Engineering Support - (b)(4) Task 7, Subtask 2: Communications Security (COMSEC) Manager - $ (b)(4) Task 7, Subtask 3: Certification & Accreditation (C&A) Support - $ (b)(4) Task 7, Subtask 4: IA/IP for USTRANSCOM Component Commands - $ (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 1012 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
1013 OPTION	CSS:SS Task Area 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 8, Project and Program Management, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 Task 8, Subtask 1: Technical Project Management - (b)(4) Task 8, Subtask 2: Enterprise Infrastructure Management Support - $ (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 1013 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1014		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 9 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Audiovisual and Video Teleconferencing Support (includes Subtasks 1 through 6 only), in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1015		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 9, Subtask 7 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 7: Briefing and Display Systems Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2012 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
1016		1	Lot	(b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 9, Subtask 8 Support				
	LH				
	Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center, in accordance with the attached PWS.				
	Period of Performance: 1 October 2012 through 30 September 2013				
	FOB: Destination				
	SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1017		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Cyber Security Requirements				
	FFP				
	(OPTIONAL) Corporate Services Support: Service Support - Cyber Security Requirements, in accordance with PWS paragraphs 5.4 through 5.8 and paragraphs 5.10 through 5.16				
	Period of Performance: 1 October 2012 through 30 September 2013				
	FOB: Destination				
	SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1018			Lot		$55,000.00
OPTION	Travel				
	COST				
	Travel, in accordance with PWS paragraph 4.3				
	Period of Performance: 1 October 2012 through 30 September 2013				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$55,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1019			Lot		$22,500.00
OPTION	Other Direct Costs (ODCs)				
	COST				
	Other Direct Costs (ODCs) in accordance with PWS paragraph 4.4				
	Period of Performance: 1 October 2012 through 30 September 2013				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$22,500.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 1, Contract Level and Task Order Management, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2002		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 2, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 1: SDDC Helpdesk and Desktop Customer Support, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2003		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 2, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 2: USTRANSCOM Service Desk Support, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2004		1	Lot	$ (b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 2, Subtask 3 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task 2, Subtask 3: USTRANSCOM Service Desk Extended Support, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2005		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 3 Support FFP Corporate Services Support: Service Support - Labor for Task Area 3, Computer System Maintenance and Logistics Support, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2006		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 4, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 1: PC Maintenance, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2013 FOB: Destination SIGNAL CODE: A				

NET AMT $ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2007		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 4, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 2: Software Management, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2008		1	Lot	(b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 5 Support LH Corporate Services Support: Service Support - Labor for Task Area 5, Special C4 Support Function, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 Task 5, Subtask 1: Senior Management Support - (b)(4) Task 5, Subtask 1, para 1.3.5.1.2: SDDC Senior Management Support - $ (b)(4) Task 5, Subtask 2, Portable Electronic Device (PED) Support Services - $ (b)(4) Task 5, Subtask 3: Telephone Support Services - $ (b)(4) FOB: Destination SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 2008 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2009 OPTION	CSS:SS Task Area 5, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 5, Subtask 4: Telephone Implementation and Integration Support, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	(b)(4) NTE

TOT ESTIMATED PRICE $ (b)(4) NTE

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2010 OPTION	CSS:SS Task Area 6 Support FFP Corporate Services Support: Service Support - Labor for Task Area 6, Training/Lab Function (includes Subtasks 1 through 3 only), in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A	12	Months	$ (b)(4)	$ (b)(4)

NET AMT $ (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2011 OPTION	CSS:SS Task Area 6, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 6, Subtask 4: Training Videos and Computer Based Training, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	$ (b)(4) NTE
			TOT ESTIMATED PRICE		$ (b)(4) NTE
			CEILING PRICE		$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2012 OPTION	CSS:SS Task Area 7 Support LH Corporate Services Support: Service Support - Labor for Task Area 7, USTRANSCOM Information Assurance and Information Protection (IA/IP), in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 Task 7, Subtask 1: Engineering Support - $ (b)(4) Task 7, Subtask 2: Communications Security (COMSEC) Manager - (b)(4) Task 7, Subtask 3: Certification & Accreditation (C&A) Support - (b)(4) Task 7, Subtask 4: IA/IP for USTRANSCOM Component Commands - (b)(4) FOB: Destination SIGNAL CODE: A	I	Lot	(b)(4)	$ (b)(4) NTE
			TOT ESTIMATED PRICE		(b)(4) NTE
			CEILING PRICE		$0.00

ITEM(S) 2012 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2013 OPTION		1	Lot	(b)(4)	(b)(4) NTE
	CSS:SS Task Area 8 Support				
	LH				
	Corporate Services Support: Service Support - Labor for Task Area 8, Project and Program Management, in accordance with the attached PWS.				
	Period of Performance: 1 October 2013 through 30 September 2014				
	Task 8, Subtask 1: Technical Project Management (b)(4)				
	Task 8, Subtask 2: Enterprise Infrastructure Management Support - $ (b)(4)				
	FOB: Destination				
	SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 2013 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2014		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 9 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Audiovisual and Video Teleconferencing Support (includes Subtasks 1 through 6 only), in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2015		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 9, Subtask 7 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 7: Briefing and Display Systems Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2013 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
2016 OPTION	CSS:SS Task Area 9, Subtask 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2017 OPTION	CSS:SS Cyber Security Requirements FFP (OPTIONAL) Corporate Services Support: Service Support - Cyber Security Requirements, in accordance with PWS paragraphs 5.4 through 5.8 and paragraphs 5.10 through 5.16 Period of Performance: 1 October 2013 through 30 September 2014 FOB: Destination SIGNAL CODE: A	12	Months	(b)(4)	$ (b)(4)
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2018			Lot		$55,000.00
OPTION	Travel				
	COST				
	Travel, in accordance with PWS paragraph 4.3				
	Period of Performance: 1 October 2013 through 30 September 2014				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$55,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2019			Lot		$22,500.00
OPTION	Other Direct Costs (ODCs)				
	COST				
	Other Direct Costs (ODCs) in accordance with PWS paragraph 4.4				
	Period of Performance: 1 October 2013 through 30 September 2014				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$22,500.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 1, Contract Level and Task Order Management, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3002		12	Months	$ (b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 1: SDDC Helpdesk and Desktop Customer Support, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3003		12	Months	$ (b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 2: USTRANSCOM Service Desk Support, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3004		1	Lot	$ (b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 2, Subtask 3 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task 2, Subtask 3: USTRANSCOM Service Desk Extended Support, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3005		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 3 Support FFP Corporate Services Support: Service Support - Labor for Task Area 3, Computer System Maintenance and Logistics Support, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3006		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 4, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 1: PC Maintenance, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3007		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 4, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 2: Software Management, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				

NET AMT

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3008		1	Lot	$ (b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 5 Support LH Corporate Services Support: Service Support - Labor for Task Area 5, Special C4 Support Function, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 Task 5, Subtask 1: Senior Management Support - $ (b)(4) Task 5, Subtask 1, para 1.3.5.1.2: SDDC Senior Management Support - $ (b)(4) Task 5, Subtask 2, Portable Electronic Device (PED) Support Services - $ (b)(4) Task 5, Subtask 3: Telephone Support Services - $ (b)(4) FOB: Destination SIGNAL CODE: A				

TOT ESTIMATED PRICE (b)(4) NTE

CEILING PRICE $0.00

ITEM(S) 3008 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3009		1	Lot	(b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 5, Subtask 4 Support				
	LH				
	(OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 5, Subtask 4: Telephone Implementation and Integration Support, in accordance with the attached PWS.				
	Period of Performance: 1 October 2014 through 30 September 2015				
	FOB: Destination				
	SIGNAL CODE: A				
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3010		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 6 Support				
	FFP				
	Corporate Services Support: Service Support - Labor for Task Area 6, Training/Lab Function (includes Subtasks 1 through 3 only), in accordance with the attached PWS.				
	Period of Performance: 1 October 2014 through 30 September 2015				
	FOB: Destination				
	SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3011 OPTION	CSS:SS Task Area 6, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 6, Subtask 4: Training Videos and Computer Based Training, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3012 OPTION	CSS:SS Task Area 7 Support LH Corporate Services Support: Service Support - Labor for Task Area 7, USTRANSCOM Information Assurance and Information Protection (IA/IP), in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 Task 7, Subtask 1: Engineering Support - $ (b)(4) Task 7, Subtask 2: Communications Security (COMSEC) Manager - $ (b)(4) Task 7, Subtask 3: Certification & Accreditation (C&A) Support - $ (b)(4) Task 7, Subtask 4: IA/IP for USTRANSCOM Component Commands - $ (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 3012 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3013 OPTION	CSS:SS Task Area 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 8, Project and Program Management, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 Task 8, Subtask 1: Technical Project Management - (b)(4) Task 8, Subtask 2: Enterprise Infrastructure Management Support - (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	(b)(4)	(b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 3013 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3014		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 9 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Audiovisual and Video Teleconferencing Support (includes Subtasks 1 through 6 only), in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3015		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 9, Subtask 7 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 7: Briefing and Display Systems Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2014 through 30 September 2015 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
3016		1	Lot	(b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 9, Subtask 8 Support				

LH

Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center, in accordance with the attached PWS.

Period of Performance: 1 October 2014 through 30 September 2015

FOB: Destination

SIGNAL CODE: A

TOT ESTIMATED PRICE (b)(4) NTE

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3017		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Cyber Security Requirements				

FFP

(OPTIONAL) Corporate Services Support: Service Support - Cyber Security Requirements, in accordance with PWS paragraphs 5.4 through 5.8 and paragraphs 5.10 through 5.16

Period of Performance: 1 October 2014 through 30 September 2015

FOB: Destination

SIGNAL CODE: A

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3018			Lot		$55,000.00
OPTION	Travel				
	COST				
	Travel, in accordance with PWS paragraph 4.3				
	Period of Performance: 1 October 2014 through 30 September 2015				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$55,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3019			Lot		$22,500.00
OPTION	Other Direct Costs (ODCs)				
	COST				
	Other Direct Costs (ODCs) in accordance with PWS paragraph 4.4				
	Period of Performance: 1 October 2014 through 30 September 2015				
	FOB: Destination				
	SIGNAL CODE: A				
				ESTIMATED COST	$22,500.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 1, Contract Level and Task Order Management, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4002		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 1: SDDC Helpdesk and Desktop Customer Support, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4003		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 2, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task 2, Subtask 2: USTRANSCOM Service Desk Support, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT	
4004		1	Lot	(b)(4)	(b)(4)	NTE
OPTION	CSS:SS Task Area 2, Subtask 3 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task 2, Subtask 3: USTRANSCOM Service Desk Extended Support, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A					
				TOT ESTIMATED PRICE	(b)(4)	NTE
				CEILING PRICE		$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4005		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 3 Support FFP Corporate Services Support: Service Support - Labor for Task Area 3, Computer System Maintenance and Logistics Support, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4006		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 4, Subtask 1 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 1: PC Maintenance, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4007		12	Months	(b)(4)	(b)(4)
OPTION	CSS:SS Task Area 4, Subtask 2 Support FFP Corporate Services Support: Service Support - Labor for Task Area 4, Subtask 2: Software Management, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4008		1	Lot	(b)(4)	(b)(4) NTE
OPTION	CSS:SS Task Area 5 Support LH Corporate Services Support: Service Support - Labor for Task Area 5, Special C4 Support Function, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 Task 5, Subtask 1: Senior Management Support - $ (b)(4) Task 5, Subtask 1, para 1.3.5.1.2: SDDC Senior Management Support - (b)(4) Task 5, Subtask 2, Portable Electronic Device (PED) Support Services - $ (b)(4) Task 5, Subtask 3: Telephone Support Services - $ (b)(4) FOB: Destination SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM(S) 4008 - DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4009		1	Lot	$ (b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 5, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 5, Subtask 4: Telephone Implementation and Integration Support, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
			TOT ESTIMATED PRICE		(b)(4) NTE
			CEILING PRICE		$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4010		12	Months	(b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 6 Support FFP Corporate Services Support: Service Support - Labor for Task Area 6, Training/Lab Function (includes Subtasks 1 through 3 only), in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
			NET AMT		$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4011 OPTION	CSS:SS Task Area 6, Subtask 4 Support LH (OPTIONAL) Corporate Services Support: Service Support - Labor for Task Area 6, Subtask 4: Training Videos and Computer Based Training, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	$ (b)(4) NTE
				TOT ESTIMATED PRICE	(b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4012 OPTION	CSS:SS Task Area 7 Support LH Corporate Services Support: Service Support - Labor for Task Area 7, USTRANSCOM Information Assurance and Information Protection (IA/IP), in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 Task 7, Subtask 1: Engineering Support - (b)(4) Task 7, Subtask 2: Communications Security (COMSEC) Manager - $ (b)(4) Task 7, Subtask 3: Certification & Accreditation (C&A) Support - $ (b)(4) Task 7, Subtask 4: IA/IP for USTRANSCOM Component Commands - $ (b)(4) FOB: Destination SIGNAL CODE: A	1	Lot	$ (b)(4)	$ (b)(4) NTE
				TOT ESTIMATED PRICE	$ (b)(4) NTE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4013		1	Lot	$ (b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 8, Project and Program Management, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 Task 8, Subtask 1: Technical Project Management - (b)(4) Task 8, Subtask 2: Enterprise Infrastructure Management Support - (b)(4) FOB: Destination SIGNAL CODE: A				
				TOT ESTIMATED PRICE	$ (b)(4) TE
				CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4014		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 9 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Audiovisual and Video Teleconferencing Support (includes Subtasks 1 through 6 only), in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4015		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Task Area 9, Subtask 7 Support FFP Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 7: Briefing and Display Systems Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: I October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				

NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	ESTIMATED QUANTITY	UNIT	UNIT PRICE	AMOUNT
4016		1	Lot	$ (b)(4)	$ (b)(4) NTE
OPTION	CSS:SS Task Area 9, Subtask 8 Support LH Corporate Services Support: Service Support - Labor for Task Area 9, Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center, in accordance with the attached PWS. Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				

TOT ESTIMATED PRICE $ (b)(4) NTE

CEILING PRICE $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4017		12	Months	$ (b)(4)	$ (b)(4)
OPTION	CSS:SS Cyber Security Requirements FFP (OPTIONAL) Corporate Services Support: Service Support - Cyber Security Requirements, in accordance with PWS paragraphs 5.4 through 5.8 and paragraphs 5.10 through 5.16 Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				NET AMT	$ (b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4018			Lot		$55,000.00
OPTION	Travel COST Travel, in accordance with PWS paragraph 4.3 Period of Performance: 1 October 2015 through 30 September 2016 FOB: Destination SIGNAL CODE: A				
				ESTIMATED COST	$55,000.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4019			Lot		$22,500.00
OPTION	Other Direct Costs (ODCs)				

COST

Other Direct Costs (ODCs) in accordance with PWS paragraph 4.4

Period of Performance: 1 October 2015 through 30 September 2016

FOB: Destination

SIGNAL CODE: A

ESTIMATED COST $22,500.00

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
0003	Destination	Government	Destination	Government
0004	Destination	Government	Destination	Government
0005	Destination	Government	Destination	Government
0006	Destination	Government	Destination	Government
0007	Destination	Government	Destination	Government
0008	Destination	Government	Destination	Government
0009	Destination	Government	Destination	Government
0010	Destination	Government	Destination	Government
0011	Destination	Government	Destination	Government
0012	Destination	Government	Destination	Government
0013	Destination	Government	Destination	Government
0014	Destination	Government	Destination	Government
0015	Destination	Government	Destination	Government
0016	Destination	Government	Destination	Government
0017	Destination	Government	Destination	Government
0018	Destination	Government	Destination	Government
0019	Destination	Government	Destination	Government
1001	Destination	Government	Destination	Government
1002	Destination	Government	Destination	Government
1003	Destination	Government	Destination	Government
1004	Destination	Government	Destination	Government
1005	Destination	Government	Destination	Government
1006	Destination	Government	Destination	Government
1007	Destination	Government	Destination	Government

1008	Destination	Government	Destination	Government
1009	Destination	Government	Destination	Government
1010	Destination	Government	Destination	Government
1011	Destination	Government	Destination	Government
1012	Destination	Government	Destination	Government
1013	Destination	Government	Destination	Government
1014	Destination	Government	Destination	Government
1015	Destination	Government	Destination	Government
1016	Destination	Government	Destination	Government
1017	Destination	Government	Destination	Government
1018	Destination	Government	Destination	Government
1019	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government
2002	Destination	Government	Destination	Government
2003	Destination	Government	Destination	Government
2004	Destination	Government	Destination	Government
2005	Destination	Government	Destination	Government
2006	Destination	Government	Destination	Government
2007	Destination	Government	Destination	Government
2008	Destination	Government	Destination	Government
2009	Destination	Government	Destination	Government
2010	Destination	Government	Destination	Government
2011	Destination	Government	Destination	Government
2012	Destination	Government	Destination	Government
2013	Destination	Government	Destination	Government
2014	Destination	Government	Destination	Government
2015	Destination	Government	Destination	Government
2016	Destination	Government	Destination	Government
2017	Destination	Government	Destination	Government
2018	Destination	Government	Destination	Government
2019	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
3002	Destination	Government	Destination	Government
3003	Destination	Government	Destination	Government
3004	Destination	Government	Destination	Government
3005	Destination	Government	Destination	Government
3006	Destination	Government	Destination	Government
3007	Destination	Government	Destination	Government
3008	Destination	Government	Destination	Government
3009	Destination	Government	Destination	Government
3010	Destination	Government	Destination	Government
3011	Destination	Government	Destination	Government
3012	Destination	Government	Destination	Government
3013	Destination	Government	Destination	Government
3014	Destination	Government	Destination	Government
3015	Destination	Government	Destination	Government
3016	Destination	Government	Destination	Government
3017	Destination	Government	Destination	Government
3018	Destination	Government	Destination	Government
3019	Destination	Government	Destination	Government
4001	Destination	Government	Destination	Government
4002	Destination	Government	Destination	Government
4003	Destination	Government	Destination	Government
4004	Destination	Government	Destination	Government

4005	Destination	Government	Destination	Government
4006	Destination	Government	Destination	Government
4007	Destination	Government	Destination	Government
4008	Destination	Government	Destination	Government
4009	Destination	Government	Destination	Government
4010	Destination	Government	Destination	Government
4011	Destination	Government	Destination	Government
4012	Destination	Government	Destination	Government
4013	Destination	Government	Destination	Government
4014	Destination	Government	Destination	Government
4015	Destination	Government	Destination	Government
4016	Destination	Government	Destination	Government
4017	Destination	Government	Destination	Government
4018	Destination	Government	Destination	Government
4019	Destination	Government	Destination	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	UIC
0001	POP 01-OCT-2011 TO 30-SEP-2012	N/A	USTC/J6 - F3ST95 TERRANCE THREAT 508 SCOTT DR SCOTT AFB IL 62225-5357 618-229-4138 FOB: Destination	F3ST95
0002	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0003	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0004	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0005	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0006	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0007	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0008	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

0009	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0010	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0011	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0012	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0013	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0014	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0015	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0016	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0017	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0018	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
0019	POP 01-OCT-2011 TO 30-SEP-2012	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1001	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1002	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1003	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1004	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1005	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1006	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1007	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

1008	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1009	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1010	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1011	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1012	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1013	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1014	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1015	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1016	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1017	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1018	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
1019	POP 01-OCT-2012 TO 30-SEP-2013	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2001	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2002	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2003	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2004	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2005	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2006	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

2007	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2008	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2009	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2010	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2011	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2012	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2013	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2014	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2015	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2016	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2017	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2018	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
2019	POP 01-OCT-2013 TO 30-SEP-2014	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3001	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3002	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3003	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3004	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3005	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

3006	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3007	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3008	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3009	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3010	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3011	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3012	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3013	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3014	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3015	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3016	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3017	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3018	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
3019	POP 01-OCT-2014 TO 30-SEP-2015	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4001	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4002	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4003	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4004	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

4005	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4006	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4007	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4008	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4009	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4010	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4011	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4012	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4013	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4014	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4015	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4016	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4017	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4018	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95
4019	POP 01-OCT-2015 TO 30-SEP-2016	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	F3ST95

CLAUSES INCORPORATED BY REFERENCE

52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JAN 2011
52.212-4	Contract Terms and Conditions--Commercial Items	JUN 2010
52.212-4 Alt I	Contract Terms and Conditions--Commercial Items (Jun 2010)	OCT 2008
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.223-18	Encouraging Contractor Policies To Ban Text Messaging While Driving	AUG 2011
52.232-18	Availability Of Funds	APR 1984
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	JAN 2009
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	SEP 1999
252.232-7003	Electronic Submission of Payment Requests and Receiving Reports	MAR 2008
252.232-7010	Levies on Contract Payments	DEC 2006
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008

CLAUSES INCORPORATED BY FULL TEXT

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (AUG 2011) (DEVIATION)

(a) Comptroller General Examination of Record. The Contractor shall comply with the provisions of this paragraph (a) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, 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.

(b)(1) Notwithstanding the requirements of any other clause in this contract, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (b)(i) in a subcontract for commercial items. 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 (APR 2010) (Pub. L. 110-252, Title VI, Chapter 1 (41 U.S.C. 251 note).

(ii) 52.219-8, Utilization of Small Business Concerns (DEC 2010) (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 $650,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(iii) Reserved.

(iv) 52.222-26, Equal Opportunity (MAR 2007) (E.O. 11246).

(v) 52.222-35, Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (SEP 2006) (38 U.S.C. 4212).

(vi) 52.222-36, Affirmative Action for Workers with Disabilities (JUN 1998) (29 U.S.C. 793).

(vii) 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.

(viii) 52.222-41, Service Contract Act of 1965 (Nov 2007) (41 U.S.C. 351, et seq.).

(ix) 52.222-50, Combating Trafficking in Persons (FEB 2009) (22 U.S.C. 7104(g)).

___ Alternate I (AUG 2007) of 52.222-50 (22 U.S.C. 7104(g)).

(x) 52.222-51, Exemption from Application of the Service Contract Act to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (Nov 2007) (41 U.S.C. 351, et seq.).

(xi) 52.222-53, Exemption from Application of the Service Contract Act to Contracts for Certain Services--Requirements (FEB 2009) (41 U.S.C. 351, et seq.).

(xii) 52.222-54, Employment Eligibility Verification (JAN 2009).

(xiii) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (MAR 2009) (Pub. L. 110-247). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xiv) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (FEB 2006) (46 U.S.C. Appx 1241(b) 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 items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

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 no later than 30 calendar days before the contract expires.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

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 no later than 30 calendar days before the contract expires ; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 calendar 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 60 months, excluding the terms on FAR Clause 52.217-8, Option to Extend Services.

(End of clause)

CLAUSES INCORPORATED BY FULL TEXT

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 addresses:
http://farsite.hill.af.mil/vffara.htm
http://farsite.hill.af.mil/vfdfara.htm
http://farsite.hill.af.mil/vfustca.htm

(End of clause)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

252.212-7001 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS APPLICABLE TO DEFENSE ACQUISITIONS OF COMMERCIAL ITEMS (DEC 2010) (DEVIATION)

(a) In addition to the clauses listed in paragraph (b) of the Contract Terms and Conditions Required to Implement Statutes or Executive Orders--Commercial Items clause of this contract (FAR 52.212-5) (OCT 2010) (DEVIATION), the Contractor shall include the terms of the following clause, if applicable, in subcontracts for commercial items or commercial components, awarded at any tier under this contract:

252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel (NOV 2010) (Section 1038 of Pub. L. 111-84).
252.237-7019	Training for Contractor Personnel Interacting with Detainees (SEP 2006) (Section 1092 of Pub. L. 108-375).
252.247-7003	Pass-Through of Motor Carrier Fuel Surcharge Adjustment to the Cost Bearer (JUL 2009) (Section 884 of Public Law 110-417)
252.247-7023	Transportation of Supplies by Sea (MAY 2002) (10 U.S.C. 2631)
252.247-7024	Notification of Transportation of Supplies by Sea (MAR 2000) (10 U.S.C. 2631)

(End of clause)

252.243-7001 PRICING OF CONTRACT MODIFICATIONS (DEC 1991)

When costs are a factor in any price adjustment under this contract, the contract cost principles and procedures in FAR part 31 and DFARS part 231, in effect on the date of this contract, apply.

252.243-7002 REQUESTS FOR EQUITABLE ADJUSTMENT (MAR 1998)

(a) The amount of any request for equitable adjustment 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. All indirect costs included in the request shall be properly allocable to the change in accordance with applicable acquisition regulations.

(b) In accordance with 10 U.S.C. 2410(a), any request for equitable adjustment to contract terms that exceeds the simplified acquisition threshold shall bear, at the time of submission, the following certificate executed by an individual authorized to certify the request on behalf of the Contractor:

I certify that the request is made in good faith, and that the supporting data are accurate and complete to the best of my knowledge and belief.

(Official's Name)

(Title)

(c) The certification in paragraph (b) of this clause requires full disclosure of all relevant facts, including--

(1) Cost or pricing data if required in accordance with subsection 15.403-4 of the Federal Acquisition Regulation (FAR); and

(2) Information other than cost or pricing data, in accordance with subsection 15.403-3 of the FAR, including actual cost data and data to support any estimated costs, even if cost or pricing data are not required.

(d) The certification requirement in paragraph (b) of this clause does not apply to----

(1) Requests for routine contract payments; for example, requests for payment for accepted supplies and services, routine vouchers under a cost-reimbursement type contract, or progress payment invoices; or

(2) Final adjustment under an incentive provision of the contract.

5552.204-9000 Notification of Government security activity and visitor group security agreements.

NOTIFICATION OF GOVERNMENT SECURITY ACTIVITY AND VISITOR GROUP SECURITY AGREEMENTS (APRIL 2007)

This contract contains a DD Form 254, DOD Contract Security Classification Specification, and requires performance at a government location in the U.S. or overseas. Prior to beginning operations involving classified information on an installation identified on the DD Form 254, the contractor shall take the following actions:
(a) At least thirty days prior to beginning operations, notify the security police activity shown in the distribution block of the DD Form 254 as to:
(1) The name, address, and telephone number of this contract company's representative and designated alternate in the U.S. or overseas area, as appropriate;
(2) The contract number and military contracting command;
(3) The highest classification category of defense information to which contractor employees will have access which must coincide with the level of classification granted to the company and cage code located in the Joint Personnel Adjudication System (JPAS);
(4) The installations in the U.S. (in overseas areas, identify only the APO number(s)) where the contract work will be performed;
(5) The date contractor operations will begin on base in the U.S. or in the overseas area;
(6) The estimated completion date of operations on base in the U.S. or in the overseas area; and,
(7) Any changes to information previously provided under this clause.
This requirement is in addition to visit request procedures contained in DOD 5220.22-M, National Industrial Security Program Operating Manual.
(b) Prior to beginning operations involving classified information on an installation identified on the DD Form 254 where the contractor is not required to have a facility security clearance, the contractor shall enter into a Visitor Group Security Agreement (or understanding) with the installation commander to ensure that the contractor's security procedures are properly integrated with those of the installation. As a minimum, the agreement shall identify the security actions that will be performed:
(1) By the installation for the contractor, such as providing storage and classified reproduction facilities, guard services, security forms, security inspections under DOD 5220.22-M, classified mail services, security badges,

visitor control, and investigating security incidents; and
(2) Jointly by the contractor and the installation, such as packaging and addressing classified transmittals, security checks, internal security controls, and implementing emergency procedures to protect classified material.
(End of clause)

5552.216-9003 USTRANSCOM TASK AND DELIVERY ORDER OMBUDSMAN (JUNE 2009)

In accordance with FAR 16.505(b)(6), the individual identified below is designated as the USTRANSCOM Task and Delivery-Order Ombudsman. The ombudsman is an independent official designated to review contractor complaints and to ensure contractors are afforded a fair opportunity to be considered, consistent with the procedures in the contract. Consulting the ombudsman does not relieve the contractor from performance requirements in the contract, nor alter or postpone any timelines for any other processes. Interested parties should first address their concerns, issues, disagreements, and/or recommendations to the contracting officer for resolution. If resolution cannot be made by the contracting officer, concerned parties may contact:

Chief, Business Support/Policy Division
Telephone Number: 618-220-7021 FAX: 618-220-7959

5552.223-9001 Health and Safety on Government Installations.

HEALTH AND SAFETY ON GOVERNMENT INSTALLATIONS (APRIL 2007)
(a) In performing work under this contract on a Government installation, the contractor shall:
(1) Comply with the specific health and safety requirements established by this contract;
(2) Comply with the health and safety rules of the Government installation that concern related activities not directly addressed in this contract;
(3) Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of contractor and Government personnel performing or in any way coming in contact with the performance of this contract; and
(4) Take such additional immediate precautions as the contracting officer may reasonably require for health and safety purposes.
(b) The contracting officer may, by written order, direct Air Force Occupational safety and Health (AFOSH) Standards and/or health/safety standards as may be required in the performance of this contract and any adjustments resulting from such direction will be in accordance with the Changes clause of this contract.
(c) Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the contracting officer, shall be grounds for termination of this contract in accordance with the Default clause of this contract.
(End of Clause)

5552.242-9000 COMMON ACCESS CARDS (CACs) FOR CONTRACTOR PERSONNEL (AUG 2008)

(a) When contractor performance is required on government installation(s)/location(s), contractors shall ensure Common Access Cards (CACs) are obtained by all contract or subcontract employees who meet one or both of the following criteria:
(1) Require long-term logical access to Department of Defense computer networks and systems in either:
(i) the unclassified environment; or
(ii) the classified environment where authorized by governing security directives.

(2) Perform work on a long-term basis, which requires the use of a CAC for installation entry control or physical access to facilities and buildings.
(b) Contractors and their employees shall use the following procedures to obtain CACs:
(1) Contractors shall provide a listing of their employees that will require a CAC to the contracting officer. The listing will contain the following information in order for a CAC application to be created in the Contractor Verification System (CVS): last, middle, and first names; Social Security Number; Date of Birth; email address; the contract number; and the contract end date. The contracting officer will provide a copy of the list to the government representative in the local organization designated to authorize issuance of contractor CACs (i.e., Trusted Agent (TA)). The TA will then create a CAC application in the Contractor Verification System (CVS.)
(2) Once the TA has created the CAC application, a temporary login/password will be generated in CVS. The TA will notify each contractor employee when his/her application is created and will securely distribute the login/password to that contractor employee. Each contractor employee will then enter the CVS web site using the temporary login/password and complete the CAC application and submit it back to the TA.
(3) If contractor employees will not require access to classified information, each contactor employee will be required to complete either the Questionnaire for Non-Sensitive Positions (SF85), located at www.opm.gov/forms/pdf_fill/SF85.pdf, or the Questionnaire for Public Trust Positions (SF85P) and submit fingerprint cards (FD-258) to the USTRANSCOM contracting officer who will verify each employee and then forward the documents to the Security Services Center for processing. The questionnaires and fingerprint cards will be forwarded by the Security Services Center personnel to OPM who will conduct a National Agency Check with written Inquiries (NACI) background investigation. Before the TA approves the CAC application in CVS, the TA must verify that a background investigation has either been opened or completed by OPM, or adjudicated by the Air Force Central Adjudication Facility (AFCAF), as shown in the Joint Personnel Adjudication System (JPAS).
(4) If contractor employees will require access to classified information, the contractor's company Facility Security Officer processes the Questionnaire for National Security Positions (SF86) and the fingerprint cards (FD-258) and submits them directly to the Defense Industrial Security Clearance Office (DISCO). Before the TA approves the CAC application in CVS, the TA must verify that a background investigation has been either opened or completed by OPM, or adjudicated by DISCO, as shown in JPAS.
(5) Once the TA has approved the CAC application, the TA will inform the contractor employee to proceed to the nearest CAC issuance workstation (usually located within the local Military Personnel Flight (MPF)) with two forms of picture identification. CAC issuance workstation personnel will then issue the CAC.
(c) While visiting or performing work on government installation(s)/location(s), contractor employees shall wear or prominently display the CAC as required by the governing local policy.
(d) During the performance period of the contract, the contractor, or contractor employee as appropriate, shall:
(1) Within 7 working days of any changes to the listing of the contract personnel authorized a CAC, provide an updated listing to the contracting officer who will provide the updated listing to the TA (who will create new CAC applications or revoke those for employees no longer performing on the contract as appropriate);
(2) As part of security out-processing, or when no longer performing on the specific contract for which the CAC was approved, return their CAC to either their TA, the USTRANSCOM Security Services Center personnel; or to a designated USTRANSCOM representative.
(3) Report lost or stolen CACs immediately to the TA, the USTRANSCOM Security Services Center, or to a designated USTRANSCOM representative.
(e) Within 7 working days following completion/termination of the contract, return all CACs issued to contractor employees to the TA, the USTRANSCOM Security Services Center, or to a designated USTRANSCOM representative.
(f) Failure to comply with these requirements may result in withholding of final payment.
(g) For OCONUS contracts, in addition to the above procedures, contractor employees requiring a Geneva Convention category on their CAC will be required to complete DD Form 1172-2, Application for Department of Defense Common Access Card DEERS Enrollment. This form shall be submitted to/approved by the contracting officer and then be presented to the CAC issuance workstation personnel in conjunction with the CVS application for CAC issuance.

(End of clause)

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Attachment 1	Atch 1 - PWS	66	14-JUN-2011
Attachment 2	Atch 2 - DD254	2	06-SEP-2011

ADMINISTRATIVE MATTERS

1. This is a Firm-Fixed Price Task Order, with Labor Hour and Cost Reimbursable Contract Line Items (CLINs).

2. Block 18b of the SF 1449 is hereby considered checked.

3. The contractor's technical proposal, dated 14 July 2011 including all revisions, is incorporated into this task order by reference. In the event of inconsistencies between the Performance Work Statement and the contractor's technical proposal, the provisions of the Performance Work Statement will take precedence.

4. Inspection and Acceptance: Personnel designated as the Contracting Officer's Representative (COR) responsible for the administration, inspection, and acceptance of worked performed under this task order will be provided via letter to the contractor upon award of this task order or as changes occur, if necessary.

5. If FAR 52.217-8, Option to Extend Services, is exercised, the monthly prices paid will be equal to the monthly price paid on the last month of the task order.

6. Invoice and Payment: The contractor shall submit invoices in accordance with DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports. The contractor shall utilize Wide Area Work Flow (WAWF) for the creation of electronic receiving reports (DD Form 250) and electronic invoices. The WAWF routing information is provided below.

7. The Performance Work Statement (PWS) is hereby incorporated as Attachment 1.

8. The DD 254 is hereby incorporated as Attachment 2.

WIDE AREA WORK FLOW-FFP CLINS

Invoices and Payments – Firm-Fixed Price CLINs

The contractor shall invoice using Wide Area Work Flow (WAWF). The contractor is required to submit a Combo Document for all Firm Fixed Price (FFP) CLINs.

ALL FIRM-FIXED PRICE REQUIREMENTS

WIDE AREA WORKFLOW
ELECTRONIC INVOICING INSTRUCTIONS

IN ACCORDANCE WITH DFARS 232.7002, USE OF ELECTRONIC PAYMENT REQUESTS IS MANDATORY. USE OF WAWF WILL SPEED UP YOUR PAYMENT PROCESSING TIME AND ALLOW YOU TO MONITOR YOUR PAYMENT STATUS ONLINE. THERE ARE NO CHARGES OR FEES TO USE WAWF.

Requests for payments must be submitted electronically via the Internet through the Wide Area WorkFlow system at https://wawf.eb.mil.

Questions concerning payment should be directed to the Defense Finance Accounting Services (DFAS) Limestone at (800) 756-4571 or faxed to (866) 392-7971 or e-mailed to cco-af-vpis@dfas.mil. Please have your contract and task order number and invoice number ready when contacting DFAS about payment status. You can also access payment information using the DFAS myInvoice web site at https://myinvoice.csd.disa.mil//index.html

THE FOLLOWING CODES WILL BE REQUIRED TO ROUTE YOUR COMBO (INVOICE AND RECEVING REPORTS) DOCUMENTS AND ADDITIONAL E-MAILS CORRECTLY THROUGH WAWF.

These routing instructions are to be used for the Firm Fixed Price CLINS as follows: **0001, 0002, 0003, 0005, 0006 0007, 0010, 0014, 0015, 0017, 1001, 1002, 1003, 1005, 1006, 1007, 1010, 1014, 1015, 1017, 2001, 2002, 2003, 2005, 2006 2007, 2010, 2014, 2015, 2017, 3001, 3002, 3003, 3005, 3006, 3007, 3010, 3014, 3015, 3017, 4001, 4002, 4003, 4005, 4006, 4007, 4010, 4014, 4015, and 4017.**

CONTRACT NUMBER:	**HTC711-11-F-D051**
DELIVERY ORDER NUMBER:	
TYPE OF DOCUMENT:	**Invoice and Receiving Report (Combo)**
CAGE CODE:	**1HXK0**
ISSUE BY DODAAC:	**HTC711**
ADMIN DODAAC:	**HTC711**
SERVICE ACCEPTOR DODAAC:	**F3ST95**
PAY OFFICE DODAAC:	**F87700**
SEND MORE E-MAIL NOTIFICATIONS:	
CONTRACT ADMINISTRATOR:	**Nicole.ostendorf@ustranscom.mil**
ADDITIONAL NOTIFICATION:	

WIDE AREA WORK FLOW-LH/CR CLIN
Invoices and Payment – Labor-Hour/Cost Reimbursable CLINs

The contractor shall invoice using Wide Area Work Flow (WAWF). The contractor is required to submit a cost voucher for all Labor-Hour and Travel CLINs.

FOR ALL LABOR-HOUR AND COST REIMBURSABLE REQUIRMENTS

WIDE AREA WORKFLOW
ELECTRONIC INVOICING INSTRUCTIONS

IN ACCORDANCE WITH DFARS 232.7002, USE OF ELECTRONIC PAYMENT REQUESTS IS MANDATORY. USE OF WAWF WILL SPEED UP YOUR PAYMENT PROCESSING TIME AND ALLOW YOU TO MONITOR YOUR PAYMENT STATUS ONLINE. THERE ARE NO CHARGES OR FEES TO USE WAWF.

Requests for payments must be submitted electronically via the Internet through the Wide Area WorkFlow system at https://wawf.eb.mil.

Questions concerning payment should be directed to the Defense Finance Accounting Services (DFAS) Limestone at (800) 756-4571 or faxed to (866) 392-7971 or e-mailed to cco-af-vpis@dfas.mil. Please have your contract and task order number and invoice number ready when contacting DFAS about payment status. You can also access payment information using the DFAS myInvoice web site at https://myinvoice.csd.disa.mil//index.html

THE FOLLOWING CODES WILL BE REQUIRED TO ROUTE YOUR COST VOUCHERS AND ADDITIONAL E-MAILS CORRECTLY THROUGH WAWF.

These routing instructions are to be used for the Labor Hour CLINs as follows: **0004, 0008, 0009, 0011, 0012, 0013, 0016, 1004, 1008, 1009, 1011, 1012, 1013, 1016, 2004, 2008, 2009, 2011, 2012, 2013, 2016, 3004, 3008, 3009, 3011, 3012, 3013, 3016, 4004, 4008, 4009, 4011, 4012, 4013, and 4016.**

These routing instructions are to be used for the Cost Reimbursable CLINs as follows:
Travel CLINs: 0018, 1018, 2018, 3018, and 4018.
ODC CLINs: 0019, 1019, 2019, 3019, and 4019.

CONTRACT NUMBER:	**HTC711-11-F-D051**
DELIVERY ORDER NUMBER:	
TYPE OF DOCUMENT:	**Cost Voucher**
CAGE CODE:	**1HXK0**
ISSUE BY DODAAC:	**HTC711**
ADMIN DODAAC:	**HTC711**
DCAA OFFICE:	**HAA47F**
SERVICE ACCEPTOR DODAAC:	**HTC711**
PAY OFFICE DODAAC:	**F87700**
SEND MORE E-MAIL NOTIFICATIONS:	
CONTRACT ADMINISTRATOR:	**Nicole.Ostendorf@ustranscom.mil**
ADDITIONAL NOTIFICATION:	

DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

DFAS PAYMENT INSTRUCTIONS

In accordance with DFARS Procedure Guidance Information (PGI) 204.7108(d)(12), Payment Instructions - Other, specific instructions will be provided when funding is made available on 1 October of each Fiscal Year.

PERFORMANCE WORK STATEMENT
FOR
UNITED STATES TRANSPORTATION COMMAND
COMMAND, CONTROL, COMMUNICATIONS & COMPUTER SYSTEMS DIRECTORATE (TCJ6)
CORPORATE SERVICES SUPPORT:
SERVICE SUPPORT

14 June 2011

PERFORMANCE WORK STATEMENT
FOR UNITED STATES TRANSPORTATION COMMAND COMMAND, CONTROL, COMMUNICATIONS & COMPUTER SYSTEMS DIRECTORATE (TCJ6) FOR CORPORATE SERVICES SUPPORT: SERVICE SUPPORT

Table of Contents

Appendices

PERFORMANCE WORK STATEMENT (PWS)

1. DESCRIPTION OF SERVICES

1.1. Background

The United States Transportation Command (USTRANSCOM) located at Scott Air Force Base (SAFB), IL, is one of ten Joint Unified Combatant Commands (JUCC) that provide Operational Control for the United States' combat forces. USTRANSCOM provides command and control (C2) for the synchronized transportation, distribution, and sustainment of personnel and assets, making possible the projection and maintenance of national power wherever needed with speed and agility, high efficiency and a high level of trust and accuracy.

USTRANSCOM's mission is to provide air, land and sea transportation for the Department of Defense (DOD) and other Government and non-Government organizations during both peace and war. The Commander, USTRANSCOM, is tasked as the single manager of the Defense Transportation System (DTS) to oversee defense common-user transportation assets. The Secretary of Defense further expanded the USTRANSCOM mission by tasking USTRANSCOM to manage key components of the Joint Deployment and Distribution Enterprise (JDDE). An important functional requirement is the integration of the Transportation Component Commands (TCCs) – Air Mobility Command (AMC), Surface Deployment and Distribution Command (SDDC), and Military Sealift Command (MSC). USTRANSCOM Command, Control, Communications, and Computer (C4) Systems (C4S) Directorate (TCJ6) provides essential C4S support to the USTRANSCOM Commander and the TCCs in performance of the command's mission to provide global air, land and sea transportation to meet national security objectives.

SDDC's mission is to provide global surface transportation to meet national security objectives in peace and war. SDDC executes its mission through three core processes: surface movements, personal property and passenger movement, and deploy-ability engineering. SDDC is a joint-service major Army command, and the surface transportation component of the USTRANSCOM. Its mission, "To provide global surface distribution management and services to meet National Security objectives in peace and war," positions this organization as the link between DOD shippers, commercial carriers and the warfighters in providing safe, responsive, efficient distribution and deployment solutions for our military. Information Technology provides the vehicle for the DOD to provide surface distribution and deployment worldwide and to have in-transit visibility throughout the process.

The SDDC Information Management mission is to manage the mission area support functions (communications, automation, storage area networks, audio-visual, publications and records management disciplines), manage the Automated Information Systems Security Program (AISSP), which includes: developing, coordinating, and integrating information requirements and architectures. Additionally, this mission is to provide training and technical assistance to end users, and manage the development, testing, and fielding of systems that automate transportation/distribution functionality.

The USTRANSCOM C4 environment interfaces with numerous on-site and remote commercial, DOD, service, and common-user networks (i.e., Secret Internet Protocol Router Network (SIPRNET), Non-secure Internet Protocol Router Network (NIPRNET), and the Scott AFB Local Area Network (LAN), Wide Area Network (WAN) or Metropolitan Area Network (MAN)). A myriad of applications make use of the USTRANSCOM C4 infrastructure by providing access and services to the USTRANSCOM user community.

USTRANSCOM operates the Distribution Process Owner (DPO) Secure Enclave (DSE) consisting of a Common Computing Environment (CCE) surrounded by a network defense infrastructure. The USTRANSCOM DSE, supported by TCJ6 and multiple United States Air Force (USAF) organizations, are comprised of several operating systems on clients and servers (See operating systems, software, applications supported listed in Appendix 6 and Protocols In Use listed in Appendix 7). The diversity of the applications riding on the USTRANSCOM DSE (C2 systems, information management systems, mail/message systems, and security systems) compound the integration of new system requirements. The information security environment on the segments of the USTRANSCOM DSE is a unique integration of products demanding a high degree of technical capability.

1.2. Scope

The contractor shall plan for all tasks identified in this task order and gather all pertinent information. Contractor estimates and timelines shall be determined based on the deliverable due dates specified in each task. The contractor shall coordinate with the Government to ensure that all activities are well synchronized and integrated with other USTRANSCOM and distribution management efforts, and that replicated or overlapping efforts do not occur. All reports, studies, or policies identified in the PWS to be accomplished shall be prepared and submitted for Government approval.

The contractor shall provide the necessary trained and fully qualified personnel, supervision, task management, and technical services required for the successful accomplishment of the requirements of this task order. During the course of the performance of the task order, Government changes in the technical environment or functional areas of the systems under the task order may occur that will require contractor personnel to obtain new skills and training. In such situations the Government, with prior agreement, may permit the contractor to attend Government provided training or share the cost of outside technical training. Such situations are anticipated to be rare occurrences and will be evaluated on a case-by-case basis by the Contracting Officer Representative (COR). Requirements for this task order are envisioned to be primarily on-site, but could extend to remote site interfaces and support with Government approval. The contractor shall provide all of the requirements described in this PWS.

The task areas and associated specific tasks are:

Task 1: Contract Level and Task Order Management
Task 2: Helpdesk, Desktop Customer, and Service Desk Support
Task 3: Computer System Maintenance and Logistics Support
Task 4: PC Maintenance and Software Management Support
Task 5: Special C4 Support Function
Task 6: Training/Lab Function
Task 7: USTRANSCOM Information Assurance and Information Protection (IA/IP)
Task 8: Project and Program Management
Task 9: Audiovisual and Video Teleconferencing Support

1.3. Specific Tasks

1.3.1. Task 1: Contract Level and Task Order Management

This task consists of the functional activities relating to the administration and management of this effort. The contractor shall provide program management of contractor personnel performing tasks in

this task order. The contractor shall designate a principal point of contact for technical issues. The contractor shall provide a centralized program management capability at the contractor site. This function shall encompass administrative, clerical, documentation, and related functions that provide general support for the program. The contractor shall provide support by preparing documents such as briefings, point papers, and meeting minutes related to status of the performance of this task order. The contractor shall be required to provide support in the specific areas outlined below in this PWS.

The contractor shall provide all deliverables listed in paragraph 1.4, referenced documents, and contractor-developed and Government approved plans, schedules, and milestones. The contractor shall meet stated Government requirements and milestones. If milestones are missed, the Government must be notified in writing within 24 hours of the missed deadline.

The Project Manager is the authorized point of contact with the Government COR. Responsibilities include, but are not limited to, interfacing with Government management personnel, staffing of all tasks, formulating and enforcing work standards, assigning schedules, reviewing work discrepancies, and communicating policies, purposes, and goals of the organization to subordinates.

All decisions regarding Government requirements or Government actions shall be made by Government personnel and the contractor's representative shall submit evaluations, recommendations, etc. to the COR and/or Contracting Officer (CO) for further action.

1.3.1.1. Task 1 Subtask 1: Task Order Management Plan (TOMP)

The contractor shall update the TOMP submitted with their proposal within fifteen (15) business days of the task order start date. The Government will review the plan and provide comments to the contractor. The contractor shall have five (5) business days from receipt of the Government's comments to submit the final plan. The contractor shall update the TOMP each option year within fifteen (15) business days of the option year being exercised.

1.3.1.2. Task 1 Subtask 2: Monthly Status Report (MSR)

The contractor shall provide a MSR no later than the 15th of the following month. The status report shall list, by each active task/project area, the accomplishments of the reporting period. The MSR should outline a brief synopsis of the efforts completed, deliverables provided, and conferences and trips conducted/attended during the reporting period, and an overall evaluation of the task order to date. The report shall list for each task any issues, problem areas, and items that require Government action. The final MSR shall be submitted no later than the last business day of the final period of performance.

1.3.1.3. Task 1 Subtask 3: Conduct In-Process Reviews (IPRs)

The contractor shall conduct quarterly IPRs as scheduled by the Government. The IPR shall summarize status, progress, recommendations, and concerns in the development of any tasks or documentation described within this PWS. Presentation materials shall be prepared and provided to the COR two (2) business days prior to the IPR.

1.3.1.4. Task 1 Subtask 4: Trip Reports

Within five (5) business days of completion of any travel, the contractor shall submit a trip report to include the following details: purpose, location, length of trip, travelers, actual travel costs, individuals

contacted during trip, synopsis of all discussions, future actions identified, decisions made, and issues of concern arising during the trip.

1.3.1.5. Task 1 Subtask 5: Meeting/Conference Minutes

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes that detail the results as well as the impact of the meetings/conferences within two (2) business days after completion of the meeting/conference. Meetings/Conferences will generally take place during the normal duty hours listed in paragraph 4.1 but can extend beyond these core hours when needed to support major exercises, contingencies, and emergencies.

1.3.2. Task 2: Helpdesk, Desktop Customer, and Service Desk Support

1.3.2.1. Task 2 Subtask 1: SDDC Helpdesk and Desktop Customer Support

The contractor shall provide customer support in the form of technical and subject matter on-site and on-call assistance to the internal and external users. The contractor shall provide on-site Tier 1 and Tier 2 support for SDDC's Office Information Systems (OIS) NIPRNET and SIPRNET customers. SDDC Helpdesk Tier 1 and Tier 2 support shall be predominately located in the SDDC designated area of Building 1900W to accommodate the majority of SDDC users. The contractor shall also provide Tier 2 support to SDDC users in building 1700 by physically locating support in that building. The contractor shall provide courteous service to all customers. SDDC customer support hours are from 0630-1800 Monday through Friday. The contractor shall establish and maintain a documented knowledge base of problem resolutions, related to service requests and inquiries for both the NIPRNET and SIPRNET.

The contractor shall provide Tier 1 customer support to include but not be limited to answering calls, logging tickets, resetting passwords, and providing basic hardware/software support. The contractor shall also provide telephone resolution and remote desktop administration. The contractor shall create, track, monitor, and route all customer support tickets to the appropriate work teams (i.e. Information Assurance, firewall, system administrators, and telephone support).

The contractor shall provide Tier 2 support to include but not limited to operation and maintenance, setup and teardown of location LAN, Personal Computers (PCs), other hardware, WAN connections, Internet connectivity, including e-mail capability, or other voice and data communications, multimedia and printer capability. Desktop Support shall include configuration, maintenance, and troubleshooting of desktop platforms. The contractor shall perform workstation (Windows, Sun, UNIX, Linux, Apple) upgrades, new workstation setup/installations and/or replacement of workstations and peripherals troubleshooting analysis, diagnosis, and resolution of workstation and peripheral problems in accordance with (IAW) standard configuration for both NIPRNET and SIPRNET machines. The contractor shall provide integration of pre-event, post-event and operational IT support for SDDC at secondary Government local support sites, to include meetings, conferences and symposiums.

The contractor shall generate a helpdesk performance metrics report weekly no later than the first business day of each week. The report shall detail the number of calls, priority level of the calls, resolution, and time to resolution for each call. Performance metrics shall also include the number of new tickets, the number of open tickets, and the number of closed tickets; the number of tickets for moves, the number of tickets for changes, and the number of tickets for deletions. The report shall show ticket time

for resolution from open to close, number of unresolved tickets, and number of escalated tickets for each of the supporting Service Tier Levels (1, 2, and 3).

The Government estimates two (2) trips in support of this sub task.

1.3.2.2. Task 2 Subtask 2: USTRANSCOM Service Desk Support

The USTRANSCOM Service Desk, also known as the Help Desk, is the user's focal point for reporting, resolving if possible, and escalating all service delivery problems with IT systems and products. The contractor shall provide courteous service to all customers. The Service Desk provides varying levels of support depending on the system to include but not limited to answering calls, logging tickets, resetting passwords, and diagnosing and resolving issues for USTRANSCOM classified and unclassified office information systems, iDistribute.mil, Single Mobility System (SMS), Electronic Logbook, TRANSCOM Regulating and Command & Control Evacuation System (TRAC2ES), Web Services, and Electronic Information Management (EIM).

The contractor shall recommend to the Government a Service Desk tool suite that provides, at a minimum, incident logging and tracking, customizable reporting, knowledge base development and access for both network support technicians and customer searches for status updates and common problem resolution no later than 31 October of the base period. The contractor shall implement the recommended Service Desk tool suite upon approval of the Government. USTRANSCOM currently uses a Remedy based trouble ticket and reporting application maintained within USTRANSCOM.

The contractor shall provide support from 0630 to 1830 local time, Monday through Friday. The contractor shall provide on-call, off-site support utilizing cell phone and laptop with Unclassified Virtual Private Network (VPN) capability 1831 – 0629 local time on weekdays, and all day on weekends and holidays. A Government representative shall make the determination if the on-call helpdesk technician needs to come on-site to respond to the ticket. The contractor shall augment weekend coverage for reserve forces requirements and for USTRANSCOM exercise support, on average once a month with a four-hour time frame on a specified weekend day.

The contractor shall perform Equipment Custodian (EC) duties and maintain proper accountability of all Government owned/purchased hardware IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each task order year.

1.3.2.2.1. Incident Reporting

The contractor shall be the central point of contact for all calls and e-mails related to any IT incidents or requests affecting USTRANSCOM customers utilizing USTRANSCOM systems, applications and/or services. The contractor shall log all incidents and requests and categorize and prioritize each IAW paragraph 2.1. In response to a reported incident the contractor shall record each incident within the approved USTRANSCOM event management application and if possible, provide an immediate recommended solution, or search for a workaround.

1.3.2.2.2. Incident Management

The contractor shall manage the lifecycle of all incidents and requests from initiation to closure, actively pursuing updates and escalation IAW paragraph 2.1. The contractor shall perform first-line investigation and diagnosis of the incident and attempt to resolve on customer's first call to the Service Desk. For those calls the Service Desk determines they are unable to resolve on the first call, the technician shall provide the customer applicable information on their incident and escalate to the applicable work center for continued diagnosis and resolution. The contractor shall insure all users are informed of their incident or request status when the issue persists beyond the resolution times IAW paragraph 2.1.

1.3.2.3. Task 2 Subtask 3: USTRANSCOM Service Desk Extended Support (Optional)

The contractor shall provide service desk support IAW and to the same level of support as detailed in paragraph 1.3.2.2 on-site, versus on-call, on a 24/7 basis as required by the Government.

1.3.3. Task 3: Computer System Maintenance and Logistics Support

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

The contractor shall provide life cycle support (equipment in use beyond warranty) for unclassified and classified USTRANSCOM C4 infrastructure located at Scott AFB IL and the Defense Enterprise Computing Center (DECC)-St. Louis site.

A list of equipment in use beyond warranty shall be maintained by the contractor and referred to as the B-3 Table. An initial B-3 Table shall be submitted to the Government no later than ten (10) business days after task order start. Updates to the B-3 Table shall be provided to the Government within five (5) business days upon any change.

The contractor response time from Government notification is 24 hours to start work on location, excluding weekends and holidays. Expected restoral is within 48 hours, excluding weekends and holidays, after work start. Maintenance under this category shall not be required during other than principal period of maintenance (PPM) periods. B-3 Table equipment is "per call" and includes materials, tools, diagnostics, test equipment, documentation, and travel. Replacement parts or equipment shall be acquired IAW paragraph 4.4. The Government estimates approximately 20 calls per year. As previously stated, there may be occasional situations where the Government will waive the specified repair time. This will occur when there is no impact on the mission and it is cost advantageous for the Government to wait for the shipment of replacement parts.

1.3.4: Task 4: PC Maintenance and Software Management Support

The contractor shall maintain USTRANSCOM IT assets existing at the client level (tier 1 assets) and manage a software library of all software in use at USTRANSCOM.

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

The contractor shall identify a focal point to the Government for this task.

1.3.4.1. Task 4 Subtask 1: PC Maintenance

The scope of this task covers all manufacturers' brands of desktop and laptop computers used by USTRANSCOM personnel in their day-to-day business. The estimated number of workstations and laptops is listed in Appendix 4. There is an expected growth rate of workstations and laptops of approximately one percent per year.

The contractor shall perform on-site support for this subtask during the normal duty hours listed in paragraph 4.1. PC Maintenance office operations may be extended to 24-hours per day and 7-days per week during real-world events, contingencies, exercises, or as requested by the Government.

The contractor shall perform Equipment Custodian (EC) duties and maintain proper accountability of all Government owned/purchased hardware under their control IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each period of performance.

1.3.4.1.1. Maintain UOIS Baseline Images

The contractor shall create, edit and coordinate UOIS baseline images for USTRANSCOM; coordinate UOIS image instruction with appropriate functional areas and obtain approval from the process owner; create UOIS baseline image for each hardware platform implemented within 14 business days after hardware receipt by PC Maintenance; coordinate an image security scan; coordinate image functionality test; record and store copies of all created UOIS images; and update stored copies of all UOIS images with approved application software, application patches and registry changes.

1.3.4.1.2. Install OIS Client Workstations

The contractor shall insure installation of the applicable, approved baseline image (e.g. USTRANSCOM, Air Force Standard Desktop Configuration, etc.) on workstations to include peripherals; install unique software on the USTRANSCOM or US Air Force Approved Products List (APL) approved through the Cyberspace Infrastructure Planning System (CIPS) process; deliver workstation to customer work area; configure and connect workstation, and test workstation for functional operation.

1.3.4.1.3. Repair OIS Client Workstations

The contractor shall respond to customer requests for maintenance actions submitted through the USTRANSCOM Service Desk IAW paragraph 2.1; track customer requests for maintenance using the USTRANSCOM trouble ticketing system; regularly update user and trouble ticket with troubleshooting actions, diagnosis of problem, and resolution actions; respond to customer work area when needed; retrieve customer system for repair if required; and deliver customer system after repair within one (1) business day for on-site customers and two (2) business days for off-site customers.

1.3.4.1.4. Warranty Claims Processing

The contractor shall determine if failed system or component is warranted; contact appropriate manufacturer; obtain replacement parts; and return defective system or component to manufacturer in accordance with manufacturer's disposition instructions.

1.3.4.1.5. Laptop Loaner Program

The contractor shall manage and control the temporary issuance of laptop computers to USTRANSCOM personnel. The contractor shall staff the customer service area during normal duty hours listed in paragraph 4.1; issue laptop computers as requested by the customer; complete an equipment hand receipt; issue equipment; configure laptop computer as needed by the customer to include synchronizing with the customer's mailbox, if requested; test the VPN connection software and hardware with the customer; inventory ancillary equipment; provide customer with operating instructions; respond to customer questions; receive equipment; inventory ancillary equipment; provide customer with receipt of return; re-image laptop computer; track overdue equipment; contact customer requesting status of the overdue laptop; and inform Government task lead of status of overdue laptops.

1.3.4.1.6. Implement Computer Equipment Replacement Program (CERP)

The contractor shall track lifecycle of installed workstations based upon a 4 year life expectancy; provide the Government with annual projection of hardware requirements based on life cycle expectancy and warranty expiration no later than 1 July each period of performance; and use Government furnished equipment to accomplish CERP.

1.3.4.1.7. Prepare Inoperable or Lifecycle Depleted Computers for Turn-in

The contractor shall remove magnetic media, degauss media IAW degaussing device manufacturer's directions, and wipe media IAW Government instructions; track degaussing/wiping activities in a log; and transfer to Inventory Control Team for disposition. The contractor shall provide the degaussing function for USTRANSCOM users and additional Scott AFB organizations when requested and as available.

1.3.4.2. Task 4 Subtask 2: Software Management

The Government estimates three (3) trips in support of this sub task.

1.3.4.2.1. Configuration Management

The contractor shall assist with the development and maintenance of Enterprise Software (ES) policy for USTRANSCOM.

The contractor shall document, track, and maintain inventory of software owned by USTRANSCOM by contract number and provide the inventory no later than the 5th business day of each month. The contractor shall develop a catalog of ES within 40 business days of the task order start date. The contractor shall maintain the ES catalog to reduce duplication and distribution of ES. The contractor shall maintain documentation of all ES software transactions such as allocation, media distribution, requirements gathering, and return of unused software. The contractor shall work with sales representatives to ensure that USTRANSCOM ES has copies of all software owned by USTRANSCOM. The contractor shall distribute documentation as needed by software users. The contractor shall work with USTRANSCOM program managers (PMs) to develop an accurate list of required software and maintain an ES requirement list by program, for future reference, and provide the requirement list no later than the 5th business day of each month.

The contractor shall prepare and deliver ES cost/benefit analyses within ten (10) business days of the Government's request. The contractor shall work in coordination with the PMs and COR to clearly define the options for ES products and define the costs, benefits, and potential risks associated with any course of action. The contractor shall provide a recommendation for proceeding based on cost/benefit

findings. The contractor shall prepare an initial cost/benefit briefing within 80 business days of the task order start date and an annual briefing no later than 31 March each period of performance.

The contractor shall work in coordination with the COR, PMs, contract managers, and budget managers to assist in the development of acquisition packages for execution of new and renewal of ES license contracts.

1.3.4.2.2. Software Library

The contractor shall create and maintain a library of software approved via the USTRANSCOM CIPS process to include operating systems (including service packs), commercial applications, and Government applications implemented within USTRANSCOM; create and maintain the USTRANSCOM APL; publish the APL on a Government provided information system accessible to the entire command; use the existing USTRANSCOM Automated Data Processing Equipment (ADPE) environment to create a logical storage framework for all enterprise software artifacts to include: Software Product information, Enterprise Software Initiative (ESI) Cost/Benefit Analyses, Software Allocations, ES transactions, ES Briefs, point papers, related documents, ES contracts and acquisition documentation; and maintain a record of the software library content. Updates and additions to the software library will be completed within five (5) business days of the Government's request.

1.3.5. Task 5: Special C4 Support Function

The contractor shall provide a special C4 support function responsible for implementing and maintaining C4 executive-level information technology services to include but not limited to mobile/wireless computing support and telecommunication support to USTRANSCOM and SDDC senior-level executives, their immediate support staff, USTRANSCOM Liaison Officers (LNOs) located at various Combatant Commands throughout the world (currently 7), and other senior managers approved by the USTRANSCOM Chief Information Officer (CIO). The service provided to the LNO shall be in accordance with standing Command Arrangement Agreements.

On-site services for this task shall be provided 24x7 as required to support major exercises, contingencies, and emergencies. A technician's work week shall not exceed 40 hours. Other periods can be covered with on-call service. Response time during on-call periods shall be no more than two (2) hours to begin work on-site. The contractor shall provide inputs to weekly activity reports no later than the close of business on Wednesday of each week.

The contractor shall identify a focal point to the Government for this task.

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

1.3.5.1. Task 5 Subtask 1: Senior Management Support

The duties of the contractor require the research, design, testing, and implementation of C4 technical solutions supporting senior level management, their support staff, and LNOs for both unclassified and classified command and control requirements. These duties shall also include the analysis, development, and integration of Distribution Process Owner (DPO) communications requirements and capabilities. Support includes building, deleting, and maintaining UOIS domain, COIS domain, and e-mail accounts; configuring, supporting and troubleshooting desktops, laptops, software, printers, desktop Video

Teleconferencing (VTC) equipment, and other peripherals; and supporting and troubleshooting network connectivity. These requirements also include remote worldwide command and control connectivity, and command and control functions in quarters and during Temporary Duty (TDYs). This support shall provide network systems administration, client configuration, technical and troubleshooting activities supporting the remote access program for both the classified and unclassified local area networks.

The contractor shall act as the liaison for coordinating communications and computer support requirements for the commanders' worldwide visits. The contractor shall monitor and report planned, unplanned, and potential system outages to senior-level executives for coordination and approval. The contractor shall provide executive-level users off-site unsecure and secure remote access service (e.g. dial-up, VPN, etc.) capabilities into the UOIS and COIS, to include support to AMC's classified network, allowing full access to network resources to include: email, network folders, and worldwide web browsing capabilities. The contractor shall provide set-up and configuration of laptop, appropriate software, and troubleshooting diagnosis of equipment required for remote access. The contractor shall be knowledgeable on the technical/architectural requirements associated with DPO communications interfaces and supporting network infrastructures. The contractor shall provide continuous support to flag officers and Very Important Person (VIPs) on a daily basis, five (5) days per week, 12 hours per day and on-call as required.

1.3.5.1.1. USTRANSCOM Senior Management Support

The contractor shall provide support to USTRANSCOM senior management IAW and to the same level of support as detailed in paragraph 1.3.5.1.

Core on-site hours are from 0500 to 1700, Monday through Friday. On-call hours are from 1701 to 0459, Monday through Friday, and 24 hours per day during weekends and holidays.

The Government estimates four (4) trips in support of this paragraph.

The contractor shall perform Equipment Custodian (EC) duties and maintain proper accountability of all Government owned/purchased hardware IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each task order year.

1.3.5.1.2. SDDC Senior Management Support

The contractor shall provide support to SDDC senior management IAW and to the same level of support as detailed in paragraph 1.3.5.1.

Core on-site hours are from 0600 to 1800, Monday through Friday. On-call hours are from 1801 to 0559, Monday through Friday, and 24 hours per day during weekends and holidays.

On occasion, it may be necessary for the "flag support" to travel with the SDDC Commanding General for IT support. The Government estimates two (2) trips in support of this paragraph.

1.3.5.1.3. AMC Senior Management Support

The contractor shall provide limited support to AMC senior management IAW and to the same level of support as detailed in paragraph 1.3.5.1.

Core on-site hours range from 0500 to 1700, Monday through Friday, but a technician's work week shall not exceed 40 hours. This function shall work on-call on a periodic basis when required by the Government. On-call hours are from 1701 to 0459, Monday through Friday, and 24 hours per day during weekends and holidays.

1.3.5.2. Task 5 Subtask 2: Portable Electronic Device (PED) Support Services

The contractor shall provide support for USTRANSCOM's PED program for both the unclassified and classified devices. USTRANSCOM currently uses primarily Blackberry devices but this support is not limited to this product. Support includes issuance, initial configuration, technical support and troubleshooting, upgrades, and recommendation of hardware and software upgrades and life cycle replacement. The contractor shall provide mobile phones with worldwide capabilities to USTRANSCOM senior-level executives, as required.

The contractor shall maintain a database of accounts, and hardware/software configuration, and ensure all USTRANSCOM and National Security Agency directives for security and configuration are met for applicable devices. The contractor shall submit, provide solution recommendations within three (3) days of the Government's request, and implement approved requirements utilizing the USTRANSCOM CIPS or similar tracking systems within five (5) business days of approval. The contractor shall respond to customer service requests and inquiries using the Remedy or manual accounting IAW Section 2.1, as applicable. The contractor shall review and track billing and costs on a monthly basis. The contractor shall perform an annual revalidation of all issued user devices to include hardware inventory and recommending changes to specific mobile access plans (increasing, decreasing, or eliminating). The contractor shall provide an annual revalidation report no later than 1 February each period of performance.

1.3.5.3. Task 5 Subtask 3: Telephone Support Services

The contractor shall perform the Telephone Control Officer (TCO) Function for USTRANSCOM. The contractor shall act as the focal point for all telephone-related matters, e.g., requests new telephone service, changes to existing services, mobile phones, and relocation of existing phones. The contractor shall maintain an inventory of Government provided replacement phones (POTS (plain old telephone system) and VOIP/VOSIP (Voice over Internet Protocol/Voice over Secure Internet Protocol) for all break/fix actions. The contractor shall coordinate with the Government to refill used stock of phones when below pre-determined level. The contractor shall submit, track, and manage telephone service requests (TSRs) through the host base directed system/method, currently via CIPS. The contractor shall manage Personal Identification Numbers (PINs) for USTRANSCOM to include: PIN issuance, PIN deletion, PIN transfer, and maintenance of the PIN database.

The contractor shall submit updates to the base telephone directory and Defense Red Switch Network (DRSN) telephone directory; verify official toll calls; and provide customer education. The contractor shall verify DRSN telephones belonging to the commander and deputy commander's office daily to ensure operability and notify the 375th Communications Squadron, Maintenance Control function if problems exist and take follow-up action as required.

The contractor shall manage the USTRANSCOM Long Haul Telecommunication program. The contractor shall submit, review, and validate all telecommunication requirements via the CIPS program or similar tracking system. The contractor shall coordinate telecommunication requirements with the 375th Communications Squadron, Air Force Network Integration Center (AFNIC), Defense Information Systems Agency (DISA), and Defense Information Technology Contracting Office (DITCO), as required. The contractor shall evaluate requirements submitted through the CIPS process or similar tracking systems. The contractor shall support technical conclusions for customer's requirements, relative costs, and advantages of alternate approaches, lead times, and supporting requirements. The contractor shall negotiate with customers concerning modifications of requirements to reduce anticipated technical problems, excess costs, and schedules for required services. The contractor shall semi-annually review and validate all long haul circuits (Communication Service Authorization) utilized by USTRANSCOM. The contractor shall work with the Government to re-award circuits when current vendor's contracts expire. The contractor shall assist the Government in maintaining records on all circuits owned by USTRANSCOM.

1.3.5.4. Task 5 Subtask 4: Telephone Implementation and Integration Support (Optional)

The contractor shall support the Scott AFB telephone service provider, the 375 Communications Group, with the installation and configuration of POTS and VOIP telephony solutions to include the installation of cable (e.g. copper, fiber) and other materials for USTRANSCOM users.

The contractor shall install all patch cables and cross connects, properly labeling dressing, and tying neatly all patch-cables in compliance with industry standards. The contractor shall coordinate with Government personnel prior to programming and configuring all network switches for unclassified, classified, VOIP and VOSIP local area networks. The contractor shall coordinate with the Government when provisioning and configuring the Centrex Internet Protocol (IP) Switch prior to any configuration changes. The Government will provide the contractor with all the information necessary to program and configure all unsecure (Nortel) VOIP and secure (Cisco) VOSIP telephony handsets (for example, IP addresses and telephone call groups). The contractor shall coordinate with Government representatives from the 375 CS/SCOI voice, the 375 CS/SCPSC Computer Support Technicians (CST) network maintenance, and USTRANSCOM J6-O network technicians for all technical and oversight support standards. Conflicts will be resolved by the Government. The contractor shall be responsible for the purchase, installation, configuration, setup, and testing of all VOIP AND VOSIP communications end-to-end equipment not provided by the Government. All equipment should fully emulate the current phone configuration and service used today.

1.3.5.4.1 Telephone Configuration Services

The contractor shall install and configure, under the oversight and in coordination with the 375th Communications Group, Traditional (Analog) Voice, VOIP (NORTEL)/VOSIP (CISCO) systems, test VOIP/VOSIP end instruments, and a Dynamic Host Configuration Protocol (DHCP) Server, which are dedicated to support VOIP operations. The contractor shall decommission legacy telephones on the Scott AFB DMS100 as required when the end-user receives an IP telephone and traditional line will no longer be used. The technical environment includes, but is not limited to, the following:

Hardware:
Centrex IP Switch – Government Provided -- NORTEL DMS100 (SL-100 / CS2100)
Voice End Instrument – Details to be provided

Software:
Centrex IP Switch -- Call manager CS2100 SE0 9.1

For assistance on Nortel Engineering and prior to any part ordering please contact the Avaya Government Solutions representatives' Mr. Jim Hill and / or Doug Southall

E-mail: jim.hill@avayagov.com
Mobile Phone: 1.618.567.4072

E-mail: Douglas.Southall@avayagov.com
Mobile Phone: 1.617.515.7279

1.3.5.4.2 Traditional Voice (Analog)

The contractor shall install and configure handsets and PBX switch Government furnished traditional phone instruments and fax machines as required.

1.3.5.4.3 Unsecure Voice (VOIP)

The contractor shall engineer, furnish, install, and test all necessary additional CS2100 hardware and software needed to expand the CS2100's VOIP capabilities. The contractor shall also procure, install and configure both Government Furnished Equipment (GFE) and Contractor Furnished Equipment (CFE) VOIP telephony handsets for Succession Enterprise version: Nortel SE0 9.1. All VOIP switch configuration shall be completed at Building P-5 under the oversight and in coordination with the Government VOIP engineering team (375 CS/SCOI). The contractor shall also ensure that all base infrastructure systems (VOIP Server / DHCP server) and connectivity employed to support the voice/VOIP install are readily acceptable from a hardware, software, and connectivity standpoint back to Building P-5. The contractor shall formulate a complete master cut-sheet that allows for data input of each and every VOIP device on a per-person /per-telephone number basis to include all line key options and templates as specified. The Government will act as the end user and coordinator for services to be rendered – but the peril of the entire survey / install and configuration as concerns line datafill, options, templates, voice mail, update Telecommunications Management System (TMS) and complete all records after the fact is placed on the contractor to generate and perform. The contractor shall program and provision all devices from the Base Central Office switch/Private Branch Exchange (PBX)/or Call VOIP server. The contractor shall also build and provision voice mail boxes utilizing the local Callware (Callegra) Voice Mail System. The contractor shall also provide Certified NortelTier-3 level support and provide a certified Nortel engineer who shall install / configure the contractor furnished hardware and software on the SL100/CS2100; and then the engineer shall subsequently perform representative sample tests needed to fully demonstrate that the expansion resources and tasks for the upgraded SL100/CS2100 operate correctly in a SE0 9.1 environment. The contractor shall install and configure, under the oversight and in coordination with the 375th Communications Group SCXP, 375 CS/SCOI voice and network maintenance, the 375 CS/SCPSC CSTs and USTRANSCOM J6-O network technicians on all CFE VOIP end instruments using the current dedicated DHCP Server.

1.3.5.4.4 Secure Voice (VOSIP)

The contractor shall install a media converter at the fiber cable present at the end user's work area. The contractor shall install Category 6 shielded, twisted pair cable extending from the media converter to a VOSIP phone. The contractor shall install another category 6 shielded, twisted pair cable shall extending from the VOSIP phone to the SIPRNET computer terminating at the RJ45 port of the workstation. The

contractor shall configure the VOSIP handset to include coordinating with the VOSIP engineering team to receive the proper IP address.

The contractor shall configure each switch port to isolate VOSIP traffic to a particular voice Virtual Local Area Network (VLAN) and port security shall be modified to allow Media Access Control (MAC) address for the VOSIP phone. The directory number will be assigned by the Government VOSIP Engineering team. The contractor shall coordinate with the Government VOSIP engineering team to obtain the IP address required for the configuration of the VOSIP telephony handsets.

1.3.6. Task 6: Training/Lab Function

The contractor shall develop a training program for current and new applications or software tools and assist in the gathering of requirements for future development. The software support function applies to both classified and unclassified applications and software. The Government will provide the necessary support facilities and equipment at Scott AFB, IL. The Government will also provide reproduction of individual student course materials.

The contractor shall also augment the Unclassified OIS function by providing "individual training" or "advanced training" for those Help Desk calls regarding application questions that cannot be resolved by the help desk. The contractor may be required to submit a CIPS requirement for more complex problems.

The contractor shall perform Equipment Custodian (EC) duties and maintain proper accountability of all Government owned/purchased hardware IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each task order year.

1.3.6.1. Task 6 Subtask 1: Program Support

The tasks required in supporting the program support include but shall not be limited to: providing requirements assessments for newly identified software requirements to gather feedback from users within only the USTRANSCOM directorates for input into continued system development; providing research and analysis for new software; testing software against functional requirements for feasibility; maintaining an isolated LAN to be used with the implementation, testing, and operation of selected software prior to sending the software to the Test Center for testing against the network; suggesting software solutions; assisting with the development of product demonstrations and briefs; serving as liaison between Information Technology Services and command communication; and keeping abreast of current technology trends and software. Support may include traveling to users located at MSC. Support may also include requirements submitted by SDDC.

1.3.6.2. Task 6 Subtask 2: Training Support

The training task shall include detailed instruction on the use of selected network and other C4S services. The contractor shall be responsible for the development, presentation, and maintenance of all C4S course material, curricula, and critiques. The Government will provide at least twenty (20) business days advance notice, prior to the first scheduled class in each module, for module development and instructor preparation. Courses shall be presented in modular form unless otherwise specified by the Government. The Government will manage scheduling for all C4S courses provided by the contractor. The Government will work with the directorate training coordinators to schedule students, ensure availability

of training facilities and materials, and administer training quotas. Classes shall normally be held during the normal duty hours listed in paragraph 4.1. The Government will make final determination of level and number of classes taught; class schedule (to include dates and time); and class size. The Government will be responsible for deviations of class schedules to include notification to the student. The contractor shall provide one-on-one training for all courses to personnel as requested by O6 equivalent (or above) for either himself/herself or a member of his/her staff on an as-needed basis. The contractor shall base training plans on the complexity of the course materials and the depth of training requested by the Government. Plans are subject to Government approval. The contractor shall provide a formal training plan within twenty-five (25) business days after task order start. The plan shall summarize the contractor's training philosophy/ methods for each course; identify objectives and completion criteria for each course; outline the content of each course; and recommend a comprehensive class schedule with the start and stop dates. This training plan shall also identify any training devices, aids, or equipment needed to support each course, and the estimated lead-time the instructor needs to prepare for each course. As new modules are developed, or major changes or modifications are made to existing modules, the contractor shall deliver a revised Training Plan within twenty-five (25) business days after written notice from the Government. Change may also be required as a result of modifications to USTRANSCOM policies and procedures. Courses shall address the following at a minimum:

1.3.6.2.1. Functional Area Communications and Computer Systems Manager (FACCSM) Orientation/Awareness

Initial training for all FACCSM's shall provide guidance concerning the organizational structure of the network, clarify FACCSM duties and responsibilities, and clarify where to go for support. All incoming personnel assigned to serve as FACCSM's will be required to attend a certification course providing them with the basic knowledge required to perform their duties. Training shall include guidance in the following areas at a minimum: where to go for Tier 2 support; basic troubleshooting tips for common problems; the do's and don'ts of the unclassified network; inventory, accountability, ordering, and delivery processes; maintenance procedures; security processes and procedures. FACCSM courses shall be taught when class enrollment reaches a minimum of five students or at least every four months as determined by the Government.

1.3.6.2.2. Office Track

The contractor shall develop, prepare, maintain, and teach a range of courses and curricula required to support USTRANSCOM personnel. Courses shall encompass basic, intermediate, and advanced training for the following software: Word, Excel, PowerPoint, Access, Project, Internet Explorer, Mozilla, Outlook, SharePoint, Task Management Tool (TMT), Total Records and Information Management (TRIM), Any Business Entity – Relationship Management (xRM)

1.3.6.2.3. Automated Message Handling System (AMHS)

The contractor shall develop, prepare, maintain, and teach an AMHS course and curricula. This course shall provide instruction in the following areas at a minimum: compose, send/release, receive, and print messages; create folders; search feature; use of personal address book, global address book, and directory information tree (DIT); use of DIT browser; and basic do's and don'ts.

1.3.6.2.4. Staff Officer Tools

Staff Officer Tools include USTRANSCOM OIS products as they relate to web and portal tools, and task support tools (e.g. SharePoint, iDistribute.mil, TMT, and TRIM, etc). Students in this track will include current users transitioning to new tools/capabilities, indoctrination training for newly arrived personnel, and FACCSM's in order to understand user tool sets and requirements. Courses shall provide instruction on use and functionality of the tools to perform daily staff officer tasks.

1.3.6.2.5. Gatekeeper Training

The contractor shall develop, prepare, maintain, and teach a Gatekeepers Course and curricula in support of USTRANSCOM web sites. This course shall provide instruction in the following areas at a minimum: Gatekeeper basics; Web page approval process; basic do's and don'ts for maintaining Web pages; basic do's and don'ts for maintaining SharePoint sites; where to go for help; Portal Content Manager (PCM); and Adobe Acrobat.

The contractor shall provide support to the USTRANSCOM Web Site Portal team to ensure that training and operations are coordinated, stay current on any changes to the Gatekeeper processes; and prepare and maintain course curricula.

1.3.6.3. Task 6 Subtask 3: Support for New Training Requirements

The contractor shall develop and deliver a formal course for training USTRANSCOM personnel on new applications or software tools. The contractor shall provide appropriate training plan, manuals, and feedback forms for users. The instructor shall work with Government personnel to finalize course requirements. Once the course requirements are finalized, the contractor shall provide a formal training plan within twenty-five (25) business days. The plan shall summarize training methods for each course; identify objectives and completion criteria for each course; outline the content of the course; and recommend a comprehensive class schedule with start/stop dates. This training plan shall also identify any training devices, aids, or equipment needed to support each course and the estimated lead-time the instructor needs to prepare for each course. As technology is constantly evolving, the contractor shall prepare revised training plans within twenty-five (25) business days after written notice from the Government.

1.3.6.4. Task 6 Subtask 4: Training Videos and Computer Based Training (CBT) Development (Optional)

The contractor shall develop, prepare, maintain, and publish training videos and CBTs on designated training courses, applications, or systems as required by Government. With the exception of Government provided content, the contractor shall provide or arrange for the creation of all audio and visual content required to deliver the finished work in photo-realistic 3D animation, motion graphics, video acquisition, B-roll and voiceover talent and music. The finished work shall be delivered in the DVCPro50 format as well as DVD mastering for streaming and download via the internet. If necessary the contractor shall provide or arrange videotaping of persons using a "green screen" background for addition of themed backgrounds that can be altered. The contractor shall deliver all video graphic components including original working files, graphics, animations, audio files, and other components that shall permit the Government to edit future versions. The contractor shall produce a draft version for Government review and approval within forty (40) business days of Government request and produce a final distribution-ready version within ten (10) business days of receipt of Government comments.

1.3.7. Task 7: USTRANSCOM Information Assurance and Information Protection (IA/IP)

The contractor shall provide support for USTRANSCOM's Information Assurance (IA) Program, including system security engineering, policy review and development, certification and accreditation documentation, COMSEC coordination duties and design and deployment of service assurance infrastructure. In addition, the contractor shall provide both guidance and assistance to the TCCs in developing and maturing their IA postures.

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

The contractor shall identify a focal point to the Government for this task.

The Government estimates two (2) trips in support of subtask 1; ten (10) trips in support of subtask 2; four (4) trips in support of subtask 2, paragraph 1.3.7.2.2; and two (2) trips in support of subtask 4.

1.3.7.1. Task 7 Subtask 1: Engineering Support

The contractor shall provide security engineering support to USTRANSCOM. On-call requires a response time within one (1) hour to begin work. During periods of major exercises, contingencies, and emergencies, the contractor shall provide support on-site 24x7. In support of USTRANSCOM development activities, the contractor shall: review proposed changes to ensure that new computer systems introduced into USTRANSCOM and the TCCs are IAW DOD and command computer security policies; evaluate software and systems as part of USTRANSCOM's test bed efforts and recommend approval or disapproval; provide technical security configuration guidance to systems during entire system life-cycle; research and advise the command on recently developed countermeasures designed to protect command systems from new threats; develop, implement, and administer effective security programs that are approved by the Government; and review all safeguard procedures to measure the effectiveness of the total system security and make formal security evaluations and recommendations to the Government based on these reviews IAW suspense assigned by the Government.

1.3.7.2. Task 7 Subtask 2: Communications Security (COMSEC) Manager

The contractor shall provide COMSEC support on-site 24x7, for up to a seven (7) day period during major exercises, contingencies, and emergencies upon request by the Government. This extended coverage specifically applies to support for secure voice capabilities, which involves operation, installation, and maintenance for secure telephones, secure mobile telephones, secure facsimile machines, and cryptographic secure voice keys as well as training to users and maintenance of records for secure voice instruments throughout the command. As part of the on-going daily support, the contractor shall provide COMSEC oversight for USTRANSCOM, the TCCs, and other direct reporting elements to include all USTRANSCOM sub-accounts. The contractor shall disseminate urgent, doctrinal, policy, and procedural COMSEC information with Cryptologic Systems Group (CPSG)/DIKWM at Lackland Air Force Base, San Antonio TX and AFNIC at Scott AFB, IL. The contractor shall perform all duties IAW applicable COMSEC policies. The contractor shall order and maintain COMSEC material. The contractor shall enforce Government-established controls so only properly cleared personnel with a legitimate need to know are permitted access to COMSEC material. The contractor shall maintain and assist in developing USTRANSCOM policies and procedures for handling, controlling, and protecting COMSEC assets to include, but not limited to, procedures for receiving, issuing, destroying, daily accountability, semiannual inventories, Two Person Integrity (TPI), and COMSEC incident reporting. The contractor shall assist in training users in the rules for use, safeguarding, controlling, and the proper

destruction of COMSEC aids. The contractor shall submit ad-hoc and recurring IAW suspense assigned by the Government (e.g. ad-hoc Practices Dangerous to Security (PDS), monthly Joint Training Information Management System (JTIMS), monthly Defense Readiness Reporting System (DRRS), etc.). The contractor shall request keying material for new missions and provide disposition instructions for keying material that is no longer required. The contractor shall operate the Electronic Key Management System (EKMS) Local Management Device (LMD)/ Key Processor (KP) for the generation of electronic cryptographic keys. The contractor shall serve as a Special Security Representative (SSR) for USTRANSCOM Sensitive Compartmented Information Facilities (SCIFs) and shall ensure compliance with SSR governing directives applicable to a SCIF. The contractor shall maintain a Cryptographic COMSEC Equipment Account (CCEA) and duties shall include: serving as the CCEA Custodian with Standard Base Supply System (SBSS) at Scott Air Force Base (SAFB); responsible for ensuring complete accountability for all Controlled Cryptographic Items (CCI) for USTRANSCOM to include ensuring CCI equipment is entered into SAFB SBSS account records and the COMSEC Material Control System (CMCS) as appropriate; and conduct semiannual inventories of assigned assets IAW COMSEC policy. The contractor shall develop a continuity book no later than 1 September of the base period of performance and an update each subsequent period of performance.

The contractor shall coordinate and manage the USTRANSCOM cryptographic account in accordance with AFI 33-211, COMSEC User Requirements, and Air Force COMSEC Publication AFKAG-1N, Air Force Communications Security Operations and Air Force COMSEC Publication AFKAG-2L, Air Force COMSEC Accounting Manual, thus ensuring cryptographic account administration meets all inspection requirements. The contractor shall issue COMSEC material to authorized personnel and also shall assist the COMSEC manager in the development of a comprehensive user-training program for COMSEC Responsible Officers. The contractor shall maintain current copies of all required cryptographic regulations, manage cryptographic agent training and scheduling, provide training on Secure Voice procedures and equipment, post policy directives and guidance regarding COMSEC, and provide point papers and briefings on COMSEC issues and requirements IAW suspense assigned by the Government. The contractor shall operate and maintain accountability for secure facsimile devices and coordinate cryptographic circuit maintenance. The contractor shall conduct daily accountability and semiannual inventory to account for all USTRANSCOM cryptographic materials and devices and coordinate acquisition of cryptographic keying materials and accountability of associated keys. The contractor shall obtain annual COMSEC monitoring requirements from USTRANSCOM and the TCCs, for submission to Joint COMSEC Monitoring Activity (JCMA), and assist the Government in the preparation of the annual USTRANSCOM COMSEC monitoring requirements message to the JCMA. The contractor shall also assist with the development of USTRANSCOM Critical Information List (CIL) as part of the Information Operations Planning Cell (IOPC); maintain the USTRANSCOM Inter-theater COMSEC Package (ICP) Program; coordinate and implement the COMSEC Education, Training, and Awareness (ETA) program; and publish articles and info grams IAW suspense assigned by the Government (e.g. COMSEC Policy Messages (CPM), etc.) as part of the ETA program. The contractor shall also monitor, evaluate, and participate in exercise, system, and device evaluation; provide After Action Reviews (AARs) regarding COMSEC issues; publish annexes and integrate USTRANSCOM ICP program as required for support to Contingency Plans (CONPLANS) and Operation Plans (OPLANS); and provide support to the CAT (Crisis Action Team) during real world and exercise missions IAW suspense assigned by the Government.

1.3.7.3 Task 7 Subtask 3: Certification & Accreditation (C&A) Support

The contractor shall support development of enterprise C&A documentation, review computer systems requirements documentation for security impact, provide guidance to programs in developing their C&A

documentation, evaluate security accreditation documentation, and enter data into the Enterprise Mission Assurance Support Service (eMASS) tool on NIPRNET and SIPRNET. In addition, the contractor shall support required e-Government reporting (i.e. Federal Information Security Management Act (FISMA)).

1.3.7.3.1. C&A Verification and Configuration/Vulnerability Management Activities Support

The contractor shall perform security assessments of USTRANSCOM systems to measure the effectiveness of the total system security and make formal recommendations to Government based on these reviews IAW suspense assigned by the Government. In support of USTRANSCOM configuration/vulnerability management activities, the contractor shall perform monthly vulnerability scanning of all USTRANSCOM systems, report vulnerability scanning results to the Government within three (3) business days of the completion of the scan, work with system administrators of USTRANSCOM systems to identify potential remediation actions for all identified vulnerabilities, and gather and maintain system configuration information (e.g. Information Assurance Vulnerability Management (IAVM) compliance) to monitor the USTRANSCOM unclassified and classified systems for compliance with command security policies.

1.3.7.3.2. C&A Documentation Support

The contractor shall maintain templates for DIACAP documentation that incorporate the security information that is standard for the USTRANSCOM network environment. The contractor shall assist and collaborate with program offices for required DIACAP documentation, to ensure consistency and accuracy of USTRANSCOM DIACAP documents. The contractor shall assess the technical and functional adequacy of IA controls in order to develop a DIACAP Executive Package to provide an accurate assessment of risk to the Government IAW suspense assigned by the Government.

1.3.7.4. Task 7 Subtask 4: IA/IP for USTRANSCOM Component Commands

The contractor shall provide support to assist component commands in enhancing the security of their TWCF systems and network architectures. The contractor shall coordinate with TCC representatives as requested by the Government, assist in the implementation of USTRANSCOM security standards within TWCF programs managed by the TCCs, assist in the identification of shortfalls in the TCCs' information protection capabilities, assist in the design of technical solutions to eliminate the shortfalls, and assist in the implementation of technical solutions on-site at TCC locations upon Government request. In addition, the contractor shall assist USTRANSCOM in evaluating the progress of the TCCs in meeting the requirements of the USTRANSCOM security architecture and applying lessons learned both through procedural/process changes and technology enhancements. The Government estimates travel to assist in the deployment of security mechanisms, technical assistance, or technical interchange visits with the TCCs.

1.3.8. Task 8: Project and Program Management

The contractor shall manage the implementation of IT solutions for projects specified by the Government. This support shall consist of providing technical implementation plans, designing and engineering implementable technical solutions, and building realistic implementation schedules. Draft technical implementation plans and schedules shall be submitted within ten (10) business days of project tasking and the final draft within five (5) business days of Government comment. The contractor shall verify that appropriate Government activities and approvals have been accomplished. The contractor shall coordinate implementation tasks with all involved teams and shall also provide updated status briefings to

the Government monthly or more frequent if requested by the Government. TCJ6-O will provide project validation and act as the Government lead and focal point for all incoming IT project support requirements. TCJ6-O will also establish reasonable time lines for accomplishing project requirements, validate proposed support options, provide frequent updates on all timelines/projects, constantly verify current courses of action (COAs), act as the OPR for all Government required actions, and provide Government-to-Government coordination as required.

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

The contractor shall perform Equipment Custodian (EC) duties and maintain proper accountability of all Government owned/purchased hardware IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each task order year.

1.3.8.1. Task 8 Subtask 1: Technical Project Management

The contractor shall assist the Government in performing project management support for USTRANSCOM unclassified and classified network infrastructure. The support includes both approved projects and validated C4S requirements.

1.3.8.1.1. Project Management

This support includes both researching courses of action, presenting decision briefings and/or papers, developing implementation plans and timelines, and coordinating approved projects through completion and turnover to the appropriate organization. The contractor shall assist the Government in researching and evaluating hardware and software solutions in support of USTRANSCOM. The contractor shall assist in analysis and documentation of requirements. The detailed responsibilities of the contractor may vary from project to project; however, the Government will define the responsibilities prior to each new project start. Infrastructure projects may have pre-established USTRANSCOM requirements and resources. In these cases, the contractor's objective is to take this information and organize it into Implementation Plans and then assist in directing the execution of planned actions to achieve the established goals. The contractor shall prepare appropriate briefs and information papers in support of project goals. The contractor shall keep the Implementation Plan and associated papers and briefs current for periodic updates to the Government. The contractor shall assist in ensuring all projects conform to the guidelines established for the JDDE and Joint Deployment and Distribution Architecture (JDDA). The contractor shall assist the Government with Corporate Governance Process (CGP) documentation.

It is the contractor's responsibility to assist in implementation planning of a project and overseeing the execution of its implementation. The contractor shall organize, develop, identify shortfalls, and implement elements of assigned projects. Once hardware and software procurements are identified, the contractor shall track and provide procurement status to the Government. When newly procured hardware arrives, the contractor shall coordinate the installation, acceptance, and the turnover of operations and maintenance responsibility to the responsible organization. The contractor shall brief final completion status to the Government to finalize Technical Project Management responsibilities.

The Government estimates approximately two (2) new projects started each month with varying complexity and timeline.

1.3.8.1.2. Requirements Processing Oversight Management

The contractor shall provide management and technical orchestration, for validated C4S requirements as identified by the Government to ensure technical solution and costing (TS&C) development, oversight coordination, to include integration and implementation with all appropriate offices. This task requires the contractor to act as the primary point of contact for all requirements assigned to TCJ6-O. The contractor shall manage all assigned requirements and track through completion. The contractor shall ensure proper routing and coordination occurs, to include coordination with external organizations when appropriate, via the USTRANSCOM requirements tool, currently CIPS, for both the TS&C development and implementation.

The contractor shall provide support by providing the Government status reports every other week that include, at a minimum: number of requirements currently open, closed since last report, newly opened, where requirements are in the process (TS&C, implementation, etc), and metrics for how long in each step of the process. The contractor shall notify the Government representative when issues arise in the process that requires Government involvement or resolution. The contractor shall recommend process improvements as identified via the bi-weekly report.

The Government estimates approximately sixty (60) new requirements per month of varying level of complexity.

1.3.8.2. Task 8 Subtask 2: Enterprise Infrastructure Management Support

The contractor shall assist the Government in performing technical engineering and program management support for USTRANSCOM enterprise infrastructure programs. The contractor shall provide management assistance to USTRANSCOM to include: planning, policy development, technical integration and interoperability, and life-cycle support. The contractor shall provide managerial assistance with DOD and USTRANSCOM directed programs/projects. Some major development programs/projects may have pre-established USTRANSCOM requirements/resources, where the contractor's objective is to take information and organize it into system development, implementation, and management plans and then assist in directing the planned actions to achieve the established goals. The contractor shall provide analysis of DOD publications and instructions when requested IAW suspense assigned by the Government. Additionally, the contractor shall prepare appropriate briefs, information papers in support of program goals such as the CIPS for products necessary to assess, implement, install, and monitor supported hardware/software no later than two (2) business days prior to the briefing. The contractor shall assist in analysis and documentation of requirements. The contractor shall assist in drafting procurement documentation. The contractor shall assist the Government with CGP documentation, Program Obligation Memorandum (POM), and Presidents Budget (PB) submissions.

1.3.9. Task 9: Audiovisual and Video Teleconferencing Support

The contractor shall identify a focal point to the Government for this task. The focal point shall be available during normal duty hours listed in paragraph 4.1.

The contractor shall setup, test, and operate audiovisual technologies existing within USTRANSCOM conference rooms. The contractor shall setup, execute and take down video teleconferencing (VTC) activities within USTRANSCOM VTC studios, and is responsible to design and provide technical engineering, documentation, and program support for USTRANSCOM program management of the

command's audiovisual and VTC capabilities. This effort will not include the operation and maintenance support of the Joint Worldwide Intelligence Communications System (JWICS), Joint Executive Video System (JEVS), or the Political Advisor's (POLAD) VTC system.

While USTRANSCOM conference rooms and VTC studios are disbursed throughout the USTRANSCOM campus of buildings design and technical engineering support may be required at other locations both on and off Scott AFB.

The contractor shall provide manning of the Audiovisual/Video Teleconferencing (AV/VTC) team from 0430 - 2200, Monday through Friday and the Briefing and Display Systems Support for the Fusion Center team 0430 - 1900, Monday through Friday, excluding federal holidays. Infrequent manning of the teams shall be required to support operations that occur outside of the required duty hours, during both weekdays and during weekends. The contractor shall provide a method of calling or recalling personnel to support unscheduled or short-notice requirements. Operations may be extended to 24x7 during real-world events, contingencies, exercise, or as requested by USTRANSCOM. The contractor shall support all scheduled operations.

All personnel in support subtasks 1 through 6 require Defense Information System Network ((DISN) Video Services (DVS)) VTC Non-Resident Phase Facilitator certification (formerly known as level one Facilitator certification).

The contractor shall attend meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government, and provide meeting/conference minutes IAW paragraph 1.3.1.5.

1.3.9.1. Task 9 Subtask 1: Audiovisual (AV) Support

The contractor shall provide operational and maintenance support of AV systems in USTRANSCOM conference rooms, training rooms, auditoriums, senior leader offices, video walls (e.g. Heritage Hall 4x4, Center Lobby 2x2), signage systems (e.g. Heritage Hall, Building 1900E Center Lobby, Building 1900E/W Connector, Building 1900W) and command center work areas on Scott AFB and provide operating instructions to AV customers. The contractor shall maintain USTRANSCOM AV systems. The contractor shall document and publish operator level instructions for USTRANSCOM AV systems within 20 business days of any changes or upgrades. The contractor shall provide user assistance and instruction for operating USTRANSCOM AV systems.

The contractor shall provide on-site AV support, to include but not limited to briefing assistance, for all USTRANSCOM Commander (TCCC), USTRANSCOM Deputy Commander (TCDC), and USTRANSCOM Chief of Staff (TCCS) attended briefing events on Scott AFB.

The contractor shall provide on-site AV support, to include but not limited to briefing assistance, for all events (e.g. meetings, briefings, distinguished visitors visits, award ceremonies, retirement ceremonies, and command presentations) in the Seay Auditorium and the Heritage Hall video wall in Building 1900E.

1.3.9.2. Task 9 Subtask 2: Video Teleconferencing Support

The contractor shall provide operational and maintenance support of both portable and fixed USTRANSCOM secure and non-secure VTC systems. The contractor shall maintain and configure USTRANSCOM VTC systems. The contractor shall manage scheduling and provide operational assistance as needed for conference initiation to VTC customers. The contractor shall resolve VTC studio

schedule conflicts by position or rank of the requiring authority. The contractor shall perform equipment alignments, calibrations, and system updates. The contractor shall execute on-site first-line troubleshooting and equipment repair or replacement. The contractor shall document and publish operator level instructions for USTRANSCOM VTC systems within 20 business days of any changes or upgrades. The contractor shall provide user assistance and instruction of USTRANSCOM VTC systems to include but not limited to VTC participation professionalism, microphone operation and hazards, general courtesies, and camera presence.

The contractor shall provide on-site VTC support, to include but not limited to facilitator support, for all USTRANSCOM Commander (TCCC), USTRANSCOM Deputy Commander (TCDC), and USTRANSCOM Chief of Staff (TCCS) attended VTC events on Scott AFB.

The contractor shall provide metrics for VTCs, compiled monthly and annually, that track VTC usage by time of day, number of VTCs per hour per day, VTC denials due to personnel shortage per hour of the day, and VTC denials due to room VTC capability shortage per hour of the day. Monthly metrics shall be provided no later than the 5th business day of the following month. Annual metrics shall be provided no later than the 10th business day of January each period of performance.

1.3.9.3. Task 9 Subtask 3: Server and Multipoint Control Unit (MCU) VTC Support

The contractor shall provide operational and maintenance support of Internet Protocol (IP) VTC Multipoint Control Units (MCUs), network traversal systems and software, VTC suite management systems. All personnel in support of this subtask require DVS VTC Resident Phase Facilitator certification (formerly known as level two Facilitator certification).

1.3.9.4. Task 9 Subtask 4: Engineering Design Support

The contractor shall assist the Government in the engineering design of AV/VTC systems. The contractor shall perform annual reviews of installed AV/VTC equipment and provide recommendations for upgrading equipment no later than 31 March of each period of performance. Recommendations may include but are not limited to brand-name equipment recommendations, installation methods and practices, data communication methods and practices, and updating of system operation guides. The contractor shall provide technical consultation during AV/VTC upgrades or equipment changes. The contractor shall work with the vendor contracted to execute system design and installation, insuring Government system operational requirements and capabilities are achieved. The contractor shall provide technical assistance to the Test and Integration Facility in the development and testing of new or modified equipment. The contractor shall provide technical assistance to assist the Government in developing migration strategies for implementing new AV/VTC capabilities.

The contractor shall submit circuit actions to support AV/VTC operations.

The contractor shall maintain and update a graphical representation of the VTC architecture quarterly no later than the 5th business day of each quarter in a format that can be modified by the Government. The contractor shall develop and maintain AV/VTC C&A products for connection approvals and DOD Information Assurance Certification and Accreditation Process (DIACAP) Authority to Operate (ATOs) IAW DOD Directive (DODD) 8115.01, Information Technology Portfolio Management. Additionally, when configuration changes are implemented, the contractor shall develop C&A products, in the format specified by the USTRANSCOM C&A team, to obtain an Interim Authority to Operate (IATO) followed by an ATO.

The contractor shall maintain and manage all AV/VTC control systems and audio processor software, system drawings, and other documentation in support of engineering design.

The contractor shall support the integration of the DISA provided collaboration tool, currently Defense Connect Online (DCO), capability into existing AV/VTC systems, provide support for USTRANSCOM-led DISA collaboration tool sessions, and conduct training sessions on the use of the DISA collaboration tool.

1.3.9.5. Task 9 Subtask 5: Communications Security (COMSEC) Responsible Officer (CRO) Duties and Secure Voice Responsible Officer (SVRO)

The contractor shall provide primary CRO and alternate CRO(s) as required to manage COMSEC material necessary for classified AV/VTC communication encryption within the AV/VTC support team. The contractor shall provide primary SVRO and alternate SVRO(s) as required to manage STEs, STU, and material necessary for classified voice communication encryption within the AV/VTC support team.

1.3.9.6 Task 9 Subtask 6: Automated Data Processing Equipment (ADPE) Equipment Custodian (EC), and Functional Area Communications and Computer Systems Manager (FACCSM) Duties

The contractor shall perform primary and alternate EC duties and maintain proper accountability of all Government owned/purchased hardware assigned to the AV/VTC team IAW United States Transportation Command Instruction (USTCI) 33-16 and Air Force Instruction (AFI) 33-112 as well as maintain inventory information for all warranty and maintenance contracts. The contractor shall provide inventory information no later than 31 December and 30 June each period of performance. The contractor shall provide a Functional Area Communications and Computer Systems Manager (FACCSM) duties for USTRANSCOM's Video Teleconferencing function IAW United States Transportation Command Instruction USTCI 33-1 and USTCI 33-16.

1.3.9.7. Task 9 Subtask 7: Briefing and Display Systems Support for the Fusion Center

The contractor shall provide briefing and display systems support for USTRANSCOM's Fusion Center to include the Deployment and Distribution Operations Center (DDOC), Joint Planning Teams (JPT), and Working Groups (WG) 0430 - 1900, Monday through Friday, excluding federal holidays. The contractor shall ensure audiovisual equipment is operational and shall provide initial troubleshooting for malfunctioning equipment. The contractor shall be responsible for the operation and oversight of existing equipment. The contractor shall be responsible for preventive maintenance and repair of audiovisual equipment in accordance with OEM guidelines as well as equipment upgrades, alignments, and convergence. The contractor shall prepare, flip slides, and coordinate computer-generated briefings for the TCJ3 and staff in the Fusion Center to include the DDOC, JPTs, and WGs. The contractor shall coordinate, prepare, and perform short notice updates and slide decks for the USTRANSCOM DDOC, JPT and WG VTCs. The contractor shall update the USTRANSCOM Briefing and Display Home Page with the DDOC, JPT, WG, VTC, Daily Operations Briefs, and other information as required.

1.3.9.8. Task 9 Subtask 8: Augmentation of Briefing and Display Support for the Fusion Center

The contractor shall provide on-site support to augment a Government requirement for 24x7 support when requested by the Government. The contractor, in conjunction with military and Government personnel, shall provide graphics/C4S integration needs for joint operations personnel in the Fusion Center to include the DDOC, JPTs, and WGs in support of current operations, future integration, and contingency operations. The contractor shall provide customer support to the TCCC, TCJ3, TCJ3 staff, and other directorates, as required. The contractor shall prepare, flip slides, and coordinate computer-generated briefings for the TCJ3 and staff in the Fusion Center to include the DDOC, JPTs, and WGs. The contractor shall coordinate, prepare, and perform short notice updates and slide decks for the USTRANSCOM DDOC, JPT and WG VTCs. The contractor shall update the USTRANSCOM Briefing and Display Home Page with the DDOC, JPT, WG, VTC, Daily Operations Briefs, and other information as required.

1.4. DELIVERABLES

All deliverables shall meet professional standards and meet the requirements set forth in contractual documentation. The contractor shall provide all deliverables electronically in Microsoft Office (Word, Excel, PowerPoint, Project, etc.) formats pursuant to the following schedule. The deliverables are not separately priced, but are included in the monthly price.

PWS Para	Deliverable Title	Delivery Schedule
1.3.1.1	Task Order Management Plan	Update – within fifteen (15) business days of the task order start date Final – within five (5) business days of Government comment Option Year Update – within fifteen (15) business days of option year being exercised
1.3.1.2	Monthly Status Reports	No later than the 15th of the following month. Final – no later than the final business day of the final period of performance
1.3.1.3	IPR Presentation Materials	Two (2) business days prior to the IPR
1.3.1.4, 1.3.2.1, 1.3.4.2, 1.3.5.1.1, 1.3.5.1.2, 1.3.7.1, 1.3.7.2, 1.3.7.2.2, 1.3.7.4	Trip Reports	Within five (5) business days after completion of travel
1.3.1.5, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 1.3.8, 1.3.9	Meeting/Conference Minutes	Within two (2) business days after completion of the meeting/conference
1.3.2.1	Helpdesk Performance Metrics Report	Weekly no later than the first business day of each week
1.3.2.2	Service Desk Tool Suite Recommendation	No later than 31 October of the base period
1.3.2.2, 1.3.5.1.1, 1.3.6, 1.3.8, 1.3.9.6	Warranty and Maintenance Contract Inventory Information	No later than 31 December and 30 June each task order year

PWS Para	Deliverable Title	Delivery Schedule
1.3.3	B-3 Table	Initial – within ten (10) business days of task order start Update – within five (5) business days of any change
1.3.4.1	Warranty and Maintenance Contract Inventory Information	No later than 31 December and 30 June each period of performance
1.3.4.1.6	Hardware Requirement Projection	Annually no later than 1 July each period of performance
1.3.4.2.1	USTRANSCOM owned software inventory	No later than the 5th business day of each month
1.3.4.2.1	ES Catalog	Within 40 business days of the task order start date
1.3.4.2.1	Required Software List/Enterprise Software Requirement List	No later than the 5th business day of each month
1.3.4.2.1	Enterprise Software Cost/Benefit Analyses and Recommendations	Within ten (10) business days of Government request
1.3.4.2.1	Cost/Benefit Briefing	Initial – Within eighty (80) business days of the task order start date Annual – No later than 31 March each period of performance
1.3.5	Weekly Activity Report Inputs	Weekly no later than the close of business on Wednesday of each week
1.3.5.2	PED Annual Revalidation Report	Annual – No later than 1 February each period of performance
1.3.6.2	Training Plans	Twenty-five (25) business days after task order start
1.3.6.2	Revised Training Plans	Twenty-five (25) business days after written notice from Government
1.3.6.3	Training Plan	Twenty-five (25) business days after Government request
1.3.6.3	Revised Training Plans	Twenty-five (25) business days after written notice from Government
1.3.6.4	Training Videos and CBT Video Graphic Components	Draft – within forty (40) business days of Government request Final – within ten (10) business days of receipt of Government comments
1.3.7.1	Security Evaluations and Recommendations	IAW suspense assigned by the Government
1.3.7.2	Recurring and Ad-hoc Reports	IAW suspense assigned by the Government
1.3.7.2	Continuity Book	No later than 1 September of the base period of performance
1.3.7.2	Continuity Book Update	No later than 1 September each subsequent period of performance
1.3.7.2	Point Papers and Briefings	IAW suspense assigned by the Government
1.3.7.2	Articles and Info grams	IAW suspense assigned by the Government
1.3.7.3.1	Security Assessments and Formal Recommendations	IAW suspense assigned by the Government

PWS Para	Deliverable Title	Delivery Schedule
1.3.7.3.2	Vulnerability Scan Results	Within three (3) business days of the completion of the scan
1.3.7.3.2	DIACAP Executive Packages	IAW suspense assigned by the Government
1.3.8	Technical Implementation Plans and Schedules	Initial draft within ten (10) business days of project tasking. Final draft within five (5) business days of Government comment
1.3.8	Status Briefs	Monthly or more frequent as requested by the Government
1.3.8.1.2	Status Reports	Every other week
1.3.8.2	Analysis of DOD Publication and Instructions	IAW suspense assigned by the Government
1.3.8.2	Briefs and Information papers	No later than two (2) business days prior to the briefing
1.3.9.1	AV Equipment Operator Level Instructions	Within twenty (20) business days of any changes or upgrades
1.3.9.2	VTC Operator Level Instructions	Within twenty (20) business days of any changes or upgrades
1.3.9.2	VTC Metrics	Monthly no later than the 5th business day of the following month Annually no later than 10th business day of January each period of performance
1.3.9.4	AV/VTC Annual Review/Upgrade Recommendations	No later than 31 March of each period of performance
1.3.9.4	VTC Architecture Graphical Representation	Quarterly no later than the 5th business day of each quarter
1.3.9.4	Annual VTC Hardware and Software Upgrade Recommendations	No later than 31 March of each period of performance

Cyber Security Deliverable Table

PWS Para	Deliverable Title	Delivery Schedule
5.2	Contractor Security Plan	Upon Government Request
5.4	CFE IA Compliance Verification	Monthly (included in the MSR, see paragraph 1.3.1.2)
5.5.1 – 5.5.4 (Optional)	Contractor Cyber Intrusion Incident Report	Initial Report: Within four (4) hours of event Update Report: Within 24 hours of event
5.10 (Optional)	Contractor Development Environment Security Program Documentation	Upon Government Request
5.11 (Optional)	Information System Security Engineering Change Evaluation Documentation	Upon Government Request
5.12 (Optional)	System Security Accreditation Documentation	Upon Government Request
5.13 (Optional)	System Security Engineering Change Control Documentation	Within 30 calendar days of evaluation completion

PWS Para	Deliverable Title	Delivery Schedule
5.16 (Optional)	Source Code	On the day of software release

1.4.1. Packaging, Packing and Shipping Instructions

The contractor shall provide all deliverables and other project related products, reports, etc., as an electronic file e-mail attachment whenever possible. The contractor shall generate all document deliverables in standard office automation software products, i.e. standard Microsoft Office products. If the contractor determines that it would be more beneficial to use non-standard office automation software to generate any of the required deliverables, the contractor must notify and receive approval from the COR prior to generation of those deliverables. In the event deliverables cannot be delivered via e-mail they shall be hand delivered on Compact Disc (CD). Multiple deliverables may be combined on a CD.

2. SERVICE DELIVERY SUMMARY

The Services Delivery Summary (SDS) represents the most important task order objectives that, when met, will ensure task order performance is satisfactory. Although not all PWS requirements are listed in the SDS, the contractor is fully expected to comply with all requirements in the PWS.

PWS Para	Performance Objective	Performance Threshold
1.3.1.2	Monthly Status Reports	98% of the time Monthly Status Report is timely each month and contains appropriate status of the month's activities
1.3.1.3	IPR Presentation Materials	95% of the time IPR Presentation Materials are received two (2) business days prior to the IPR and contain current status, progress, recommendations, and concerns for applicable tasks
1.3.1.4, 1.3.2.1, 1.3.4.2, 1.3.5.1.1, 1.3.5.1.2, 1.3.7.1, 1.3.7.2, 1.3.7.2.2, 1.3.7.4	Trip Reports	97% of the time Trip Reports are received within five (5) business days after completion of travel and contains all details related to the trip and information on the traveler
1.3.1.5, 1.3.3, 1.3.4, 1.3.5, 1.3.7, 1.3.8, 1.3.9	Meeting/Conference Minutes	98% of the time minutes are provided within two (2) business days upon request by the Government and contain all results and impacts of the meeting/conference
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Acknowledgement	95% of the time tickets are acknowledged IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Resolution	95% of the time tickets are resolved IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Assignment	95% of the time tickets are assigned appropriately IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Missed Acknowledgment	95% of the time missed acknowledgements notifications are handled IAW paragraph 2.1

PWS Para	Performance Objective	Performance Threshold
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Proactive Notification	95% of the time proactive notifications are provided IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Missed Resolution	95% of the time missed resolutions are escalated IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Escalation	95% of the time tickets are escalated appropriately IAW paragraph 2.1
1.3.2.1, 1.3.2.2, 1.3.4.1	Ticket Notification	95% of the time the Government is properly notified IAW paragraph 2.1
1.3.3	Life Cycle Support Response Time	95% of the time the contractor is on location to start work within 24 hours from receipt of Government notification
1.3.3	Equipment Restoral Time	95% of the time restoral is within 48 hours after work start
1.3.4.1.1	Create new USTRANSCOM PC image	95% of the time image for new hardware is created within 14 business days after hardware receipt by PC Maintenance Team
1.3.4.1.2	Client workstations installed and made operational	No more than one (1) customer complaint for every 10 installations
1.3.4.1.3	Acknowledge problem receipt	95% of the time technician acknowledges receipt of reported problems from the Helpdesk IAW paragraph 2.1
1.3.4.1.3	Repair USTRANSCOM Client Workstations and Laptops	95% of the time systems are repaired within one (1) business day for on-site customers and (2) business days for off-site customers
1.3.4.1.4	Warranty Claims Processing for USTRANSCOM workstations and laptops	98% of all warranty claims are processed without error
1.3.4.1.4	Warranty Claims Processing for USTRANSCOM workstations and laptops	100% of the time no procurement action is generated to replace a system or component under warranty
1.3.4.1.5	Laptop Loaner Program	No more than one (1) customer service complaint for every ten (10) service requests associated with service point staffing
1.3.4.1.5	Laptop Loaner Program	Nine (9) out of every ten (10) laptops are issued at the PC Maintenance customer service location within one (1) hour from customer walk-in to transaction completion
1.3.4.1.7	Prepare Inoperable or Lifecycle Depleted Computers for Turn-in	100% of all magnetic media of inoperable computers is degaussed IAW manufacturer's instructions
1.3.4.1.7	Prepare Inoperable or Lifecycle Depleted Computers for Turn-in	100% of all magnetic media of lifecycle depleted computers is wiped IAW Government instructions
1.3.4.1.14	On-call Support	TCJ6 Global C4S Coordination Center is able to contact the on-call technician nine (9) of every ten (10) attempts made outside of normal duty hours

PWS Para	Performance Objective	Performance Threshold
1.3.4.2.2	Library record check	Record checks comparing recorded library content to actual content reveal 95% accuracy
1.3.5.1	Response to senior management support requests	98% of the time response is made within 30 minutes of problem notification and problem is corrected within the agreed upon timeframe.
1.3.9.1	Preventative maintenance as prescribed by the equipment manufacturer	98% of the time preventative maintenance is accomplished in accordance with the manufacturer's instructions.
1.3.9.1	AV Operator level instructions	95% of the time instructions are published within 20 business days of any changes or upgrades and are 100% error free
1.3.9.1	On-site AV support for TCCC, TCDC, and TCCS	100% of the time support is provided on-site for TCCC, TCDC, and TCCS attended briefing events.
1.3.9.2	Preventative maintenance as prescribed by the equipment manufacturer	98% of the time preventative maintenance is accomplished in accordance with the manufacturer's instructions.
1.3.9.2	VTC Operator level instructions	95% of the time instructions are published within 20 business days of any changes or upgrades and are 100% error free
1.3.9.2	On-site VTC support for TCCC, TCDC, and TCCS	100% of the time support is provided on-site for TCCC, TCDC, and TCCS attended briefing events.
1.3.9.5	CRO Duties	100% of the time COMSEC materials are properly accounted and controlled in accordance with established policies
1.3.9.6	ADPE EC Duties	100% of the time ADPE is properly accounted and controlled in accordance with established policies

2.1. Requirements for Task 2, Subtask 1, Task 2 Subtask 2, Task 2 Subtask 3, and Task 4 Subtask 1 (1.3.2.1, 1.3.2.2, 1.3.2.3, 1.3.4.1)

Priority	P1	P2	P3	P4
Acknowledgement	10 min.	30 min.	1 hr.	8 hrs.
Resolution	ASAP	4 hrs.	8 hrs.	1 Day (24 hours)
Assignment	15 min. Help Desk, assign to appropriate office lead	15 min. Help Desk, assign to appropriate office lead or analyst	15 min. Help Desk, assign to appropriate office analyst	Help Desk
Missed Acknowledgement	Notify management with hourly updates until acknowledgement received	Reminder call and e-mail at 2 hours	Reminder call and e-mail at 4 hours	Reminder call and e-mail at 12 hours
Proactive Notification	Hourly Updates to Help Desk			Reminder email 8 hours prior to resolution
Missed Resolution	N/A	Auto-escalate to next support level; Metrics Report	Auto-escalate to Lead Metrics Report	Notify Management Metrics Report
Escalation Level	N/A	Escalate to next level of management after missed resolution; 150% of Resolution time (6 hours): Metrics Report	Escalate to Lead after missed resolution; Escalate to Management after 150% of Resolution time (12 hours): Metrics Report	Metrics Report
Notification Level	Email to Help Desk Lead within 30 minutes; IT Managers, IT Directors	Metrics Report	Metrics Report	Metrics Report

Priority	Justification / Description
P1	Multiple users with no workaround
P2	Multiple users with workaround available, single user with no workaround, and/or VIP
P3	Single user with a workaround
P4	Scheduled requests

3. GOVERNMENT WORKSTATIONS AND EQUIPMENT

3.1. The Government will provide an office environment and the following resources to the contractor for performance of this task order.

The Government will provide sufficient workspace at a Government facility for the contractor in support of this requirement. The Government will provide all standard office equipment (telephone, computer, software, base network access, etc.) for official use only during task order performance.

The use of contractor requested Government office space shall be evaluated on an "as needed" basis and USTRANSCOM shall grant approval for use if it does not conflict with mission requirements.

3.2. The Government will provide no Government Furnished Equipment (GFE) at off-site contractor locations for use within the performance of this task order.

4. GENERAL INFORMATION

4.1. Place of Performance

The contractor shall perform services both on-site at Scott AFB, IL and DISA Defense Enterprise Computing Center (DECC) St Louis, MO during normal duty hours, 0730 – 1630, Monday-Friday, excluding Government holidays, and at the contractor's off-site facility. Hours are subject to change due to increased requirements for operations outside the normal workday. 0730 – 1630 are the normal duty hours under this task order unless otherwise specified within the task areas.

4.2. Period of Performance

Period of Performance for the Base Year is 1 October 2011 through 30 September 2012.
Period of Performance for the First Option Year is 1 October 2012 through 30 September 2013.
Period of Performance for the Second Option Year is 1 October 2013 through 30 September 2014.
Period of Performance for the Third Option Year is 1 October 2014 through 30 September 2015.
Period of Performance for the Fourth Option Year is 1 October 2015 through 30 September 2016.

4.3. Travel

Performance under this task order may require contractor travel within and outside the Continental United States. The Government will reimburse the contractor for travel expenses subject to Federal Acquisition Regulation (FAR) and Joint Travel Regulation (JTR). All contractor travel shall be coordinated with and validated by the primary or alternate COR prior to incurring any travel expenses. The contractor shall identify personnel who will be traveling in sufficient time to obtain the lowest possible rates for airfare, rental car and lodging. For long distance travel, a minimum of five (5) business days advance notice from the travel commencement date is required. The travel request shall be in writing and contain the dates, location, and estimated travel costs. Contractor invoices (along with associated receipts) shall support all travel reimbursement requests. The contractor shall report actual travel costs in accordance with paragraph 1.3.1.4.

Task	Number of Trips	Number of Days	Number of People
1.3.2.1	2	5	2
1.3.4.2	3	5	1
1.3.5.1.1	4	5	1
1.3.5.1.2	2	5	1
1.3.7.1	2	5	1
1.3.7.2	10	5	1
1.3.7.2.2	4	5	1
1.3.7.4	2	5	1

4.4. Other Direct Costs (ODCs)

The Government will reimburse materials and fees incurred in the performance of the PWS based on prior coordination with the COR. The contractor shall request authorization from the COR to procure items or services that will be billed under the ODC Contract Line Item Number (CLIN), and shall obtain written authorization from the COR prior to purchasing or incurring any expenses. The Government anticipates costs to be incurred for the acquisition of replacement parts and equipment for life cycle support, mobile phone or pager services for on-call support, acquisition of low-cost unforeseen requirements/assets, and other related expenses. Any mobile phone or pager services paid for by the Government under this task order shall be used exclusively for the performance of this task order. Any additional mobile phone or

pager services must be identified to the Government. Any unforeseen requirements must be coordinated with the Government prior to incurring any expenses.

4.5. Task Order Manager

The contractor shall provide a Task Order Manager who shall be responsible for the performance of the work. The name of the Task Order Manager and alternate(s), who shall act for the contractor when the Task Order Manager is absent, shall be designated in writing to the CO within three (3) business days after task order start. The contractor shall notify the CO in writing to any changes to the Task Order Manager or alternate(s) within three (3) business days after information is known. Task Order Manager responsibilities include, but are not limited to, interfacing with Government management personnel, staffing of all tasks, formulating and enforcing work standards, assigning schedules, reviewing work discrepancies, and communicating policies, purposes, and goals of the organization to subordinates. The contractor shall ensure all personnel assigned to this task order meet the minimum requirements specified in the contractor's proposal, IAW the generic position descriptions provided as part of the contractor's staffing approach. The contractor shall notify the COR in writing of any changes to personnel within three (3) business days after information is known.

4.6. Contractor Furnished Equipment and Services

Except for those items or services specifically stated in paragraph 3, the contractor shall furnish everything needed to perform this task order. For those tasks to be performed off-site at the contractor's facilities, the contractor shall provide all necessary office furnishings and equipment.

4.7. Contractor Employee Qualifications/Certifications

The contractor shall ensure that all personnel employed to perform services under this task order are qualified, trained, certified, and licensed, as deemed necessary by applicable laws and regulations. A file containing the qualifications and certifications of each employee shall be maintained by the contractor and made available to the Government for review, upon request.

4.8. Quality Assurance

The contractor shall support Government agency reviews and audits of all services and support provided under this task order. The contractor shall be prepared to support Quality Assurance reviews conducted by the Government. The Government reserves the right to authorize an independent verification and validation of the contractor's procedures, methods, data, equipment, and other services provided at any time during the performance of this task order.

4.9. Non-Disclosure Agreement (NDA) for Contractor Employees

Due to the sensitive nature of the data and information being worked with on a daily basis, completion of non-disclosure statements will be required by contractor personnel to ensure information that is considered sensitive or proprietary is not compromised. All contractor personnel will be required to sign a NDA. The Government will retain these documents. See Appendix 3, Non-Disclosure Agreement.

4.10. Packaging, Packing and Shipping Instructions

The contractor shall provide all deliverables and other project related products, reports, etc., as an electronic file e-mail attachment whenever possible. The contractor shall generate all document deliverables in standard office automation software products, i.e. standard Microsoft Office products. If the contractor determines that it would be more beneficial to use non-standard office automation software to generate any of the required deliverables, the contractor must notify and receive approval from the COR prior to generation of those deliverables. In the event deliverables cannot be delivered via e-mail they shall be hand delivered on Compact Disc (CD). Multiple deliverables may be combined on a CD.

5. SECURITY

5.1. Handling of Non-Public Information

In performance of this task order, the contractor may have access to sensitive, non-public information. The contractor agrees to: (a) Use and protect such information from unauthorized disclosure in accordance with DTM 08-027 - Security of Unclassified DOD Information on Non-DOD Information Systems, 31 July 2009; (b) Use and disclose such information only for the purpose of performing this task order and to not use or disclose such information for any personal or commercial purpose; (c) Obtain permission of the CO and/or COR before disclosing/discussing such information with a third party; (d) Return and/or electronically purge, upon Government request, any non-public, sensitive information no longer required for contractor performance; and (e) Advise the CO and/or COR of any unauthorized release of such information.

5.2. Requirements for Contractor Provision of Security Plan, Information Assurance Controls

The contractor shall establish an Information Assurance Program to implement and sustain appropriate Information Assurance management, operational, and technical controls and processes required to safeguard DOD non-public information resident on or transiting the contractor's unclassified information systems from unauthorized access and disclosure. Protection measures applied must be commensurate with the risks (i.e. consequences and their probability) of loss, misuse, unauthorized access, or modification of information. The contractor shall submit for Government approval an overarching security plan that describes their strategy for implementation of Information Assurance and Industrial Security requirements throughout the life of the task order. The security plan shall address the security controls described in National Institute of Standards & Technology (NIST) Special Publication 800-53 (current version), Recommended Security Controls for Federal Information Systems and Organizations (http://csrc.mist.gov/publications/PubsSPs.html), and should be tailored in scope and depth appropriate to the effort and the specific unclassified DOD information.

5.3. Periodic Government Inspections

The contractor shall authorize Government inspections and reviews to assure compliance with DOD Information Assurance requirements throughout the task order performance period. The contractor shall be responsible for taking corrective action based upon the impact and severity of identified weaknesses.

5.4. Remote Access (Optional)

Contractor Furnished Equipment (CFE) employed for remote access to a Government network must meet equivalent GFE Information Assurance computing requirements. The contractor shall ensure that all CFE (hardware and software) employed to access these environments meet the following minimum

Government Information Assurance requirements and provide periodic certification of compliance as a pre-requisite to being granted network access.

(a) Use of personal systems is prohibited
(b) Operating systems and applications must be configured for compliance with the Defense Information Systems Agency (DISA) Gold Disk and applicable Security Technical Implementation Guides (STIGs)
(c) DOD approved anti-virus and anti-spyware software must be installed and signatures must be configured to automatically update on a daily basis
(d) DOD approved personal firewall must be utilized and configured to permit traffic by exception only, dropping all other traffic. If the personal firewall provides intrusion detection or prevention; the signatures or rules must be updated at the same intervals as the anti-virus software
(e) Computers must be Information Assurance Vulnerability Management (IAVM) compliant
(f) Computers must be scanned with the DOD version of E-eye Retina vulnerability scanner (or current approved DOD scanner solution) at a minimum of every 30 calendar days. All vulnerabilities must be remediated and reported to the cognizant Information Assurance Manager
(g) Contractor employees must possess a current Government issued Common Access Card (CAC) and install Government certified CAC readers; and
(h) Verification of compliance with these requirements must be provided to COR on a monthly basis. The contractor shall include the verification of compliance in the MSR.

5.5 Detect, Analyze, Respond (Optional)

5.5.1. Reporting Requirements

The contractor shall report to the USTRANSCOM Technical Information Analysis Center (TIAC) and USTRANSCOM designated Government personnel within 4 hours of discovery of any suspected cyber intrusion events that affect DOD information resident on or transiting the contractor's unclassified information systems. Initial report shall be provided even if some details are not yet available, with follow-on detailed reporting within 24 hours. Reportable cyber intrusion events include the following: (a) A cyber intrusion event appearing to be an advanced persistent threat; (b) A cyber intrusion event involving data exfiltration or manipulation or other loss of any DOD information resident on or transiting the contractor's, or its subcontractors', unclassified information systems; (c) Intrusion activities that allow unauthorized access to an unclassified information system on which DOD information is resident or transiting.

Definition of advanced persistent threat: An extremely proficient, patient, determined, and capable adversary, including two or more of such adversaries working together.

5.5.2. Incident Report Content

The incident report shall include, at a minimum, the following information: (a) Applicable dates (date of suspected compromise and date of discovery); (b) Threat methodology (all known resources used such as Internet Protocol (IP) addresses, domain names, copies malware, etc.); (c) An account of what actions the threat(s) may have taken on the victim system/network and what information may have been accessed; (d) A description of the roles and functions of the threat-accessed system; (e) An initial list of potentially impacted Government programs and each program's classification; (f) What information may have been

exfiltrated that may impact Government programs; (g) A list of all employees and subcontracted employees who work or have worked with the victim system/network; (h) A point of contact to coordinate damage assessment activities.

5.5.3. Incident Report Submission

The contractor will submit unclassified network cyber incident reports to the USTRANSCOM TIAC and USTRANSCOM designated Government personnel via encrypted email or another mutually agreed upon secure communications method. Copies of malware require special handling and pre-coordination must be accomplished prior to submission.

5.5.4. Incident Report Coordination

In the event of a known or potential intrusion, the contractor agrees to allow follow-on actions by the Government to further characterize and evaluate the suspect activity. The contractor acknowledges that damage assessments may be necessary to ascertain intruder methodology and identify systems compromised as a result of the intrusion. The contractor acknowledges that in certain cases a complete forensic analysis may be necessary to ascertain intruder methodology and identify systems compromised as a result of the intrusion. Once an intrusion is identified, the company 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 intrusion for subsequent forensic analysis so that an accurate and complete damage assessment can be accomplished by the Government. The contractor is not required to maintain an organic forensic capability, but must ensure data is preserved until forensic analysis can be performed by the Government (e.g. removing an affected system, while still powered on, from the network meets the intent of this requirement). Any follow-on actions will be coordinated with the contractor via the COR.

5.6. Law Enforcement / Counterintelligence (Optional)

In the event of a known or potential intrusion, the contractor shall consent to responding counterintelligence or law enforcement investigative agency requests to apply forensic analysis tools to contractor information systems affected by the intrusion, including monitoring tools, imaging tools, and any other techniques that the agency seeks to apply to effectively analyze the intrusion. The contractor shall allow the responding counterintelligence and/or law enforcement investigative agency to image affected systems, including systems containing proprietary information. Nothing in this task order shall limit the ability to conduct law enforcement or counterintelligence activities, or other activities in the interest of the Government.

5.7. Information Sharing (Optional)

The Government may use and disclose reported information (e.g., information regarding threats, vulnerabilities, incidents, or best practices) that does not include attribution information at its discretion to assist entities in protecting information or information systems (e.g. threat information products, threat assessment reports); provided that such use or disclosure is otherwise authorized in accordance with applicable statutes, regulations, and policies.

5.8. Confidentiality and Non-Attribution Statement (Optional)

The Government shall take reasonable steps, by controlled access and need-to-know procedures, to protect against public release of attribution information of the contractor. The Government may use and disclose reported information that includes attribution information only on a need-to-know basis to authorized persons for cyber security and related purposes (e.g., in support of forensic analysis, incident response, compromise or damage assessments, law enforcement, counter intelligence, threat reporting, trend analysis). The Government may disclose attribution information to support contractors that are supporting the Government's cyber security and related activities if the support contractor is subject to legal confidentiality requirements that prevent any further use or disclosure of the attribution information. The Government agrees to consider available exemptions of the Freedom of Information Act to protect against disclosure of attribution information of the contractor to unauthorized persons. Within a reasonable period necessary to perform an analysis after completion of the assessment, all contractor proprietary information or third party proprietary information in the possession of the Government as a result of the assessment will be destroyed unless other disposition is agreed upon in writing by the Parties or is required by law, Executive Order or regulation.

5.9. Information Assurance Workforce Improvement Program (IAWIP)

DOD 8570.01-M, IAWIP, requires contractor personnel performing IA functions, on either a full or part-time basis, to receive a commercial certification. Appendix 5 Information Assurance Contractor Training and Certification describes which functions require a particular level of certification. Contractor personnel assigned to those functions must achieve the appropriate certification as specified in DOD 8570.01-M, IAWIP, prior to task order award.

Personnel in IA positions must sign a "Statement of Acceptance and Responsibilities." Additionally, contractor personnel performing IA functions must take appropriate actions to complete continuing education and re-certification requirements applicable to their certification. The contractor shall have their personnel properly certified at all times after task order start, unless a waiver has been granted.

Contractor personnel holding an IA certification must release their certification information to the DOD by registering their certification in the Defense Workforce Certification Application (DWCA): https://www.dmdc.osd.mil/appl/dwc/index.jsp

The contractor shall complete an on-the-job skills practical evaluation for their personnel in Information Assurance Technical (IAT) positions and provide supporting documentation indicating completion to the CO or designee. After completion of the evaluation and verification of certification, personnel will be issued an appointment letter for the performance of IA duties including a statement of responsibilities.

In addition to the baseline IA certification requirement for their level, the contractor shall ensure that personnel in IAT positions with privileged access possess the appropriate Computing Environment (CE) certification for the operating system or security related tools/devices they support, and provide supporting documentation indicating possession of the CE certification to the CO or designee.

5.10. Developer Environment, Mission Assurance Category (MAC) and Confidentiality Level (Optional)

The contractor development environment shall be physically and logically isolated from other networks, to include its enterprise unclassified network. Security guidelines for the environment must be documented and the security program implemented shall address the security controls described in NIST Special Publication 800-53 (current version), Recommended Security Controls for Federal Information

Systems and Organizations (http://csrc.mist.gov/publications/PubsSPs.html). The contractor shall provide the security program documentation upon request by the Government.

5.11. System Design, Information System Security Engineering Principles (Optional)

The contractor shall ensure that information system security engineering is employed during any/all changes to the system architecture. Such modifications shall be made in compliance with all analogous or interfacing Information Assurance component(s) of the Global Information Grid (GIG) Architecture and shall be designed to make maximum use of the DOD enterprise Information Assurance capabilities and services. As part of the contractor's change control process, the contractor shall ensure participation by an Information System Security Engineer or a qualified Information Assurance representative in the evaluation of the impact of each change on security. The contractor shall document the results of this evaluation and provide the evaluation documentation upon request by the Government.

5.12. DOD Information Assurance Certification & Accreditation Process Requirements (Optional)

The contractor shall be responsible for the development of system security documentation to facilitate the security accreditation of the system according to DODI 8510.01 DIACAP and the associated Mission Assurance Category (MAC) and Confidentiality Level (CL) as defined in DOD Instruction 8500.2, Information Assurance (IA) Implementation (current version). The contractor shall update the DOD Enterprise Mission Assurance Support Service (eMASS) system as required and provide supporting IA documentation for upload as artifacts in eMASS.

5.13. Software Assurance and Security Engineering Practices (Optional)

In coordination with the Government, the contractor shall design, develop and implement secure applications and configurations through applying applicable DOD Security Technical Implementation Guides (STIGs), checklists, vendor security guidance, industry best practices, and applicable vendor product security patches. The contractor shall ensure applications are in compliance with DOD Instruction 8500.2 Information Assurance Implementation (current version) and DODI 8551.1 Ports, Protocols, and Services Management (PPSM) (current version). The contractor shall leverage, to the maximum extent possible, automated tools to identify and remediate vulnerabilities or weaknesses in the application design/coding, such as those described in Common Weakness Enumeration/System Administration, Networking, and Security Institute (CWE/SANS) TOP 25 Most Dangerous Programming Errors and Open Web Application Security Project (OWASP) Top Ten, that could be exploited by unauthorized sources.

The Information System Security Engineer shall participate in Government and contractor formal and informal design reviews to identify potential security weaknesses, deficiencies, and/or vulnerabilities in the design. The Information System Security Engineer shall also ensure appropriate security requirements are included as part of the requirements traceability matrix and are evaluated as part of the security test and evaluation (ST&E). As part of the contractor's change control process, the contractor shall ensure participation by the Information System Security Engineer or a qualified Information Assurance representative to evaluate the impact of each change on security. The contractor shall document the results of this evaluation and provide the results within 30 calendar days of completion of the evaluation.

5.14 Non-Secure Software (Optional)

If the Government determines, after a security audit (e.g. ST&E), that software delivered under this task order is non-secure, the Government will provide written notice to the contractor of each non-conformity. Software shall be "non-secure" under this task order if it contains a programming error listed on the current approved version of the CWE/SANS TOP 25 (which can be located at http://www.sans.org/top25-programming-errors) or a web application security flaw listed on the current approved version of the OWASP Top Ten (which can be located at http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project). Such notice constitutes revocation of acceptance of any delivered software.

The contractor shall have 30 calendar days after receipt of such notice (Remedy Period) to remedy each non-conformity by modifying/replacing and redelivering the software to the Government. If the Government determines, after a security audit following a Remedy Period, that the redelivered software is non-secure, and thus non-conforming, the Government may reject the delivery, provide notice of the non-conformance, and document the contractor's performance record. Alternatively, the Government may accept non-conforming software, receive appropriate consideration (equitable price reduction on a fixed price contract, reimbursement for costs of security audit, reimbursement for costs to correct the non-compliances, etc.), and document the contractor's performance record

5.15. Malicious Code Warranty (Optional)

The contractor represents and warrants that the software shall be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information.

5.16. Source Code Configuration Control (Versioning) (Optional)

The contractor shall utilize a strict version control process for software development and provide two copies of source code, on the day the software is released, for all software versions developed under this task order. The source code shall be provided on optical removable media (burned for read only) or another mutually agreed type of media.

5.17. RESERVED

5.18. Security: (Physical, Personnel, Information, Antiterrorism/Force Protection and Industrial)

5.18.1. 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 restricted (classified areas and systems) located at various locations listed in paragraph 4.1, Place of Performance, of the PWS, which require SECRET eligibility/access.

Furthermore, contractor personnel with access to Information Assurance (IA) administrative privileges and/or who will monitor DOD Information Technology (IT) systems or software as designated by DOD 8500.1/5200.2-R may be rated at the various levels listed in paragraph 5.18.2. below. The stipulation of the numbers and what IT/Automated Data Processing (ADP) levels the contractors will have is approved by the COR or the CO before the start of the task order. The contractor shall not divulge any financial, planning, programming, or budgeting information without the express consent of the Government as outlined in Operational Security (OPSEC) and Information Security regulations or be held liable for

punitive damages incurred as a result of release of such information. The contractor shall comply with all appropriate provisions of applicable security regulations while assigned to this task order for DOD and USTRANSCOM.

Specific security requirements are identified in the DD Form 254, DOD Contract Security Classification Specification. A completed/signed DD Form 254 is attached to the task order.

5.18.2. Personnel Security Requirements

The contractor's, subcontractors, and/or partner's personnel performing services under this task order, shall be citizens of the United States of America. Dual citizens will not be authorized interim or final security clearance determinations. US Citizens who currently have (either expired or active) foreign passports will not be able to obtain or hold interim or final security clearance determination within DOD. These contractors who maintain or have in their possession a valid or expired foreign passport are considered dual-citizens and will not be authorized classified material or access. The contractor, subcontractor(s), and/or partner(s) shall possess the capability to articulate well, speak and write fluently in the English Language, and comprehend the English Language. Overall, all contractor personnel shall possess the appropriate personnel security investigation for the position(s) occupied. Contractor personnel shall be required to have a background investigation that corresponds with the sensitivity level of the tasks to be performed.

The following guidance will be followed when determining background investigation and clearance levels for this task order depending on requirements:

POSITION LEVEL:
Information Technology (IT)-I
Automated Data Processing (ADP)-I
or Critical Sensitive Positions (TOP SECRET):
IT/ADP-I and Critical Sensitive Positions are those positions that: require access to Top Secret information; development or approval of plans, policies, or programs that affect the overall operations of the DOD or of a DOD component; development or approval or war plans, plans or particulars of future major or special operations of war, or critical and extremely important items of war; investigative and certain investigative support duties, the issuance of personnel security clearances or access authorizations, or the making of personnel security determinations; fiduciary, public contact, or other duties demanding the highest degree of public trust; duties falling under Special Access programs; directly responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain; and any other position so designated by the head of the component or designee.

BACKGROUND INVESTIGATION REQUIREMENTS:
(IT-I/ADP-I or Critical Sensitive) Requirements for TOP SECRET:
Positions designated by the Government as Critical Sensitive/ADP-I/IT-I rating require a Single Scope Background Investigation (SSBI) (or acceptable periodic reinvestigation) favorably adjudicated (a favorable adjudication grants eligibility at the TOP SECRET level as prescribed by DOD 5200.2-R). The IT-I/ADP-I requirements mandate the contractor have a minimum Facilities Clearance Level (FCL) at the TOP SECRET level due to investigation submissions as directed in DOD 5220.22-M, DOD 5200.1-R and the Joint Personnel Adjudications System (JPAS).

POSITION LEVEL:
Information Technology (IT)-II
Automated Data Processing (ADP)-II
Or Non-Critical Sensitive Positions (SECRET):
IT/ADP-II and Non-Critical Sensitive Positions are those positions that: have access to Secret or Confidential information; Security police/provost marshal-type duties involving the enforcement of law and security duties involving the protection and safeguarding of DOD personnel and property; category II automated data processing positions; duties involving education and orientation of DOD personnel; duties involving the design, operation, or maintenance of intrusion detection systems deployed to safeguard DOD personnel and property; responsible for the direction, planning, design, operation, or maintenance of a computer system, and whose work is technically reviewed by a higher authority of the ADP-I category to ensure the integrity of the system; and any other position so designated by the head of the Component or designee.

BACKGROUND INVESTIGATION REQUIREMENTS:
(IT-II/ADP-II/Non-Critical Sensitive) Requirements for SECRET:
Positions designated by the Government at the Non-Critical Sensitive/ADP-II/IT-II rating require a National Agency Check with Local Credit (NACLC) (or acceptable periodic reinvestigation) favorably adjudicated (a favorable adjudication grants eligibility at the SECRET level as prescribed by DOD 5200.2-R). The IT-II/ADP-II requirement mandates the contractor have a minimum FCL at the SECRET (or higher) level due to investigation submissions as directed in DOD 5220.22-M, DOD 5200.1-R and JPAS.

POSITION LEVEL:
Information Technology (IT)-III
Automated Data Processing (ADP)-III
Or Non-Sensitive Positions (Position of Trust Determination) (No Classified Access)
All other positions involved in computer activities and Common Access Card. No clearance is granted for classified access and only a Position of Trust (PoT) is awarded and posted in JPAS.

BACKGROUND INVESTIGATION REQUIREMENTS:
(IT-III/ADP-III/Non-Sensitive) Requirements for Position of Trust Determinations (No Classified Access):
Positions designated by the Government at the Non-Sensitive/ADP-III/IT-III rating require a National Agency Check with Inquiries (NACI) (or acceptable investigation/reinvestigation) favorably adjudicated (a favorable adjudication issues a Position of Trust determination as prescribed by DOD 5200.2-R and DOD DTM 08-003 (Dated Dec 08). Favorable NACI or equivalent investigation results must be posted in JPAS before a Common Access Card (CAC) or Non-classified Internet Protocol Router Network (NIPRNET) access will be granted. To obtain interim CAC/NIPRNET access, NACI investigations will be opened with fingerprint, name and criminal records checks returned favorably before the credentials (CAC and NIPRNET) are issued. NACI submissions will be completed on the Standard Form (SF) 85P and submitted with fingerprint cards (FP 258) to USTRANSCOM Force Protection, Security Services Center (SSC) for processing. No classified access will be granted based on the NACI investigation.

NOTE: The above requirements for IT-III/ADP-III/Non-Sensitive Positions are for access to unclassified systems only. Contractors who require access to classified systems or areas must have interim or final adjudication of background investigations at the Critical or Non-Critical Sensitive levels.

USTRANSCOM will only process National Agency Check with Inquiries (NACI)/Position of Trust investigations and will not complete any personnel security investigations for classified access. It is incumbent upon the contractor to have the appropriate investigations completed upon start of the task order. Personnel who do not have the proper investigation will be denied the ability and access to USTRANSCOM facilities until investigations have been favorably adjudicated.

5.18.3. Security Clearance and Special Access Requirements

All positions on this contract require a minimum of a SECRET clearance. In addition some positions on this contract require access to Sensitive Compartmented Information (SCI). Tasks that require collateral TOP SECRET and TOP SECRET/SCI security clearances or TOP SECRET/SCI special access are outlined in the table below. SCI will not be released to contractor employees without specific release approval of the originator.

Task	Task Area	TOP SECRET	SCI
7.1	Engineering Support		X
7.2	COMSEC		X
7.3 (Para 1.3.7.3.1)	Certification & Accreditation Verification and Configuration / Vulnerability Management	X	

5.18.4. Facilities Clearance Level (FCL)

The contractor must have a valid FCL at the SECRET level (or higher). Interim FCLs are acceptable provided they are not expired. FCL procedures and security guidelines for adjudicative requirements are outlined in DOD 5220.22-M and DOD 5200.2-R. FCLs and Interim FCLs must be awarded by the Defense Security Service (DSS) or Defense Industrial Security Clearance Office (DISCO).

5.18.5. Personnel and Facilities Clearance Validation

Upon task order award, the contactor shall submit the names of contractor personnel to USTRANSCOM Security Services Center (SSC) for vetting through JPAS to ensure investigative and clearance requirements have been satisfied. This will be completed before the COR/Trusted Agent (TA) accesses the DOD Contract Verification System (CVS) and submits a request for issuance of the Common Access Card (CAC) to the contractor's personnel. If a contractor's employee does not have the required investigative or security clearance level based on the Government's determination, the contractor's employee will be denied the ability to work in support of this task order and the employee's information will not be loaded into CVS.

5.18.6. Common Access Card Issuance Procedures

Upon notification by the SSC that contractor personnel meet the required investigative and clearance levels, the personnel will be loaded in CVS for an expiration on their CAC for the base year, plus two option years, for a three year total, if the contractor is fully funded. If the contract is unfunded or funded on a yearly basis requiring recertification of funding by USTRANSCOM Acquisition Directorate (TCAQ) and USTRANSCOM Program Analysis and Financial Management Directorate (TCJ8), CACs will only be approved for the current period of performance. Once approved in CVS, the contractor employees may go to the nearest RAPIDS/DEERS office for CAC issuance.

5.18.7. Scott Air Force Base/USTRANSCOM Physical Access

Upon receipt of the CAC, permanently assigned contractor personnel located at USTRANSCOM at Scott AFB (SAFB), IL, may obtain the AF 1199 (Restricted Area Badge) if the employee meets the requirements set forth in the SAFB Instruction 31-101. This stipulates that personnel who request AF 1199's be assigned physically on SAFB at least four (4) days a week with a desk computer and phone before a AF 1199 will be issued.

The Government will provide unrestricted access to facilities, consistent with security clearance and need to know, necessary for the on-site personnel to perform their work in accordance with the task order. Contractor personnel assigned on-site at USTRANSCOM will wear the black contractor lanyard (provided by the Government at no cost) and display the Restricted Area badge at all times while in Government facilities. Visits to SAFB by contractor personnel who do not possess the CAC will be facilitated by the COR/CO sponsoring the employee through the online base access system.

5.18.8. Visits to USTRANSCOM/SDDC Building

General Visits: Any visit(s) by contractor personnel not permanently assigned to this task order (i.e., company presidents, company security managers, contractor personnel not permanently assigned at SAFB, etc.) require an electronic visit request be submitted using JPAS. JPAS visits can be forwarded to the Security Management Office (SMO) code: USTC -SDDC. The visit request shall annotate the task order number in the POC block of the visit request and the name/phone number of either the functional, COR or CO in the phone number block.

Permanently Assigned Contractors: Permanently assigned contractor employees on SAFB will require a visit request for the current period of performance posted in JPAS to SMO: USTC- SDDC. The visit request will annotate the contract number in the POC block of the visit request and the name/phone number of either the functional, COR or CO in the phone number block. Upon in-processing permanently assigned contractors will require a copy of the DD254 for this task order to show the classified access level for this task order and to assist in assigning permissions on restricted area badges.

5.18.9. Security Training

Contractor personnel physically assigned at USTRANSCOM/SDDC at SAFB shall attend/complete the following training as prescribed by DOD, USTRANSCOM and Air Force Instructions: Employee Initial Security Briefing, Annual Security Awareness Training, OPSEC, DOD Antiterrorism Level I training and any Security Stand Down Day Training scheduled by the Commander, USTRANSCOM. Contractor personnel assigned elsewhere shall attend security training established by their respective Government security offices and/or installations.

5.18.10. Additional Security Conditions

All contractors assigned to USTRANSCOM/SDDC on SAFB will complete the contactor in-processing checklist before the start of work on this or any contract/task order in USTRANSCOM. Contractor personnel shall complete the out-processing checklist on the last day of the task order or upon termination or reassignment from duties under this task order.

Upon completion of this task order, the contractor's personnel shall surrender all Government supplies, materials and equipment to the COR. All contractor personnel assigned to this task order who possess

CAC cards shall return those cards to the SSC when completing out-processing. No CAC's or AF 1199 (Restricted Area badges) will be turned into the contractor's company.

Contractor personnel physically working at USTRANSCOM at SAFB, IL, shall complete a security debriefing statement (SF 312) upon completion of the task order.

5.18.11. The Government shall ensure the roles/privileges assigned to contractor personnel on the Government computing platforms are limited to the roles/privileges essential to that individual's performance of his/her assignments. The Government may limit or revoke these roles or privileges for any reason.

5.18.12. Derogatory Information

If the Government 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 the worksite. This includes security deviations/incidents and credible derogatory information on contractor personnel during the course of the task order's period of performance as noted in JPAS. Personnel who have incident reports posted in JPAS will be denied the ability to support the task order until the issues have been resolved and the incident has been removed in JPAS. The contractor shall make any changes necessary in the appointment(s).

Security Regulation Guidance:
Department of Defense (DOD):
2000.16 (DOD Antiterrorism (AT) Standards)
5200.1-R (DOD Information Security Program)
5200.2-R (DOD Personnel Security Program)
5200.08-R (DOD Physical Security Program)
5220.22-M (National Industrial Security Program)
8500.1 (Information Assurance (IA))
2000.12 (DOD Antiterrorism (AT) Program)
8500.2 (Information Assurance (IA) Implementation)
DOD regulations found at: http://www.dtic.mil/whs/directives/corres/pub1.html

Scott Air Force Base:
SAFB Instruction 31-101 (Installation Security Instruction)
(Restricted publication. Sent only to .mil domains when forwarding. Not for public distribution.)

Forms:
DD 254, DOD, Contract Security Classification Specification

DOD forms found at:
http://www.dtic.mil/whs/directives/corres/pub1.html

USTRANSCOM Force Protection (Industrial Security) Points of Contact:
Patrick Collins or Steven Strait
508 Scott Drive
Security Services Center (SSC)
Scott AFB IL 62225

Commercial: 618-220-6551/229-8287 (respectively)
Email at Patrick.Collins@ustranscom.mil or Steven.Strait@ustranscom.mil
USTCJ3-FP Approval: Steve Strait
USTCJ3- FP Tracking #: USTRANSCOM-FP-00005-11

6. CONTRACTOR TRANSITION

6.1. Exit Requirements.

If this task order is terminated for any reason by the Government or if an option year is not exercised, the contractor may at the discretion of the Government be given up to a sixty (60) calendar day transition period. The contractor shall organize all work related documents and files, store them on the designated Government collaboration tool and provide a file plan outlining the file structure. Status for each project will be documented, to include recent, current, and pending actions. The contractor shall provide all-inclusive inventories, a listing of all Commercial Off The Shelf (COTS) utilized in support of this task order, accountability of licenses, and soft copies of all procedures and training materials developed as part of this task order. In addition, the contractor shall provide a complete list of all badges, vehicle passes, and Government software access permissions by individual currently working on the task order. The contractor must ensure no logistics or task order data is corrupted, changed, or altered in a manner that would cause damage to the Government. The contractor shall meet performance requirements and cooperate with the successor contractor in the transition period.

During the transition period, the incumbent contractor shall provide the assistance and support required to ensure the orderly transition of all logistics support, and provide transitional planning necessary to enable the follow-on contractor to commence uninterrupted operations at the end of the transition period. The contractor shall ensure follow-on contractor personnel are permitted access to observe all operations, including work flow, priorities, scheduling, equipment handling/processing, parts storage, safety, and security. Familiarization visits shall not interfere with the activities of the incumbent contractor or Government personnel.

APPENDICES:

1. **ACRONYMS**
2. **APPLICABLE DOCUMENTS**
3. **NON-DISCLOSURE AGREEMENT**
4. **ESTIMATED WORKLOAD**
5. **INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION**
6. **OPERATING SYSTEMS/SOFTWARE/APPLICATIONS SUPPORTED**
7. **PROTOCOLS IN USE**

Appendix 1

ACRONYMS

Acronym	Definition
AAR	After Action Review
ADP	Automated Data Processing
ADPE	Automated Data Processing Equipment
AF	Air Force
AFB	Air Force Base
AFI	Air Force Instruction
AFNIC	Air Force Network Integration Center
AISSP	Automated Information Systems Security Program
AMC	Air Mobility Command
AMHS	Automated Message Handling System
APL	Approved Products List
ATO	Authority To Operate
AV	Audio Visual
AV/VTC	Audiovisual/Video Teleconferencing
C2	Command and Control
C4	Command, Control, Communications, and Computer
C4S	Command, Control, Communications, and Computer Systems
C&A	Certification & Accreditation
CAC	Common Access Card
CAT	Crisis Action Team
CCE	Common Computing Environment
CCEA	Cryptographic COMSEC Equipment Account
CCI	Controlled Cryptographic Items
CD	Compact Disc
CDE	Common Development Environment
CERP	Capital Equipment Replacement Program
CERT	Computer Emergency Response Team
CFE	Contractor Furnished Equipment
CFR	Code of Federal Regulations
CGP	Corporate Governance Process
CIL	Critical Information List
CIO	Chief Information Officer
CIPS	Cyberspace Infrastructure Planning System
CJCSI	Chairman Joint Chiefs of Staff Instruction
CL	Confidentiality Level
CMCS	COMSEC Material Control System
COA	Course of Action
COMSEC	Communications Security
CO	Contracting Officer
COIS	Classified Office Information System
COMSEC	Communications Security

CONPLAN	Contingency Plan
COR	Contracting Officer Representative
COTS	Commercial Off The Shelf
CPM	COMSEC Policy Message
CPSG	Cryptologic Systems Group
CRO	COMSEC Responsible Officer
CST	Computer Support Technician
CVS	Contract Verification System
CWE/SANS	Common Weakness Enumeration/System Administration, Networking, and Security Institute
DCO	Defense Connect Online
DDOC	Deployment Distribution Operations Center
DECC	Defense Enterprise Computing Center
DHCP	Dynamic Host Configuration Protocol
DIACAP	Department of Defense (DOD) Information Assurance Certification and Accreditation Process
DISA	Defense Information Systems Agency
DISCO	Defense Industrial Security Clearance Office
DISN	Defense Information System Network
DIT	Directory Information Tree
DITCO	Defense Information Technology Contracting Office
DMS	Defense Message System
DNS	Domain Name Service
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DPO	Distribution Process Owner
DRRS	Defense Readiness Reporting System
DRSN	Defense Red Switch Network
DSE	DPO Secure Enclave
DSS	Defense Security Service
DVS	DISN Video Services
EC	Equipment Custodian
EKMS	Electronic Key Management System
eMASS	Enterprise Mission Assurance Support Service
ES	Enterprise Software
ESI	Electronically Stored Information
ETA	Education, Training, and Awareness
FACCSM	Functional Area Communications and Computer Systems Manager
FAR	Federal Acquisition Regulation
FCL	Facilities Clearance Level
FISMA	Federal Information Security Management Act
GFE	Government Furnished Equipment
GIG	Global Information Grid
GIS	Geographic Information System
HP	Hewlett-Packard
IA	Information Assurance

IA/IP	Information Assurance and Information Protection
IATO	Interim Authority to Operate
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IAWIP	Information Assurance Workforce Improvement Program
ICP	Inter-theater COMSEC Package
IOPC	Information Operations Planning Cell
IP	Information Protection
IPR	In-Process Review
IPTV	Internet Protocol Television
IT	Information Technology
ITS	Information Tool Suite
JALIS	Joint Air Logistics Information System
JCMA	Joint COMSEC Monitoring Activity
JCS	Joint Chiefs of Staff
JDDA	Joint Deployment and Distribution Architecture
JDDE	Joint Deployment and Distribution Enterprise
JFAST	Joint Flow Analysis System for Transportation
JOPES	Joint Operations Planning and Execution System
JPAS	Joint Personnel Adjudications System
JTEN	Joint Training and Experimentation Network
JTIMS	Joint Training Information Management System
JTR	Joint Travel Regulation
JUCC	Joint Unified Combatant Commands
JWICS	Joint Worldwide Intelligence Communications System
KP	Key Processor
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMD	Local Management Device
LNO	Liaison Officer
MAC	Media Access Control
MAC	Mission Assurance Category
MAN	Metropolitan Area Network
MSC	Military Sealift Command
MSR	Monthly Status Report
NACI	National Agency Check with Inquiries
NACLC	National Agency Check with Local Credit
NDA	Non-Disclosure Agreement
NIPRNET	Non-secure Internet Protocol Router Network
NIST	National Institute of Standards & Technology
NSA	National Security Agency
OCONUS	Outside Contiguous United States
OEM	Original Equipment Manufacturer
OPLAN	Operations Plan
OPR	Office of Primary Responsibility
OPSEC	Operational Security
OS	Operating System

OWASP	Open Web Application Security Project
PB	Presidents Budget
PBX	Private Branch Exchange
PC	Personal Computer
PCM	Portal Content Manager
PD	Policy Directive
PDS	Practices Dangerous to Security
PDS	Protected Distribution System
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point of Contact
POLAD	Political Advisor
POM	Program Obligation Memorandum
PoT	Position of Trust
PPM	Principal Period of Maintenance
PPSM	Ports, Protocols, and Services Management
PWS	Performance Work Statement
SAFB	Scott Air Force Base
SBSS	Standard Base Supply System
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SDDC	Surface Deployment and Distribution Command
SF	Standard Form
SIPRNET	Secret Internet Protocol Router Network
SMO	Security Management Office
SMS	Single Mobility System
SOA	Service Oriented Architecture
SQL	Structured Query Language
SSC	Security Services Center
SSBI	Single Scope Background Investigation
SSR	Special Security Representative
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guides
TA	Trusted Agent
TCAQ	USTRANSCOM Acquisition Directorate
TCC	Transportation Component Command
TCCC	USTRANSCOM Commander
TCCS	USTRANSCOM Chief of Staff
TCCS-IM	USTRANSCOM Chief of Staff Information Management
TCDC	USTRANSCOM Deputy Commander
TCJ3	USTRANSCOM Operations and Plans Directorate
TCJ6	USTRANSCOM Command, Control, Communications and Computer Systems Directorate
TCJ8	USTRANSCOM Program Analysis and Financial Management Directorate
TCO	Telephone Control Officer
TDY	Temporary Duty
TIAC	Technical Information Analysis Center

TMART	Transaction Management Application Response Timer
TMS	Telecommunications Management System
TMT	Task Management Tool
TOMP	Task Order Management Plan
TPI	Two Person Integrity
TRAC2ES	TRANSCOM Regulating and Command & Control Evacuation System
TransViz	Transportation Visualization
TRIM	Total Records and Information Management
TSR	Telephone Service Requests
UDDI	Universal Description, Discovery and Integration
UOIS	Unclassified Office Information System
USAF	United States Air Force
USC	United States Code
USTCI	United States Transportation Command Instruction
USTRANSCOM	United States Transportation Command
VLAN	Virtual Local Area Network
VIP	Very Important Person
VOIP	Voice Over Internet Protocol
VOSIP	Voice Over Secure Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconference, Video Teleconferencing
WAN	Wide Area Network
WG	Working Group
WWW	World Wide Web
XML	Extensible Markup Language
xRM	Any Business Entity – Relationship Management

Appendix 2

APPLICABLE DOCUMENTS

Federal and DOD Regulations

Air Force COMSEC Publication AFKAG-1N, Air Force Communications Security (COMSEC) Operations
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFKAG1N.pdf

AFKAG-2L, Air Force COMSEC Accounting Manual
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFKAG_2L.pdf

AFKAG-31F, Positive Control Material
Classified Document

Air Force Instruction 33-106, Managing High Frequency Radios, Personal Wireless Communication systems, and the Military Affiliate Radio System
http://www.e-publishing.af.mil/shared/media/epubs/AFI33-106.pdf

AFI 33-111, Voice Systems Management
http://www.e-publishing.af.mil/shared/media/epubs/AFI33-111.pdf

AFI 33-112, Information Technology Hardware Asset Management
http://www.e-publishing.af.mil/shared/media/epubs/AFI33-112.pdf

AFI 33-201, Volume 1, Communications Security (COMSEC)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI_33-201V2_through_Change_1.pdf

AFI 33-201, Volume 2, Communications Security (COMSEC) User Requirements
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI_33-201V2_through_Change_1.pdf

AFI 33-201, Volume 4, Cryptographic Access Program
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI33-201V4.pdf

AFI 33-201, Volume 5, Controlled Cryptographic Item (CCI)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI33-201v5_through_Change_1.pdf

AFI 33-201, Volume 7, Management of Manual Cryptosystems
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI33-201V7.pdf

AFI 33-201, Volume 8, Communications Security: Protected Distribution Systems

AFI 33-201, Volume 9, Operational Instructions for Secure Voice Devices
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFI33-201V9.pdf

AFI 33-203 V1, Emission Security
http://www.e-publishing.af.mil/shared/media/epubs/AFI33-203V1.pdf

AFI 33-230, Information Assurance Assessment and Assistance Program
http://www.e-publishing.af.mil/shared/media/epubs/AFI33-230.pdf

Air Force Manual (AFMAN) 23-110, CD Basic USAF Supply Manual
http://www.e-publishing.af.mil/shared/media/epubs/AFMAN23-110.pdf

AFMAN 23-220, Reports of Survey for Air Force Property
http://www.e-publishing.af.mil/shared/media/epubs/AFMAN23-220.pdf

AFMAN 33-326, Preparing Official Communications
http://www.e-publishing.af.mil/shared/media/epubs/AFMAN33-326.pdf

Air Force Operating Instruction AFKAO-10C, Air Force Operating Instruction for the AN/CYZ-10/10A Data Transfer Device

Air Force Systems Security Instruction (AFSSI) 3013, Operational Instruction for Trunk Encryption Devices (TEDs); KG-81, KG-94 Family, KG-95 Family, and KG-194 Family, and KIV-19 in Stand Alone Applications
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3013.pdf

AFSSI 3014, Operational Security Instruction for the Motorola Network Encryption system (NES)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3014.pdf

AFSSI 3017, Operational Security Instruction for Non-TRI-TAC KG-84A, KG-84C, KIV-7, KIV-7HS, KIV-7HSA, and KIV-7HSB
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3017.pdf

AFSSI 3021, Operational Security Instruction for the AN/CYZ-10/10A Data Transfer Device
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3021.pdf

AFSSI 3027, Interim AF Operational Security Doctrine for the KOK-13/TSEC Remote Rekey Equipment
Classified Document

AFSSI 3031, Operational Systems Security Instruction for the Local Management Device/Key Processor (LMD/KP) (KOK-22)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3031.pdf

AFSSI 3032, Operational Security Instruction Fastlane (KG-75 and KG-75A)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3032.pdf

AFSSI 3035, Operational Systems Security Instruction for TACLANE (KG-175)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3035.pdf

AFSSI 3036, Operational Security Instruction for the Sectra In-Line Network Encryptor (KG-235)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3036.pdf

AFSSI 3038, Operational Security Instruction for the Remote Access Security Program (RASP) SECRET Dial-In Solution
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3038.pdf

AFSSI 3041, Operational Systems Security Instruction for the AN/PYQ-10 (C) Simple Key Loader (SKL) with the Embedded KOV-21 Crypographic Card
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3041.pdf

AFSSI 3042, Operational Systems Security Instruction for ALTASEC KG-250 In-line Network Encryptor (INE) and KG-250A Theatre High Altitude Area Defense (THADD) Launcher Encryption Module (TLEM)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_3042.pdf

AFSSI 4212, Reporting COMSEC Deviations
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_4212.pdf

AFSSI 7700, Emission Security (EMSEC)
Limited/Restricted Distribution,
https://private.afca.af.mil/ip/Documents/AFSSI_7700_Emission_Security-2_OCT_07_(IC-_14_April_2009).pdf

AFSSI 7702, Emission Security Countermeasures Reviews
Limited/Restricted Distribution,
https://private.afca.af.mil/ip/Documents/AFSSI_7702_30Jan08_through_Change_1_17Oct08.pdf

AFSSI 7703, Protected Distribution Systems (PDS)
Limited/Restricted Distribution, https://private.afca.af.mil/ip/Documents/AFSSI_7703_26Aug08.pdf

Air Force Systems Security Manual 4003, Emergency Destruction of Communications Security Equipment Elements
Classified Document

Chairman Joint Chiefs of Staff Instruction (CJCSI) 3231.01B, Safeguarding Nuclear Command and Control Extremely Sensitive Information
Limited/Restricted Distribution, https://ca.dtic.mil/cjcs_directives/cdata/limited/3231_01.pdf

CJCSI 6215.01C, Policy for Department of Defense Voice Networks
http://www.dtic.mil/cjcs_directives/cdata/unlimit/6215_01.pdf

CJCSI 6510.02D, Cryptographic Modernization Plan
Limited/Restricted Distribution, https://ca.dtic.mil/cjcs_directives/cdata/limited/6510_02.pdf

Committee on National Security Systems (CNSS) NACSI-6002, Protection of Government Contractor Telecommunications, National COMSEC Instruction
http://www.cnss.gov/Assets/pdf/nacsi_6002.pdf

CNSS Policy No. 1 (CNSSP-1), National Policy for Safeguarding and Control of COMSEC Material
http://www.cnss.gov/Assets/pdf/cnssp_1.pdf

CNSSP-3, National Policy on Granting Access to U.S. Classified Cryptographic Information
http://www.cnss.gov/Assets/pdf/CNSSP-3.pdf

CNSSP-15, Use of Public Standards for the Secure Sharing of Information Among National Security Systems
http://www.iad.nsa.smil.mil/resources/library/cnss_section/pdf/cnssp_15.pdf

CNSSP-19, National Policy Governing the Use of High Assurance Internet Protocol Encryptor (HAIPE) Products
http://www.cnss.gov/Assets/pdf/CNSSP-19.pdf

DOD Directive (DODD) 8000.1, Management of DOD Information Resources and Information Technology
http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf

DODD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf

DODD 8115.01, Information Technology Portfolio Management
http://www.dtic.mil/whs/directives/corres/pdf/811501p.pdf

DODD 8500.01E, Information Assurance (IA)
http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

DOD Instruction (DODI) 1100.22, Policy and Procedures for Determining Workforce Mix
http://www.dtic.mil/whs/directives/corres/pdf/110022p.pdf

DODI 5158.06, Distribution Process Owner
http://www.dtic.mil/whs/directives/corres/pdf/515806p.pdf

DODI 5200.01, DoD Information Security Program and Protection of Sensitive Compartmented Information
http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf

DODI 8115.02, Information Technology Portfolio Management Implementation
http://www.dtic.mil/whs/directives/corres/pdf/811502p.pdf

DODI 8500.2, Information Assurance (IA) Implementation
http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

DODI 8523.01, Communications Security (COMSEC)
http://www.dtic.mil/whs/directives/corres/pdf/852301p.pdf

DODI 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance (IA) Readiness Testing
http://www.dtic.mil/whs/directives/corres/pdf/856001p.pdf

DOD Regulation 5200.1-R, DoD Information Security Program
http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf

DOD 8570.01–M, Information Assurance Workforce Improvement Program
http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

E-Government Act of 2002 (Public Law 107-347)
http://csrc.nist.gov/drivers/documents/HR2458-final.pdf

Federal Acquisition Reform Act (Division D of Public Law 104-106)
http://www.cio.noaa.gov/Policy_Programs/fara.pdf

Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Information Technology Management Reform Act (Division E of Public Law 104-106)
http://www.dol.gov/ocfo/media/regs/ITMRA.pdf

National Communications Security Committee (NCSC-5), National Policy on Use of Crypto Material by Activities Operating in High Risk Environments
http://www.cnss.gov/Assets/pdf/ncsc-5.pdf

National Security Administration NAG-16F, Field Generation and Over-The-Air Distribution of COMSEC key in Support of Tactical Operations and Exercises
http://navyit.com/study%20material/NAG-16.pdf

National Security Administration NSA/CSS Policy Manual No. 3-16, Control of Communications Security (COMSEC) Material
http://www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/pdf/NSA_CSS-MAN-3-16_080505.pdf

Paperwork Reduction Act (Public Law 104-13, Chapter 35 of title 44, United States Code)
http://www.archives.gov/federal-register/laws/paperwork-reduction/3501.html

Technical Manual 00-20F-2, Inspection and Preventive Maintenance Procedures for Classified Storage Containers
http://www.robins.af.mil/shared/media/document/AFD-091005-043.pdf

USTRANSCOM Regulations

USTRANSCOM Federal Acquisition Regulation (FAR) Supplement 5552.204-9000, Notification of Government Security Activity and Visitor Group Security Agreements
http://farsite.hill.af.mil/archive/USTRANSCOM/2007-06/5552.htm#P3_63

USTRANSCOM Instruction (USTCI) 33-13, Safeguarding of Secure Voice/Data Communications Equipment

USTCI 33-16, Management of USTRANSCOM Computer Assets

http://www.transcom.mil/publications/pubs/1126-I33-16.pdf

USTCI 33-24, Publication and Forms Management
http://www.transcom.mil/publications/pubs/5394-I33-24.pdf

USTRANSCOM Policy Directive (PD) 33-10, Cellular/Multi-function Voice and Data Device Management

USTRANSCOM PD 33-21, Communications Security (COMSEC) USTRANSCOM Security Incident Reporting (SIR)

USTRANSCOM PD 33-36, User Procedures for USTRANSCOM's Remote Access Security Program (RASP)

Appendix 3

NONDISCLOSURE AGREEMENT AND AGREEMENT TO DISCLOSE POTENTIAL CONFLICTS OF INTEREST FOR CONTRACTOR EMPLOYEES ON USTRANSCOM CONTRACTS

NOTE: This Agreement is a standard agreement designed for use by contractor (including sub-contractor) employees assigned to work on USTRANSCOM contracts. Its use is designed to protect non-public Government information from disclosure, identify potential conflicts of interest, and prevent violations of federal statutes/regulations. The restrictions contained in this agreement also serve contractors by promoting compliant behavior that keeps contractors eligible to compete for Government contracts. In addition to the potential impact on future business opportunities, failure to abide by this agreement could result in administrative, civil, or criminal penalties specified by statute or regulation.

1. I, _____, currently an employee of _____, hereby agree to the terms and conditions set forth below.

2. I understand that I may have access to confidential business information, contractor bid or proposal information (as defined by FAR 3.104-1), and/or source selection information (as defined by FAR 2.101) either for contract performance, as a result of working in a USTRANSCOM facility, or of working near USTRANSCOM personnel, contractors, visitors, etc. I fully understand that such information is sensitive and must be protected in accordance with 41 US Code Section 423 and FAR SubPart 3.1.

3. In the course of performing under contract/order # _____ or some other contract or sub-contract for USTRANSCOM, I agree to:

a) Use only for Government purpose any and all confidential business information, contractor bid or proposal information, and/or source selection sensitive information to which I am given access. I agree not to disclose "non-public information" by any means (in whole or in part, alone or in combination with other information, directly, indirectly, or derivatively) to any person except to a US Government official with a need to know or to a non-Government person (including, but not limited to, a person in my company, affiliated companies, sub-contractors, etc.) who has a need to know related to the immediate contract/order, has executed a valid form of this non-disclosure agreement, and receives prior clearance by the Contracting Officer. All distribution of the documents will be controlled with the concurrence of the Contracting Officer.

b) "Non-public information," as used herein includes trade secrets; confidential or proprietary business information (as defined for Government employees in 18 USC 1905); advance procurement information (future requirements, acquisition strategies, statements of work, budget/program/planning data, etc.); source selection information (proposal rankings, source selection plans, contractor bid or proposal information); information protected by the Privacy Act (social security numbers, home addresses, etc.); sensitive information protected from release under the Freedom of Information Act (pre-decisional deliberations, litigation materials, privileged material, etc.); and information that has not been released to the general public and has not been authorized for such release (as defined for Government employees in 5 CFR 2635.703).

c) Not use such information for any non-Governmental purposes, including, but not limited to, the preparation of bids or proposals, or the development or execution of other business or commercial ventures.

d) Store the information in such a manner as to prevent inadvertent disclosure or releases to individuals who have not been authorized access to it.

4. I understand that I must never make an unauthorized disclosure or use of confidential business information, contractor bid or proposal information, and/or source selection sensitive information unless:

a) The information has otherwise been made available without restriction to the Government, to a competing contractor or to the public.

b) The Contracting Officer determines that such information is not subject to protection from release.

5. I agree that I shall not seek access to "non-public information" beyond what is required for the performance of the services I am contracted to perform. I agree that when I seek access to such information, attend meetings, or communicate with other parties about such information, I will identify myself as a contractor. Should I become aware of any improper or unintentional release or disclosure of "non-public information," I will immediately report it to the Contracting Officer in writing. I agree that I will return all forms (including copies or reproduction of original documents) of any "non-public information" provided to me by the Government for use in performing my duties to the control of the Government when my duties no longer require this information.

6. Because the Government expects unbiased judgment and recommendations from contractors performing work under its contracts and orders, I agree to advise the Contracting Officer of any actual or potential personal conflicts of interest I may have related to any work I perform under this contract/order with the government. Personal conflicts of interest include any matter in which I or my spouse, minor child, or household member has a financial interest. A financial interest is any interest in, or affiliation with, a prime contractor, subcontractor to a prime contractor, any offerors, or any prospective subcontractor to any offeror for the program, contract, or other matter for which I am performing a support task under this contract. The financial interest can take the form of any ownership interest (including but not limited to: stock; ownership of bonds; vested or unvested retirement benefits; a loan or other financial arrangement that is other than an arm's-length transaction; employment, or an arrangement concerning prospective employment including negotiations therefore; or any non arm's length loan, any gift from or other non arm's length financial arrangement with any person who is directly communicating with the government on behalf of the prime contractor, subcontractor, or any prospective subcontractor or offeror). With respect to conflict of interest disclosures required under this agreement, a financial interest in, or affiliation with, the prime contractor that is my employer under this contract does not have to be disclosed to the Contracting Officer. If any potential conflicts of interest, real or otherwise, do present themselves, then I shall immediately disclose the pertinent information to the Contracting Officer.

By signing below, I certify that I have read and understand the terms of this Non-Disclosure Agreement and Agreement to Disclose Potential Conflicts of Interest, and voluntarily agree to be bound by its terms.

_____ _____

Signature of Contractor Employee Date

_____

Printed Contractor Employee Name

_____ _____

Government Contracting Officer's Representative Date

Appendix 4

ESTIMATED WORKLOAD*

Task 2: Helpdesk, Desktop Customer, and Service Desk Support
- Task 2 Subtask 1: SDDC Helpdesk and Desktop Customer Support
  - Estimated monthly call volume: 3000
  - Estimated monthly tier-2 trouble ticket volume: 600
  - Average historical ticket resolution time: 1.85 hours
  - SDDC users supported by the help desk: 1200
- Task 2 Subtask 2: USTRANSCOM Service Desk Support
  - Estimated monthly Service Desk calls: 2900
- Task 2 Subtask 3: USTRANSCOM Service Desk Extended Support (Optional)
  - Estimated labor hours: 5,700

Task 3: Computer System Maintenance and Logistics Support
- Estimated annual lifecycle support events: 20

Task 4: PC Maintenance and Software Management Support
- Task 4 Subtask 1: PC Maintenance
  - Refer to estimated devices, accounts, etc. in Table 1 below
- Task 4 Subtask 2: Software Management
  - Estimated annual number of ES cost/benefit analyses: 10

Task 5: Special C4 Support Function
- Task 5 Subtask 1: Senior Management Support
  - Estimated labor hours: 1,900
- Task 5 Subtask 1, Paragraph 1.3.5.1.1: USTRANSCOM Senior Management Support
  - Estimated labor hours: 7,600
- Task 5 Subtask 1, Paragraph 1.3.5.1.2: SDDC Senior Management Support
  - Estimated labor hours: 5,700
- Task 5 Subtask 1, Paragraph 1.3.5.1.3: AMC Senior Management Support
  - Estimated labor hours: 1,900
- Task 5 Subtask 2: Portable Electronic Device (PED) Support Services
  - Estimated labor hours: 950
- Task 5 Subtask 3: Telephone Support Services
  - Estimated labor hours: 950
- Task 5 Subtask 4: Telephone Implementation and Integration Support (Optional)
  - Estimated labor hours: 3,800

Task 6: Training/Lab Function
- Task 6 Subtask 1: Program Support
  - Estimated number of programs/systems supported: 5
- Task 6 Subtask 2: Training Support
  - Estimated number of total courses taught: 21

Estimated number of basic/intermediate courses taught: 17
Estimated number of advanced courses taught: 4
Estimated course duration range: half day to three days
Estimated number of courses offered quarterly: 4
Estimated number of courses offered 9 times per year: 11
Estimated number of courses offered monthly: 6
Estimated number of courses requiring modification annually: 10

Task 6 Subtask 3: Support for New Training Requirements
Estimated number of new courses requiring development annually: 2

Task 6 Subtask 4: Training Videos and Computer Based Training (CBT) Development (Optional)
Estimated labor hours: 1,900

Task 7: USTRANSCOM Information Assurance and Information Protection (IA/IP)
Estimated labor hours: 39,900

Task 8: Project and Program Management
Estimated labor hours: 15,200

Task 9: Audiovisual and Video Teleconferencing Support

Task 9 Subtask 1: Audiovisual Support
Current Conference Rooms: 13
Current Training Rooms: 13
Current Auditoriums: 2
Current Senior Leader (Director/Branch Chief) Offices: 40
Current Video Walls: 2
Current Signage Systems: 10
Current Command Center Work Areas: 2
Estimated annual growth of AV systems: 10 %

Task 9 Subtask 2: Video Teleconferencing Support
Current Fixed Secure/Non-secure VTC Systems: 12
Current Fixed Non-secure VTC Systems: 4
Current Portable Secure/Non-Secure VTC Units: 2
Current Portable Non-Secure VTC Units: 2
Estimated annual growth of VTC Systems/Units: 10 %

Task 9 Subtask 3: Server and Multipoint Control Unit (MCU) VTC Support
Current Number of Secure MCUs: 1
Projecting installation of a non-secure MCU during the period of performance
Projecting replacing the secure MCU during the period of performance

Task 9 Subtask 4: Engineering Design Support
Estimated number of annual AV/VTC Engineering Designs: 15
Estimated annual growth of AV/VTC Engineering Designs: 5%
Estimated number of annual C&A Package updates: 1
Estimated number of daily USTRANSCOM-led DISA collaboration tool sessions (on business days): 2
Estimated number of annual DISA collaboration tool training sessions: 10

Task 9 Subtask 7: Briefing and Display Systems Support for the Fusion Center
Estimated number of daily briefs (and follow-on updates throughout the day): 30/month
Estimated number of Commander's Updates: 5/month

Estimated number of TCJ3 Situational Battle Update Briefs: 10/month
Estimated number of Retirement, Promotion, Etc. Events: 5/month
Estimated number of Fusion Center Distinguished Visitor tour briefings: 15/month
Estimated number of Directorate Customer Briefings: 10/month

Task 9 Subtask 8: Augmentation of Briefing and Display Systems Support for the Fusion Center

Estimated labor hours: 3,800

Table 1. Level of effort—CCE estimated devices, accounts, etc. being supported

	CPE/CDE	UOIS	COIS
Physical Servers		100	
DNS/ Mail Relay/ Management servers		20	15
Virtual Server Environment	Six (6) arrays with a minimum of 16 blade servers in each		
SAN	Six (6) storage units with ~200TB storage each		
Routers/ Switches		150	125
Security Devices		100	
Desktop Computers		3000	2000
Laptop Computers (all shall be considered to be wireless)		1000	200
Printers		350	150
Scanners		50	
User Accounts		3500	2000
Org Accounts		1000	700
Senior Leaders		150	
Mobile and Wireless Devices		200	
Voice over IP Telephones		900	1000

*The Estimated Workload is based on the duration of one Fiscal Year. Actual workload may significantly vary depending on the requirements of USTRANSCOM and other Government entities.

Appendix 5

INFORMATION ASSURANCE CONTRACTOR TRAINING AND CERTIFICATION

Task	IA Function	None	IAT I	IAT II	IAT III	IAM I	IAM II	IAM III	IASAE I	IASAE II	IASAE III
2	N/A	X									
2.1	T-II.1-31			X							
2.2	N/A	X									
2.3	N/A	X									
3	T-I.1, 10, 11, 14, 17, 19		X								
4	N/A	X									
4.1	T-I.1-11, 13-19		X								
4.2	N/A	X									
5	T-II.1-20, 23-31			X							
5.1	T-I.1-19		X								
5.2	T-I.1-19		X								
5.3	T-I.1-19		X								
5.4	T-II.1-31			X							
6	N/A	X									
6.1	N/A	X									
6.2	N/A	X									
6.3	N/A	X									
6.4	N/A	X									
7	T-III.1, 2, 4, 6, 9-13, 17, 23-24				X					X	
7.1	T-II.1-11, 14-15, 17-20, 23-28, 30-31			X						X	
7.2	N/A	X									
7.3	T-II.1-11, 13, 15, 17-18, 20, 23-28, 30-31 M-II.10, 14, 19, 21, 23			X			X				
7.3 Paragraph 1.3.7.3.1	T-II.1-20, 23-28, 30-31			X							
7.3 Paragraph 1.3.7.3.2	M-II.10, 14, 21, 23						X				
7.4	T-III.1, 2, 4, 6, 9-13, 15, 18-19, 21, 24				X					X	
8	N/A	X									
8.1	N/A	X									
8.2	N/A	X									
9	N/A	X									
9.1	N/A	X									
9.2	N/A	X									

9.3	T-I.1-19		X								
9.4	N/A	X									
9.5	N/A	X									
9.6	N/A	X									
9.7	N/A	X									
9.8	N/A	X									

Appendix 6

Operating Systems/Software/Applications Supported

ABSS
ActiveClient
Adobe Acrobat Pro, Flash, Photoshop, Shockwave Player, Creative Suite
AMHS
Anti-virus Software (e.g., Symantec, McAfee, Trend Micro)
Apache, Apache Web Server
Apple (e.g., OS X, iOS)
ARC GIS
ArcServiT
Army Gold Master Software
BCS3
Bind Version 8.0 and above
Blackberry (e.g., Desktop Manager, Enterprise Server)
BMC Patrol
CIPS
Cisco (e.g., Internet Operating Software (IOS), Cisco Works)
Classify for Outlook
ColdFusion
Commpower XML Portal
Content Filtering (e.g., Bluecoat Proxy server, Squid, SmartFilter)
Crystal Reports
DBSign Web Signer
DCO
DOORS
EMC RecoverPoint
ERWin
Firewalls (e.g., Checkpoint NG/Firewall-1, IPFilter, Raptor, Sidewinder)
Fore Internet Operating Software (IOS)
Foreview Foundation
FormFlow Filler
GEOPDF
GOGlobal
Good Technology Server
Google Earth
Hewlett Packard (HP) Open View, Network Node Manager, SOA Systinet UDDI
IBM Landesk Manager
infinite IVe b/I
InfoConnect
Intrusion Detection Systems (e.g., Snort, ISS Real Secure, Argus)
IP Ultra Scan 2000
IPTV (e.g. HaiVision InStream, Furnace, Stingray)
ITS (formerly CRIS)
J2SE Runtime Environment
JALIS
JetForm, FormFlow
JFAST
JInitiator
JTEN
LANDesk Management Suite
LDAP
Liferay Portal
Microsoft Access, DOS, Exchange, Internet Information Server, Internet Explorer, Lync, Office, Office Communicator, Outlook, Project, SMS, SQL Server, Visio, Windows, Windows Media Player
Mozilla Firefox, Thunderbird
Multi Router Traffic Grapher (MRTG)
MultiCal
mySQL
NavFit
Navisphere Manager
Netscape Communicator, iPlanet
NetViz
Network Associates Sniffer Pro
Network Tools (e.g., TCPDUMP, nmap)
On-Track
Open BSD 2.8 and above
Oracle (e.g., Database, Client)
Parallels
Perl
PES
PFPS
PowerTrak
PureEdge Viewer
Putty
Quota Advisor
Red Hat Linux 7.0 and above
Remedy (e.g., Action Request System)
Rightrix
Roxio CD Creator
Secure Shell (SSH)
Sendmail
SiteMinder
So/iKe;', Calendar Creator Plus
Sun Solaris
Symantec AntiVirus
Telos AMHS 2005
Terminal Access Controller Access Control System (TACACS)
Teradata
TightVNC
TMART
Tomcat
TransViz
UNIX operating systems (e.g., SOLARIS, HP-UX, FreeBSD)
Verity K2
Whats Up Gold
Winiip,
WinZip

VMWare (e.g., ESX,
vCenter, vMotion)
Zantaz EAS

Appendix 7

Protocols In Use

Asynchronous Transfer Mode (ATM)
Border Gateway Protocol (BGP)
Challenge Handshake Authentication Protocol (CHAP)
Common Services/Protocols (e.g., Domain Name Service (DNS))
Computer forensics
Content Delivery
Dense Wavelength Division Multiplexing (DWDM)
Domain Name Service (DNS)
Dynamic Host Configuration Protocol (DHCP)
Emulated Local Area Network (ELAN)
Ethernet (10BaseT, 10BaseF, 100BaseT, 100BaseF, 1000BaseFX, 1000BaseSX, 1000BaseT)
Ethernet 802.3 and Ethernet 802.2 (IPX/SPX)
Fiber Channel (FC)
Fiber Distributed Data Interface (FDDI)
Hot Standby Routing Protocol (HSRP)
Hyper Text Transfer Protocol (HTTP)
Information security concepts (e.g., authentication, confidentiality, integrity, non-repudiation, network segmentation, Public Key Infrastructure (PKI), and others)
Information security devices
Integrated Services Digital Network (ISDN)
Interim Local Management Interface (ILMI)
IP Port Security 802.1a
Internet Protocol Security (IPsec)
IP Network/Subnetwork design and management
LAN Emulation (LANE)
Link analysis
Network Address Translation
Network architectures and concepts (e.g., Asynchronous Transfer Mode (ATM), Classless Inter-Domain Routing (CIDR), Gigabit Ethernet, Ethernet, Network Address Translation (NAT), Router/Switch Functions, Remote Access Server (RAS), Transmission Control Protocol/Internet Protocol (TCP/IP), Virtual Private Networking (VPN))
Network traffic analysis
Novell Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)
Novell Link Support Protocol (NLSP)
Open Shortest Path First (OSPF)
Password Authentication Protocol (PAP)
Point-to-Point Protocol (PPP)
Private/Public Network Node/Network Interface (PNNI)
RADIUS
Remote Dial-in Access (Analog and Digital)
Secure Hyper Text Transfer Protocol (HTTPS)
Secure Shell (SSH)
Secure systems architectures and design
Simple Mail Transfer Protocol (SMTP)
Simple Network Management Protocol (SNMP)
Spanning Tree Protocol (STP)
Stateful packet inspection devices/applications
Storage Area Network (SAN)
Switched, routed, and bridged services
Synchronous Optical Network (SONET)
Transmission Control Protocol /Internet Protocol (TCP/IP)
UNIX and Windows operating systems environments
User Network Interface (UNI)
Virtual Local Area Network (VLAN)
Virtual Private Network (VPN)
Windows Internet Naming Service (WINS)
Wireless Ethernet (802.11a, 802.11b. 802.1)

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: TOP SECRET

b. LEVEL OF SAFEGUARDING REQUIRED: NONE

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*

X	a. PRIME CONTRACT NUMBER: HTC711-11-F-D051	
	b. SUBCONTRACT NUMBER	
X	c. SOLICITATION OR OTHER NUMBER: USTRANSCOM-FP-00006-11	DUE DATE (YYYYMMDD):

3. THIS SPECIFICATION IS: *(X and complete as applicable)*

	a. ORIGINAL *(Complete date in all cases)*		DATE (YYYYMMDD): 20110112
X	b. REVISED *(Supersedes all previous specs)*	REVISION NO: 1	DATE (YYYYMMDD): 20110906
	c. FINAL *(Complete item 5 in all cases)*		DATE (YYYYMMDD):

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____.

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
Webster Data Communications Incorporated 11250 Waples Mill Road Fairfax, VA. 22030-7422 (571) 748-4454 / dmorrow@websterdata.com	1HNK0	Defense Security Service (IOFCC2) 14428 Albemarle Point Place, Suite 140 Chantilly, VA 20151 (703) 428-0018

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
SRA International, Inc. 475 Regency Park, Suite 300 O'Fallon, IL. 62269 (618) 622-4000 ext 4 / erin_hamilton@sra.com	0GL91	Defense Security Service (IOFSL) St. Louis Field Office 303 Fountains Parkway, Suite 303 Fairview Heights, IL 62208 (618) 206-7212

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*
USTRANSCOM/TCJ6 508 Scott Drive Scott AFB, IL. 62225		Defense Security Service (IOFSL) St. Louis Field Office 303 Fountains Parkway, Suite 303 Fairview Heights, IL 62208

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

The United States Transportation Command (USTRANSCOM) mission is to provide air, land, and sea distribution for the Department of Defense (DOD), during both peacetime and when at war. The Commander of USTRANSCOM is tasked as the single manager of the Defense Distribution System (DDS). This contract supports the Command, Control, Communications and Computer Systems Directorate (TCJ6).

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION	X		a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RESTRICTED DATA		X	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	X	
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	X	
d. FORMERLY RESTRICTED DATA		X	d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE	X	
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		X
(1) Sensitive Compartmented Information (SCI)	X		f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
(2) Non-SCI	X		g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
f. SPECIAL ACCESS INFORMATION		X	h. REQUIRE A COMSEC ACCOUNT	X	
g. NATO INFORMATION	X		i. HAVE TEMPEST REQUIREMENTS		X
h. FOREIGN GOVERNMENT INFORMATION		X	j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS	X	
i. LIMITED DISSEMINATION INFORMATION		X	k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X		l. OTHER *(Specify)*	X	
k. OTHER *(Specify)* NATO access is authorized due to SIRPNET has been approved for NATO by the CUSR.	X		Classified access to systems and locations on SAFB, IL. while under this contract. This includes any COOP locations and DECC/DISA sites on SAFB.		

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE. Adobe Professional 7.0

12. PUBLIC RELEASE. Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release [ ] Direct [X] Through (Specify)

USTRANSCOM Public Affairs Office, ATTN: (TCPA)(508 Scott Drive, Scott AFB, IL 62225-5357, 618-229-4828) and USTRANSCOM Information OPSEC Security Officer: (TCJ3-F)(508 Scott Drive, Scott AFB, IL 62225, 618-220-6550)

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review. *In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

Security Requirements:

(a.) Contractor shall be responsible for ensuring all security requirements outlined in the Performance Work Statement (PWS) are accomplished after award of the contract.

(b.) For Official Use Only (FOUO) applies for all unclassified material. Reference DoD 5200.1-R, Appendix 3 and the Under Secretary of Defense for Intelligence memorandum, "Interim Information Security Guidance," dated April 16, 2004, (http: www.fas.org/sgp/othergov dod dod041604.pdf), for specific guidance on the handling and safeguarding of FOUO information.

(c.) Contractor employees who are physically assigned to USTRANSCOM at SAFB shall attend/complete the following training as prescribed by DOD, USTRANSCOM and Air Force Instructions: Employee Initial Security Briefing, Annual Security Awareness Training, Operations Security (OPSEC), DOD Antiterrorism Level 1 training and any Security Stand Down Day Training scheduled by the commander.

(d.) Contractors permanently assigned to this contract may obtain Common Access Cards (CAC) once the Trusted Agents (TA) processes the required security information in the Contract Verification System (CVS). Upon receipt of the CAC, permanently assigned contractor employees may obtain the AF 1199 (Restricted Area Badge) if the member meets the requirements set forth in SAFB Instruction 31-101 and PWS Security Standards.

(e.) Visit(s) by contract company personnel not permanently assigned to this contract (company presidents, company security managers, ect.) will require an electronic visit request in the Joint Personnel Adjudication System (JPAS). Contractors permanently assigned to USTRANSCOM at SAFB, IL will require JPAS visit requests which will contain the contract number posted in the POC section of the visit. they will also require a copy of the DD 254 for this contract to show classified access level for this contract. Both visit request types will be forwarded to JPAS SMO: USTC-SDDC.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract [X] Yes [ ] No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

Contractor will coordinate with the USTRANSCOM SSO for any issues (including indoctrination) for SCI material.

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office [X] Yes [ ] No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

(CJ2-SSO has exclusive rights and responsibility for SCI material released or developed under this contract. The CSO is relieved of responsibility to inspect TS-SCI facilities on SAFB.

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
Patrick M. Collins	Chief, Security Services Center (Industrial Sec)	618-220-6550

d. ADDRESS (Include Zip Code)	17. REQUIRED DISTRIBUTION	
USTRANSCOM, Force Protection (TCJ3-FP) 508 Scott Drive Scott Air Force Base, IL, 62225-5004	X	a. CONTRACTOR
	X	b. SUBCONTRACTOR
	X	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE		d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	X	e. ADMINISTRATIVE CONTRACTING OFFICER
	X	f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

United States Transportation Command; Corporate Services Support: Service Support

Solicitation Number: HTC711-11-R-D003
Submission Date: July 14, 2011

Volume II: Technical Approach

(Electronic Copy)

Submitted to:
USTRANSCOM/TCAQ-D
Attn: Ms. Mills/ Mr. Muskopf
508 Scott Dr., Bldg. 1900 W
Scott AFB, IL 62225

WEBSTER DATA communication

11250 Waples Mill Road, Suite 430
Fairfax, VA 22030
703.351.9977
WebsterData.com

SRA INTERNATIONAL, INC.

475 Regency Park, Suite 300
O'Fallon, IL 62269
618.622.4000
SRA.com

Volume II – Technical Approach

Solicitation # HTC711-11-R-D003

Corporate Services Support: Service Support

Prepared for
United States Transportation Command
USTRANSCOM/ TCAQ-D
508 Scott Dr., BLDG. 1900 W
Scott AFB, IL 62225
Ms. Stephanie Mills
Office: (618) 220-7096
Stephanie.mills@ustranscom.mil

Prepared by

Webster Data Communication, Inc.
11250 Waples Mill Road, Suite 430, South Tower
Fairfax, VA 22030
Office: (703) 351-9977 / Fax: (703) 673-9932
jlee@ (b)(6)

Negotiation & Signature Authority
Jay Lee, President & CEO
Office: (571) 748- (b)(6) / Mobile: (703) 651- (b)(6) / Fax: (703) 673-9932
jlee@ (b)(6)

Webster Data Communication, Inc. agrees to all terms, conditions, and provisions included in the solicitation and will furnish any or all items upon which prices are offered at the price set opposite each item.

(b)(6)

Signature

July 14, 2011, 1:00 p.m. CT

WEBSTER DATA
COMMUNICATION

July 14, 2011

ATTN: Ms. Stephanie Mills/618-220-7114
USTRANSCOM/TCAQ-D
508 Scott Dr., BLDG. 1900W
Scott AFB, IL 62225

Subject: Corporate Services Support: Service Support; **RFP No.HTC711-11-R-D003**

Dear Ms. Mills,

Webster Data Communication, Inc. (WDC) is pleased to enclose our proposal for the US Transportation Command (USTRANSCOM) Corporate Services Support: Services Support (CSS: SS). WDC, the Small Business Prime, and our subcontractor: Systems Research and Applications Corporation, a wholly-owned subsidiary of SRA International, Inc. (SRA), form *TEAM WDC*. We are a powerful Small Disadvantaged Business and large business incumbent that have worked together in related information technology (IT) enterprise environments, namely on the Military Sealift Command (MSC) AFLOAT IT Support Services contract. We are committed to making CSS: SS the strategic cornerstone of their respective companies for the entire contract period of performance.

TEAM WDC's management and technical approaches are based on understanding the USTRANSCOM's IT environment and mission objectives. The success of the CSS: SS Program is of paramount importance to *TEAM WDC*. *TEAM WDC* combines the strengths of all to ensure that the skill sets represented to USTRANSCOM are highly qualified and we provide a technical service management framework for transition.

WDC's proposal is predicated upon all the terms and conditions of this Request for Proposal. WDC offers to provide complete performance for all requirements for the 12 month base period and four (4) 12 month option periods. I am fully authorized to negotiate on WDC's behalf. Please address any inquires to my attention at: Office (571) 748- (b)(6) Cell (703) 651- (b)(6) or email jlee@ (b)(6)

Respectfully,

(b)(6)

Jay Lee
President and Chief Executive Officer

Offeror Name: Webster Data Communication, Inc.

Request for Proposal (RFP) HTC711-11-R-D003 Submission Checklist

	Included	Location (by Volume)
Completed DD254 (Attachment 2)	☒Yes ☐ No	Volume III: Price
Past Performance Submission (Attachment 4)	☒Yes ☐ No	Volume I: Past Performance
Past Performance Log (Attachment 5)	☒Yes ☐ No	Volume I: Past Performance
Staffing Matrix (Attachment 7)	☒Yes ☐ No	Volume II: Technical Approach
Technical Approach	☒Yes ☐ No	Volume II: Technical Approach
Price Proposal (including labor rates, Attachment 8 and Pricing Schedule, Attachment 9)	☒Yes ☐ No	Volume III: Price
OCI Mitigation Plan/OCI Statement	☒Yes ☐ No	Volume III: Price
Task Order Management Plan	☒Yes ☐ No	Volume II: Technical Approach
Notice of Order Size Rerepresentation (Attachment 10)	☒Yes ☐ No	Volume III: Price

Acronym List

Abbreviation / Acronym	Definition
AAR	After Action Report
AD	Active Directory
AFB	Air Force Base
AFCOMSEC	Air Force Communications Security
AIS	Automated Information Systems
AITS	Advanced Information Technology Services
ALC	Accounting Legend Codes
AMC	Air Mobility Command
API	Fig 2-4
ARNG	Army National Guard
ATO	Authorization to Proceed
AV	Audio Visual
BCA	Benefit Cost Analysis
BSA	Business Systems Analyst
BSC	Balanced Score Card
C&A	Certification and Accreditation
C4S	Command, Control, Communications, and Computer Systems
CAC	Common Access Cards
CAP	C&A Professional
CBT	Computer Based Training
CCB	Configuration Control Board
CCB	Configuration Control Board
CCEA	COMSEC Equipment Account
CCNP	Cisco Certified Network Professional
CCRI	Cyber Readiness Inspection
CDR	Call Detail Report
CEO	Chief Executive Officer
CFE	Contractor Furnished Equipment
CI	Configuration Item
CISSP	Certified Information Systems Security Professional
CM	Configuration Management
CM	Configuration Management
CMDB	Configuration Management Database
CMDB	Configuration Management Database
CMMI	Capability Model Maturity Integration
CO	Contracting Officer
COCOM	Combatant Command
COMSEC	Communications Security
COOP	Continuity of Operations
COR	Contracting Officer's Representative
COTR	Contracting Officer's Technical Representative
COTS	Commercial-off-the-Shelf
CPM	Critical Path Method
CRO	COMSEC Responsible Officer
CS	Cyber Security
CS&PS	Cyber Security and Privacy Solutions
CSS	Corporate Services Support
CSS: SS	Corporate Services Support: Service Support
CTT+	Certified Technical Training

Abbreviation / Acronym	Definition
D2C2	Deployable Distribution Command and Control
DARPA	Defense Advanced Research Projects Agency
DATO	Denial of ATO
DIACAP	DOD Information Assurance Certification and Accreditation Process
DISCO	Defense Industrial Security Clearance Office
DISN	Defense Information System Network
DoD	Department of Defense
DOI	US Department of the Interior
DOL	US Department of Labor
DON/AA	Department of the Navy, Assistant for Administration
DPO	Distribution Process Owner
DVS	DISN Video Services
EA	Executive Authority
EDI	Electronic Data Interchange
EIP	Enterprise Integration Program
EKMS	Electronic Key Management System
eMASS	Enterprise Mission Assurance Support Service
ESM	Enterprise Systems Management
ETA	Education, Training, and Awareness
FTE	Full Time Equivalent
GAO	US Government Accountability Office
GCCC	Global Command Control Center
GCIH	Global Information Assurance Certification-Certified Incident Handler
GFE	Government Furnished Equipment
IA	Information Assurance
IASAE	IA Workforce System Architecture and Engineering
IATO	Interim Authorization to Proceed
IATT	Interim Approval to Test
IAVA	Information Assurance and Vulnerability Assessment
IM	Implementation Manager
IPR	In-Process Review
IS	Information Systems
ISD	Instructional Systems Design
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISSE	Information System Security Engineering
IT	Information Technology
ITD	Information Technology Division
ITD	Individual Training Development
ITIL	IT Infrastructure Library
JDDE	Joint Deployment and Distribution Enterprise
KP	Key Processor
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LMD	Local Management Device
MCP	Mobile Command Post
MCSE	Microsoft Certified Systems Engineer
MCT	Microsoft Certified Trainer
MCU	Multipoint Control Units
MEO	Most Efficient Organization

Abbreviation / Acronym	Definition
MSC	Military Sealift Command
MSR	Monthly Status Review
NISPOM	National Industrial Security Program Operating Manual
NMCI	Navy-Marine Corp Intranet
NOC	Network Operations Center
NSA	National Security Agency
OCR	On-Call Roster
OI	Operating Instructions
OPA	SECNAV Office of Program Appraisals
PDP	Performance Development Plan
PE	Project Elements
PM	Project Manager
PMBOK	Program Management Body of Knowledge
PMI	Project Management Institute
PMM	Project Management Methodology
PMO	Program Management Office
PMP	Project Management Plan
POC	Point of Contact
PTO	Paid Time Off
PWS	Performance Work Statement
QA	Quality Assurance
QC	Quality Control
RACI	Responsible, Accountable, Consulted, Informed
ROI	Return on Investment
SAFB	Scott Air Force Base
SBSS	Standard Base Supply System
SCIF	Sensitive Compartmented Information Facilities
SDDC	Surface Deployment and Distribution Command
SDLC	System Development Life Cycle
SECNAV	Secretary of the Navy
SEI	Software Engineering Institute
SHRM	Society for Human Resource Management
SLO	Service Level Objective
SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOC	Security Operations Center
SOP	Standard Operating Procedures
SRA	Systems Research and Applications Corporation
SRR	System Requirements Review
SSCP	Systems Security Certified Professional
SSE	Systems Security Engineering
SSR	Special Security Representative
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
SVRO	Secure Responsible Officer
TACLANE	Tactical Local Area Network
TCC	Transportation Component Command
TCCC	USTRANSCOM Commander
TCCS	USTRANSCOM Chief of Staff
TCDC	USTRANSCOM Deputy Commander

Abbreviation / Acronym	Definition
TCJ6	USTRANSCOM C4S Directorate
TCO	Total Cost of Ownership
TM	Task Manager
TOMP	Task Order Management Plan
TRB	Task Review Board
TRB	Task Review Board
USAF	United States Air Force
USAID	U.S. Agency for International Development
USTRANSCOM	United States Transportation Command
VI	Visual Information
VIP	Very Important Person
VOC	Video Operations Center
VOC	Voice of the Customer
VTC	Video Teleconferencing
WAN	Wide Area Network
WBS	Work Breakdown Schedule
WDC	Webster Data Communication

TABLE OF CONTENTS

2.0 OVERVIEW

TEAM WDC is an experienced Information Technology (IT) service provider whose collective corporate experience gives J6 Directorate (TCJ6) an IT partner with innovative service-oriented solutions and approaches. Our deep knowledge of USTRANSCOM's IT enterprise environment will result in better mission, goal, and requirement fulfillment. As USTRANSCOM's role expands in support of global operations, TCJ6 must be ready to provide IT support enabling agile, flexible, and integrated processes to deliver customer-focused IT services in support of USTRANSCOM's IT enterprise. *TEAM WDC* is poised to optimize and make significant improvements in TCJ6's Corporate Services Support: Service Support (CSS: SS) IT support services. As described below, our proposal is built on three key principles: (1) Proven Partnership, (2) Predictable Service, and (3) a Plan for the Future.

A Proven Partnership. Our demonstrated performance on contracts of similar size and complexity to USTRANSCOM's CSS: SS program minimizes risk and validates our ability to address successfully all tasks within the performance work statement (PWS) in full partnership with USTRANSCOM by maintaining open, honest, and direct communications.

Predictable Service Support. Webster Data Communication, Inc. (WDC), the prime, is a USTRANSCOM partner contractor with more than 6 years experience supporting USTRANSCOM's Transportation Component Command (TCC), MSC. *TEAM WDC's* subcontractor SRA is a prime partner with USTRANSCOM for over 24 years and has consistently provided reliable, high quality support.

Plan for the Future. *TEAM WDC* presents tangible, innovative service solutions that reduce cost, improve efficiency, and increase flexibility of IT Service Support, as discussed under each task area within our Task Order Management Plan (TOMP).

TEAM WDC, a long time USTRANSCOM contracting partner (Figure **2-1**), knows the importance the Service Support team provides to USTRANSCOM. Consequently, we are committed to client satisfaction, mission partnership, innovative ideas, and continuous improvement. Figure **2-2** illustrates our understanding of the TCJ6 environment in supporting the Joint Deployment and Distribution Enterprise (JDDE). Figure **2-2** summarizes the features and exceptional benefits that *TEAM WDC* brings to USTRANSCOM, validated by our technical approach.

TEAM WDC's Relevant IT Contracts Supporting USTRANSCOM
TCJ3 Global Command and Control System/Joint Operations, Planning and Execution (GCCS/JOPES) Functional Data Management
TCJ3 Critical Infrastructure Program
TCJ3 Exercise Support Services
TCJ5/4 Concepts, Wargames, and Experimentation
TCJ5/4 Strategic Analysis Support
TCJ6 Communications and Computer Systems (C4S) Support
TCJ6 Automatic Identification Technology (AIT) Support
Military Sealift Command (MSC) AFLOAT IT Support Services

Figure 2-1. Relevant IT Contracts Supporting USTRANSCOM. *TEAM WDC has a long-standing history supporting USTRANSCOM on similar IT efforts.*

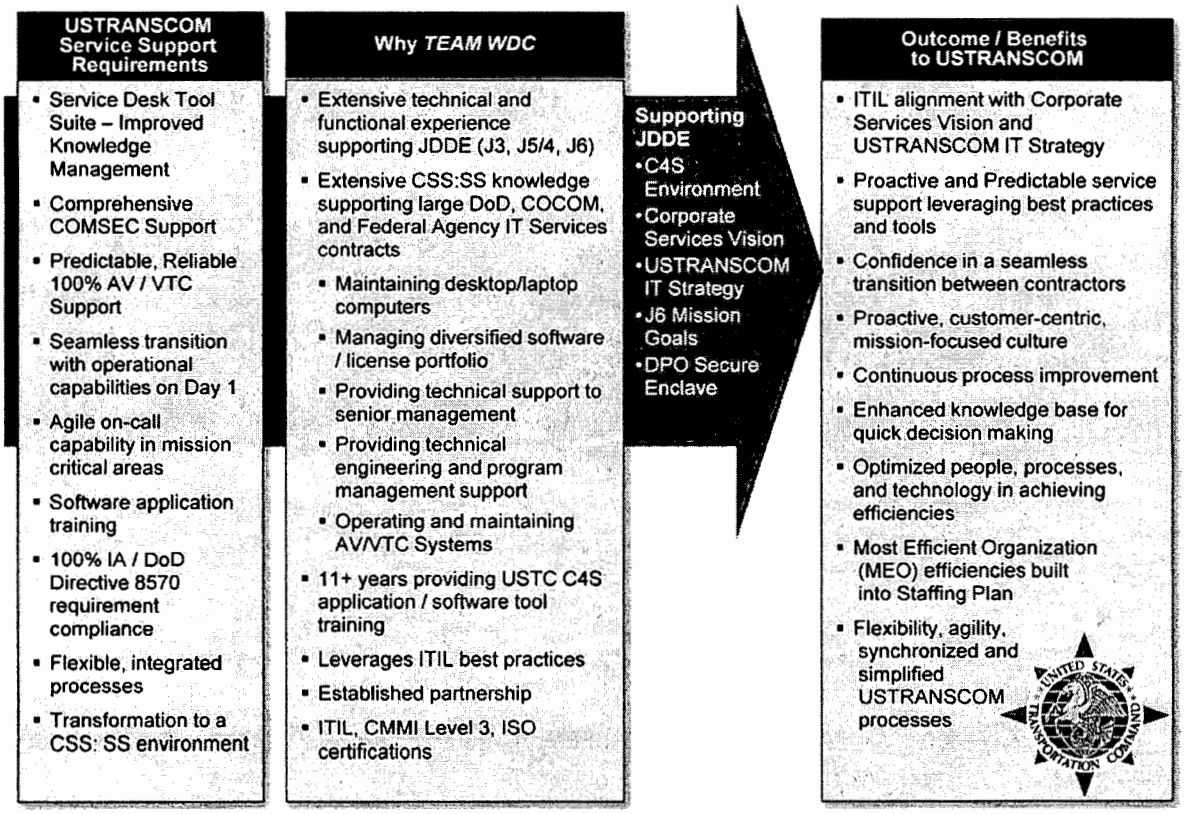


Figure 2-2. *TEAM WDC's* Outcome and Benefits to USTRANSCOM.

TEAM WDC's strong past performance is evidence of our ability to support the CSS: SS program, providing TCJ6 with a high level of confidence in our ability to perform services under this contract. Figure **2-3** provides a snapshot of the relevance of our past performance (NR = Not Relevant, SR = Somewhat Relevant, R = Relevant, HR = Highly Relevant). Full write-ups on these contracts are available in Volume I: Past Performance.

Performance Area	DARPA	ITD	NMCI	CITS	EOSS	FDIC	MSC
Demonstrate performance maintaining desktop and laptop computers for a similarly sized organization (supporting at least 3,500 desktops/laptops)	HR	HR	HR	HR	HR	HR	HR
Demonstrate performance managing a diversified (multi-vendor) software/license portfolio of at least $10 million	NR	NR	SR	HR	R	HR	NR
Demonstrate performance providing technical support to general officers, senior executive service civilians and their supporting staff or to corporate executive equivalents and their supporting staff	HR	HR	HR	HR	HR	NR	NR
Demonstrate performance providing technical engineering and program management support for programs to include: planning, policy development, technical integration and interoperability, and life-cycle support	HR	HR	R	HR	HR	HR	HR
Demonstrate performance operating and maintaining AV/VTC systems	HR	R	NR	HR	HR	HR	NR

Figure 2-3. *TEAM WDC* Past Performance Snapshot. *TEAM WDC's highly relevant past performance proves our ability to successfully perform the services under the CSS: SS contract.*

2.1 TEAMING APPROACH

TEAM WDC prime contractor Webster Data Communication, Inc. (WDC) is a Small Disadvantaged Business with a Top Secret Facility Clearance and experience providing Information Technology (IT) support services to customers similar to USTRANSCOM. Our sole subcontractor, Systems Research and Applications Corporation, a wholly-owned subsidiary of SRA International, Inc. (SRA), is a large business and current USTRANSCOM incumbent contractor. WDC and SRA enjoy a long history of teaming and are bonded through mutual trust honed on the USTRANSCOM's Military Sealift Command (MSC) AFLOAT IT Support Services contract. Our corporate experience supporting sensitive, highly classified IT programs has forged WDC into a small business with exceptional capabilities. The cornerstone of WDC's experience is embedded in its seven-year work experience with the Defense Advanced Research Projects Agency (DARPA) and its decade-long work experience with US Navy customers such as the Navy-Marine Corps Intranet (NMCI) and the Department of the Navy, Assistant for Administration's (DON/AA) Information Technology Division (ITD).

TEAM WDC offers insight into USTRANSCOM's IT enterprise, because SRA has a long partnership history with USTRANSCOM, dating back to USTRANSCOM's inception in 1987. As a result of this partnership, *TEAM WDC* has developed a strong appreciation for the critical role of strategic planning and systems integration in supporting USTRANSCOM's mission to develop and direct the JDDE. Our team member, SRA, provides technical and training support to the current TCJ6 IT Support of Selected USTRANSCOM C4 Systems and Support Functions contract. SRA also directly supports USTRANSCOM's high priority initiatives to develop and implement Deployable Distribution Command and Control (D2C2) capabilities such as the Joint Task Force – Port Opening. Within the TCC, SRA is the prime contractor providing Enterprise Support Services to the Surface Deployment and Distribution Command (SDDC) G6. This project delivers a broad range of information technology support services to SDDC including: managing the Command's Common Computing Environment, Enterprise Integration Program (EIP) data center operations, Service Oriented Architecture (SOA) implementation enterprise data engineering and standardization, enterprise Electronic Commerce and Electronic Data Interchange (EDI), system integration, system development, and portal development. *TEAM WDC* will leverage our in-depth experience, expertise, and contributions to improve USTRANSCOM's IT environment by utilizing the CSS: SS contract as a vehicle to achieve TCJ6's vision, goals, and objectives.

Our team is structured to streamline the interaction between TCJ6, its stakeholders, and its end-users and to provide a ready and accessible staff to support the command's IT projects. We will provide an efficient, high-quality support services solution by introducing innovative approaches to staffing, Service Desk tool suite research and recommendation, and Communications Security (COMSEC) and Audio Visual (AV)/ Video Teleconferencing (VTC) services. *TEAM WDC's* management structure provides rapid access from the customer to our executive management team to immediately resolve any potential program problems. *TEAM WDC* will leverage industry best practices (i.e., Information Technology Infrastructure Library [ITIL] v3, Capability Maturity Model Integration [CMMI], and International Organization for Standardization [ISO]) used on our other large IT support services programs to transfer knowledge and lessons learned to TCJ6. Illustrated in Figure **2-4**, *TEAM WDC* provides highly relevant services similar to those required under this contract. We provide TCJ6 with a team who is familiar with and is working in the

USTRANSCOM IT environment today, as well as one who has designed, implemented, and sustained IT service solutions, large and small, for DoD and commercial customers.

TEAM WDC	
Webster Data Communication, Inc. 11250 Waples Mill Road, Suite 430 Fairfax, VA 22030	**SRA International, Inc.** 475 Regency Park, Suite 300 O'Fallon, IL 62269
• Extensive complex program management, deep help desk, service desk, and IA experience • Proven leadership capability in managing large IT contracts • Extensive end-user and VIP support at DARPA, NMCI, and SECNAV ranging from as many as 3,000 users and over 7,500 devices and peripherals • Monitoring & management of network operations for Navy Marine Corps Intranet • More than 98 percent of staff possess security clearances; many hold professional certifications • Small Disadvantaged Business with a Top Secret Facility Clearance • IA and IT personnel are DoD 8570 compliant. WDC personnel certified in: CISSP, C&A Professional (CAP), Global Information Assurance Certification-Certified Incident Handler (GCIH), PMP, Comptia A+, CCNP, MCSE, MCP, HDI Support Center, SSCP, BMC Remedy	• Currently serves USTRANSCOM at both the Command and the Transportation Component Command levels • 70 plus personnel on eight USTRANSCOM projects currently providing strategic planning and advisory services to the J2, J3, and J5/4 • 50 plus personnel serving SDDC on the Enterprise Support Services Contract providing support for the Command's Enterprise Common Computing Environment • Infrastructure management, service support, and service delivery support experience across multiple contracts including the Military Sealift Command (MSC) Afloat contract • Provides full spectrum of communications and information technology services for US European Command and US Africa Command • ISO 9001:2008 certified; ISO 20000-1:2005 certified; CMMI Level 3 certified; and NSA IA-CMM Rating

Figure 2-4. ***TEAM WDC.*** *A well-qualified team that simplifies interaction with the TCJ6 and provides efficient, high quality IT support solutions to meet USTRASCOM Directorate needs*

2.2

(b)(4)

(b)(4)

(b)(4)

2.2.1

(b)(4)

(b)(4)

(b)(4)

Figure 2-5. (b)(4)

(b)(4)

We will compare and assess each product based on product description, capabilities, platforms supported, servers (UNIX, Windows, Linux, etc.), clients (e.g., Windows 2003, NT and XP etc.), databases supported, and Web browsers. We will conduct a product comparison of each product based on the following criterion:

- **System Management Features.** Ensures that the service desk products easily integrate with the TCJ6's enterprise systems. The enterprise systems management (ESM) feature helps us assess the full-fledged capability of the service desk product—the more robust and versatile the product the better it is for TCJ6.
- **Call Management Capability.** Facilitates staff tracking of all activity for service request. Comparing this feature enables quick call logging with minimal keystrokes. Our technicians will ensure precuts have support for standard and customizable templates to assist in rapid tracking and calls documenting.
- **Asset Tracking and Validation.** Evaluation is based on the availability of asset tracking and validation features in the service desk product.
- **Web Interface.** Evaluation consists of determining if products have a Web interface that provides administrative and user access (i.e., log calls, monitor priority of calls, track their calls, monitor category calls and service requests, incident reports, etc.) to service desk functionalities and features using a Web browser.
- **ITIL Processes Supported.** *TEAM WDC* will ensure all evaluated products are compliant with ITIL defined processes.
- **Integration with Other ESM Products.** In order to provide seamless and proactive support, it is imperative that the ESM product and the service desk tool integrate seamlessly. We will evaluate tools on a key criterion: integration capability.

- **Knowledge Management.** We will examine the tool's ability to be authored in multiple formats, and we will build a knowledge base from incidents and problems that will improve and contribute to USTRANSCOM's Knowledge Management initiatives.
- **Performance Reporting**. This criterion is essential when considering performance measurements against Service Level Agreements. The selected product must have the out-of-the-box ability to produce reports (e.g., outage percentages, number of users affected, etc.) and provide drill-down capabilities allowing the user to obtain detailed information on a problem, a change, or an incident.
- **Scalability**. Evaluated based on the product's ability to be scaled to meet Tier 3 support capability should TCJ6 require expanded Service Desk requirements.
- **Security**. Evaluated to ensure all products have adequate security measures to ensure Tiered access to the service desk tool and that the tool can facilitate third party access interface for security authentication and authorization.

Examples of criteria evaluated during this phase are outlined in Figure **2-6**.

Help Desk Software	Asset Management	ITIL Ready	Integrations
Self-Service Portal Knowledge Base Service Level Agreements Multi-Site Support Custom Request Form Scheduler Help Desk Reports Flash Reports Help Desk API Automated Password Reset Tool	IT Asset & Inventory Management Track Assets Software Asset Management Software License Tracking Product Catalog Purchase Order Tracking Contract Management Inventory Reports	ITIL Service Catalog ITIL Incident Management ITIL Problem Management ITIL Change Management ITIL Configuration Management Database (CMDB)	OpManager Integration Applications Manager Integration MSP Center Lite Integration Desktop Central Integration

Figure 2-6. Service Desk Tool Suite Evaluation Criteria Topics. *A well-defined set of topics assists TEAM WDC is ensuring we have made a thorough evaluation.*

TEAM WDC's technical staff also will conduct a Strengths and Weaknesses analysis of all products evaluated. In addition, we will provide a Service Desk Features Checklist to ensure we have captured all the required features TCJ6 must have in a service desk tool. Notional samples (at the high level and not all inclusive) of the types of features we expect to assess are in our checklist are shown in Figure **2-7**.

Service Desk Features Checklist	
• General Features • ITIL Standards Support • Call Tracking/Request Management • Service Catalog • Incident Management • Self Service • Knowledge Management • Problem Management • Systems Requirements- - Operating systems, databases, and browsers supported • Pricing • Trial software versions	• Change Management • Asset Management • SLA Management • Purchase Management • Reporting • Survey Generation • Integration of API, eMail, remote control, telephony, and desktop central • Active Directory- import users, rights from AD, LDAP • Implementation- quick- easy implementation, no client software required documents database

Figure 2-7. *TEAM WDC* Service Desk Features Checklist. *TEAM WDC will measure each tool suite against a pre-determined set of criteria to ensure consistent evaluation across the board.*

2.2.2 Recommendation Phase

Once research is complete and our assessments and analyses are finalized, *TEAM WDC* will make our recommendation to TCJ6 based on our findings using our Product Alternative Analysis "Filtering" process. Recommendation will be based upon a definition of the investment, our analysis of the investment, and priorities associated with any given projects or programs. We will deliver our recommendation no later than 31 October 2011 and will make recommendations to key TCJ6 technical staff (including TCJ6 PM, TCJ6 Business Sponsor, and *TEAM WDC's* TM, Quality Assurance [QA] specialist, Security, and Application Developer).

2.2.3 Implementation Phase

A Service Desk tool suite implementation leads to changes which usually affect all core factors: people, technology, information, and processes. The Carnegie Mellon's Software Engineering Institute (SEI) analysis of software implementation projects indicates software implementations can fail, are often costly, and may not meet schedule timelines. These findings stress that management support is critical to project success. Therefore, our Service Desk Tool Suite Implementation Team will use the Task Review Board (TRB) process described in Proposal Section 2.7.4.8, Task 8: Project and Program Management, to engage TCJ6 management and *TEAM WDC* in a working group forum. (b)(4)

(b)(4)

(b)(4) This Implementation Project Plan will be a subject of discussion at TRB and our other meetings. The decision to implement the Service Desk tool suite will be treated as a strategic business decision supported by the management, stakeholders, and IT staff.

(b)(4)

Figure 2-8.

TEAM WDC, with government concurrence, will establish (at no additional cost to the government) the (b)(4) – a collection of product research material and documents used to implement the selected Service Desk tool suite. The (b)(4) stores

and archives research documentation in different formats (e.g., guidebooks, tool suite references material, presentations, demonstration results, white papers, etc.). The (b)(4) is the place to house specific information about the transition to the new Service Desk tool suite, and provides awareness for the end-user and helps to reduce the learning curve associated with implementation. The components of the (b)(4) are shown in Figure **2-9**.

(b)(4)

Figure 2-9. (b)(4)

(b)(4)

Through the use of a checklist during implementation, we will ensure *TEAM WDC* and TCJ6 management are engaged at every step in the process. Figure **2-10** depicts a Sample Implementation Checklist used to ensure the recommended tool is integrated into the TCJ6 enterprise smoothly.

Implementation Checklist for Introducing a Service Desk Tool for TCJ6			
Identifier	**What**	**When**	**Who**
1	Decide who will be your Service Desk users	TBD	TBD
2	Decide on which type of Service Desk to introduce	TBD	TBD
3	Decide on who will staff the Service Desk	TBD	TBD
4	Decide where the Service Desk will be located	TBD	TBD
5	Decide which additional furniture or equipment is required	TBD	TBD
6	Obtain the additional furniture or equipment	TBD	TBD
7	Decide how incidents and requests will be logged	TBD	TBD
8	Decide how incidents and requests will be passed to technical support staff	TBD	TBD
9	Decide how resolutions will be written up and recorded	TBD	TBD
10	Decide who carries out follow up actions and how that will be done	TBD	TBD
11	Decide on the review process	TBD	TBD
12	Create an incident / request sheet	TBD	TBD
13	Create a Service Desk Call log	TBD	TBD
14	Create the review forms	TBD	TBD

15	Create training materials for users on how the Service Desk will operate	TBD	TBD
16	Decide how to keep staff informed	TBD	TBD
17	Plan your first communication about the Service Desk to the school	TBD	TBD
18	Prepare a pilot group to run for approximate 1 month	TBD	TBD
19	Carry out the pilot and pilot review	TBD	TBD
20	Feedback changes into the system from the pilot review	TBD	TBD
21	Plan the launch date of the Service Desk	TBD	TBD
22	Ensure enough of the incident / request forms are available	TBD	TBD
23	Test any computerized systems from each PC they are available on	TBD	TBD
24	Train the users and Service Desk support staff	TBD	TBD
25	Train the staff providing technical support on how the process works	TBD	TBD
26	Launch the service desk	TBD	TBD
27	Carry out the first review and feedback to all	TBD	TBD

Figure 2-10. *TEAM WDC's* Sample Checklist for Implementing a Recommended Service Desk Tool Suite. *Through the use of a checklist during implementation, we will ensure TEAM WDC and TCJ6 management are engaged at every step in the process.*

Our implementation process provides TCJ6 a low-risk approach embedded with industry best practices (PMI, ITILv3, DoD's Alternatives of Analysis Product vetting model, Total Cost of Ownership, Benefit Cost Analysis, ROI models, and Business Process Improvement Gap Analysis), leading market research access to the Gartner Group, and innovative solutions (i.e., The Knowledge Corner). TCJ6's benefits from our detail approach because:

- Deliverables will be well defined
- Technical pre-requisites will be well documented
- Our delivery process is easily understood and a process for stakeholder involvement exists
- Our process is designed to meet TCJ6's systems specifications
- We introduce mechanisms to document and communicate outcomes to key TCJ6 participants
- We have introduced an approach which manages and controls change
- Issues are logged, tracked and acted upon
- Our deployment solution is controlled (phased) and risk balanced
- Knowledge is shared and reused

2.3 COMSEC MANAGER AND CRO DUTIES (PWS 1.3.7.2, 1.3.9.5)

TEAM WDC Significant Strength: Knowledge and experience to conduct and generate a USTRANSCOM security training program that encompasses team and individual roles and responsibilities for Communications Security.
Customer Benefit: Security Aware workforce as it relates to USTRANSCOM mission.

TEAM WDC's approach to COMSEC resonates with USTRANSCOM's reputation of providing a security conscientious staff to guide its Distribution Process Owner Mission to success. *TEAM WDC* will provide on-site COMSEC operations support and oversight to USTRANSCOM and its

sub-accounts. This includes 24/7 COMSEC support (which includes exercises, contingencies, and emergencies) as requested by the Government. We adhere to the underlying premise of COMSEC to deny unauthorized individuals information derived from telecommunications and to ensure the authenticity of such telecommunications. Our COMSEC Responsible Officer (CRO) is fully trained and will accept oversight responsibility for maintaining, monitoring, handling, protecting, and controlling USTRANSCOM's communications security program. These responsibilities include: Tactical Local Area Network (TACLANE), secure voice capabilities, secure telephones, secure mobile telephones, secure facsimile machines, and cryptographic secure voice keys, training to users (e.g., safeguarding, controlling, and destruction of COMSEC aids), and records maintenance for secure voice instruments throughout the command. As discussed below in Proposal Section 2.4.3.2, Classified VTC Support, we will designate a primary and alternate CRO to manage all COMSEC material necessary for classified AV/VTC communication encryption within the AV/VTC support team. The nature and importance of securing COMSEC requires expedient dissemination of urgent information. We coordinate and collaborate with both Lackland and Scott AFB points of contact to ensure all parties involved are aware and abreast of current advisories. The specific areas of responsibility fall into accountability, operations, and user assistance.

2.3.1 Accountability

Accountability begins with maintaining accurate lists of all persons authorized access to COMSEC holdings and ensuring proper logging occurs. Our CRO (and his alternate) is trained to use, control, and store COMSEC material, as well as conducting audits and inventories of all user's accounting legend codes (ALC) -1 and ALC -2 COMSEC material control system holdings. Annually, we review the COMSEC material requirements for validity and review requests of any new required materials from managers. This activity requires managing a Cryptographic COMSEC Equipment Account (CCEA); therefore, our CRO serves as the CCEA Custodian with Standard Base Supply System (SBSS) at Scott Air Force Base (SAFB). Upon receipt of COMSEC materials, our CRO takes responsibility for the handling, use and safeguarding of materials until they are destroyed or returned to the appropriate COMSEC account. We setup necessary controls to deny unauthorized access by complying with applicable storage procedures for material and equipment. The nature and importance of securing COMSEC requires expedient dissemination of urgent information. We will coordinate and collaborate with both Lackland and Scott AFB points of contact to assure all parties involved are aware and abreast of current advisories.

The CRO conducts monthly inspections of USTRANSCOM users to ensure compliance with inventory policies and locally developed operating instructions (OI). Items of interest are the proper documentation of Air Force Communications Security (AFCOMSEC) Form 16 to record daily, shift, or other local inventories. During these inspections, the CRO reviews the authorized access list for accuracy and annotates by dating and signing the list. Semiannually, we participate in COMSEC functional reviews with the COMSEC manager either at scheduled times or on an ad-hoc basis to validate USTRANSCOM COMSEC material is properly received, controlled, handled, safeguarded, stored and destroyed per current directives.

Not all material is in direct control of the CRO and not all accounts are incident free. Our trained CRO activates the procedures required when any known or suspected compromise of COMSEC material is reported. We emphasize to the users the importance of reporting any known,

suspected or possible compromised COMSEC material to ensure the integrity of our national security. After receiving notification from a user, a preliminary investigation is conducted immediately to determine the severity and reportable incident category. Types of reportable incidents fall into three categories; physical, personnel or cryptographic. The CRO will assist in preparing and submitting the initial incident report and assisting external agency throughout the process until resolved.

2.3.2 Operations

On **Day 1**, our CRO reviews the current COMSEC OI, begins the update process, and evaluates for compliance with updated COMSEC instructions, policy, or guidance from the COMSEC Manager. We ensure the OI contains provisions for securely conducting COMSEC operations and for safeguarding COMSEC material. Some of the key points during the evaluation are to ensure USTRANSCOM specific procedures and instructions are addressed for USTRANSCOM, the TCCs, and other direct reporting elements to include all sub-accounts. We validate the OI adequately addresses procedures for cryptographic operations, local accountability for COMSEC material, COMSEC maintenance support, access restriction, storage, routine and emergency destruction, incident reporting, and procedures for relieving individuals from accountability once they are reassigned. Our CRO serves as a Special Security Representative (SSR) for USTRANSCOM Sensitive Compartmented Information Facilities (SCIFs) and ensures compliance with SSR governing directives applicable to a SCIF. We are ready to assist the Special Security Officer in security management, operation, implementation, use and dissemination of all Communications Intelligence and other types of SCI material within the command.

Critical to the success of a sound COMSEC program is the daily security checks. The CRO uses a checklist to ensure or perform daily checks at the end of each workday and at the beginning of each shift for accounts with 24-hour operations. These checks ensure proper safeguarding of all classified COMSEC material. Activities associated with each check are the operational status of all physical security systems or devices such as door locks, vent covers and any other potential entry. Periodically, we verify alarms as operational with Security Forces and record the test on an All Purpose Checklist or Master Station Log (tailored to each project) to gain confidence that unattended material is secure. Every 30 days we perform inspections on any of USTRANSCOM Continuity of Operations (COOP) sites to confirm integrity and to eradicate superseded or extraneous inventory.

COOP sites allow the mission to continue, but events (accidental or hostile) leading to activation of a COOP present another set of issues for the handling of COMSEC material. It is imperative that everyone involved with COMSEC is aware that emergencies have the potential to compromise or create a loss of COMSEC material. We will review USTRANSCOM existing emergency action plans to ensure they address activities required for precautionary actions, destruction methods and procedures, destruction priorities, and necessary reports required in an event. Execution of any plan requires every individual to understand and carry out their responsibility to harmonize as a team. As part of our approach, we exercise our emergency action plan quarterly and evaluate responses, conduct after action analysis and re-accomplish training if required to assure everyone reacts together as a cohesive unit.

Ancillary operational support includes assuring USTRANSCOM Joint Exercise, Training, and Readiness is capable of successfully conducting realistic applications through real world communications. We provide COMSEC support from initial planning to after action reviews

and when required publish annexes and integrate with USTRANSCOM Inter-Theater COMSEC Package program for support to Contingency and Operation Plans. During real world missions, timely, accurate communications are critical to exchange information and transmit directions during a crisis. We understand the urgency and will be USTRANSCOM's COMSEC point of contact on the Crisis Action Team assuring oral transmission or video teleconferencing or telecommunications are capable of going secure. Practicing operations security applies to all in order to protect military operations, capabilities, limitations, intentions, personnel, and programs from our adversaries. We will assist with the development of USTRANSCOM's critical information list as part of the Information Operations Planning Cell so all work areas understands the information they possess requires secure means of communication.

2.3.3 User Assistance

The purpose for establishing a COMSEC account is to support the end users. *TEAM WDC*'s CRO and alternates prepare these users in the rules for safeguarding, controlling, and proper destruction of COMSEC aids. . No matter how flawless our processes, the ultimate success or failure of the COMSEC program rests with the material's end users. To this point, we make it our mission to provide the knowledge and direction so users are afforded the opportunity to succeed. An irresponsible user or the user who fails to follow procedures for using, safeguarding, and destroying COMSEC material defeats all security efforts. COMSEC users must make sure that anyone who receives materials has authorization; therefore, we provide users' instructions on how to determine authorized users and whether these users have received instruction on proper handling procedures.

TEAM WDC's experience in COMSEC has uncovered a false notion that COMSEC only applies to cryptographic security, and the other three areas used to prevent unauthorized persons from obtaining information of intelligence value and/or gaining access to critical operations is overlooked. Users must practice all four elements, transmission, cryptographic, physical and emissions security to ensure reliable and consistent protection. We will assist in the development of a comprehensive COMSEC Education, Training, and Awareness (ETA) program to educate USTRANSCOM on communications security. *TEAM WDC* has provided clients with security awareness and training support since the early 1980s. We have developed successful training solutions supporting regulatory, role-based, performance, or mission-essential task requirements spanning civilian and defense agencies, including US Government Accountability Office (GAO), Department of the Interior (DOI), Department of Labor (DOL), Treasury, the US Geological Survey, the Naval Sea Command, and the US Missile Defense Agency. *TEAM WDC* has

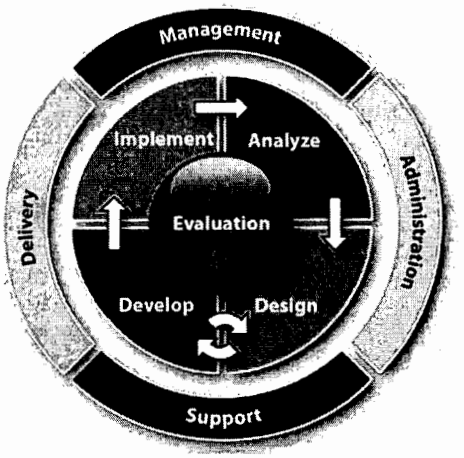


Figure 2-11. *TEAM WDC uses the industry standard Instructional Systems Development process to create instructionally valid, yet cost-effective, consistent solutions.*

experience developing security-related training for DoD personnel, ranging from general to policy-specific in nature. We can tailor our curriculum/courses to the USTRANSCOM-specific requirements upon request.

As depicted in Figure **2-11**, we deploy an instructional system design method consisting of a 5-Step process. The analyze step determines current security knowledge level and relevant training. During program design, we will work with USTRANSCOM to define learning objectives, specify training media generate the syllabi, and specify individual lesson designs. The develop step builds on the learning objectives through diagrams and outlines to identify necessary activities. Program implementation entails deployment of the training program via USTRANSCOM's preferred environment (e.g., briefing, intranet, CD, or individual training). Finally, evaluation is ongoing during all phases of course development to assist in review and improvement of the training program. Our team provides the focal subject matter expertise for Electronic Key Management System (EKMS) Local Management Device (LMD)/ Key Processor (KP) for the generation of electronic cryptographic keys. Troubleshooting key loaders requires having a knowledgeable support element to check fill cables, readers, and other crypto devices allows the user receive local assistance for quick resolution. *TEAM WDC* is prepared to assume the partnering role and join USTRANSCOM in securing its mission.

2.4 AUDIOVISUAL AND VIDEO TELECONFERENCING SUPPORT (PWS 1.3.9.1, 1.3.9.2)

***TEAM WDC* Significant Strength:** **Providing enhancements to operator level instructions, implementation of an AV/VTC knowledge database and additional VTC support training for Tandberg users.**
Customer Benefit: **Ensures proactive, customer-centric, mission focused AV/VTC support to improve communications, process efficiency, and user satisfaction.**

TEAM WDC has the expertise and skills to effectively manage, deploy, and securely sustain USTRANSCOM's AV and VTC Systems by implementing our process-oriented AV/VTC methodology designed to optimize efficiencies. We have proven AV/VTC experience and our extensive capabilities are reflected through our current work supporting the Army National Guard's Enterprise Network (ARNG). Since 2001, our partner, SRA, operates and maintains a 24/7/365 ITIL-based Video Operations Center (VOC) similar to the scope and magnitude of DISA's Defense Information Systems Network (DISN) Video Services (DVS). The ARNG employs a large-scale distance learning footprint that consists of multiple strategically dispersed bridging hubs, 330+ state of the art/VTC-ready classrooms, 60 PolyCom MGC-50/100 multipoint control units (MCU), and over 1500 VTC systems of various manufactures to include Tandberg, Polycom, Cisco and Sony. The VOC operates, administers, and maintains collaborative services to include the scheduling of audio/video conferences for approximately 40,000 users within the United States, Hawaii, Alaska, Guam, Puerto Rico, and the Virgin Islands. In addition, the VOC provides operational instructions, technical guidance and maintenance support functions for classroom-based peripherals, fixed and portable VTC systems, H.323/H.320 network elements and associated secure and non-secure video teleconferencing equipment. *TEAM WDC* also has extensive experience with coordinating AV/VTC scheduling through our various USTRANSCOM projects (e.g., Exercises Support Contract, Critical Infrastructure Protection, etc).

TEAM WDC's technicians also provide VTC support for research scientists, Industry C-Level executives, leading researchers in academia, senior executives, General Officers, and Flags officers during technology demonstration conferences such as the Defense Advanced Research Projects Agency (DARPA) Challenge. Our AV/VTC technicians received the DARPA *Grand Challenge Medal* for excellence supporting DARPA's annual technology shoot-off. *TEAM WDC* improved collaboration across the DARPA enterprise by installing, operating, maintaining, and troubleshooting 24 conference rooms and A/V systems (e.g., A/V rack, LCD projectors, DVD/VCRs, Integrated Services Digital Network (ISDN) video teleconferencing equipment, plasma screens, smarts boards, laptops) for remote conferences and special events. At the Secretary of the Navy (SECNAV) (Pentagon-Washington, DC), our AV technicians schedule, operate, and maintain executive conference rooms in support of the US Navy Secretariat (i.e., including the Secretary of the Navy, all Under Secretary(ies) of the Navy, and the Deputy Undersecretary of the Navy, Business Operations & Transformation).

We know the importance of and are sensitive to the high demands of scheduling limited conferencing and collaboration resources among very highly positioned VIPs. We will regularly monitor and test all equipment to ensure that TCJ6 systems are fully operational and ready for use, and will consistently monitor the VTC sector to ensure that we leverage the latest collaborative tools and systems. Our visual information (VI) technicians will perform weekly systems checks as part of their standard AV/VI job duties. For TCJ6, our technicians will make recommendations for improvements and communicate deficiencies to maintenance vendors.

As depicted in our staffing chart, *TEAM WDC* will use trained Voice and Data Communication Specialists from our AV/VTC Team and Briefings and Display Team to support all AV and VTC requirements. All team members will be Defense Information System Network (DISN) Video Services (DVS) VTC Non-Resident Phase Facilitator certified. Our AV/VTC Team will be matrixed and cross trained to provide VTC core team manning from 0430-2200 Monday through Friday and to provide Briefing and Display System support for the Fusion Center from 0430 to 1900 Monday through Friday. To accommodate working hours, one individual from our team will support the early shift between 0430 – 1230 for all early morning VTC's, and another technician will work from 1200 to 2000 or until the last VTC of the day is complete if after 2000. All other core team members will be available for support between 0730 and 1630. Our staffing plan also considers that AV and Briefings and Display personnel may be required outside of these hours to support unscheduled or short-notice requirements during weekdays and weekends. We will provide our team lead with the Mobile Command Post (MCP) (see Proposal Section 2.6.2, On-Call Staffing Approach) on a rotated schedule between contract task leads. Our MCP contains an on-call cell phone, a laptop with 24/7 Rapid Response software, a technician assignment matrix, pre-determined response options, important person contact list, and escalation procedures. Our team approach will utilize our 24/7 support "Mobile Command Post" including an AV/VTC SOP detailing key support activities to ensure timely receipt, management, and resolution of requests. We will assign team members to respond during non-duty hours based on our on call schedule.

Figure **2-12** depicts our three-tiered approach for the operations and maintenance support of USTRANSCOM's AV and VTC systems: (1) Support (2) Monitoring and Maintenance, and (3) Configuration and Administration. Our approach encompasses an IT Infrastructure Library

(ITIL) approach using DoD best practices and *TEAM WDC* lessons learned through our extensive AV/VTC experience.

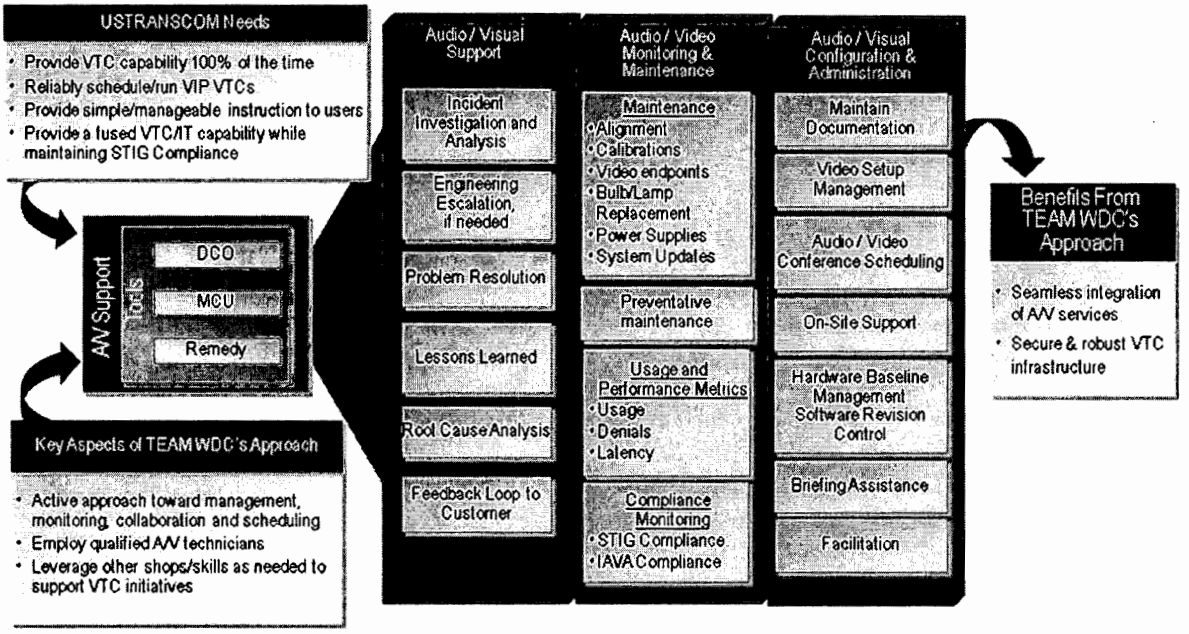


Figure 2-12. Audio/Visual Approach. *TEAM WDC's AV/VTC Approach provides seamless integration of A/V services and a secure and robust VTC infrastructure.*

2.4.1 AV / VTC Problem Support

Our problem support process begins with initial contact from a user requiring AV or VTC services. Our AV/VTC shop begins an analysis on the issue. Analysis begins with researching our knowledge database for similar issues and actions taken for resolution. Upon analysis results, the team will provide on-site first-line troubleshooting of the problem, which may consist of equipment repair or replacement. If during analysis it is determined that the issue needs escalation, our team will coordinate with the point of contact (e.g. vendor) for resolution. An example of this would be when a specialized part under manufacturer warranty requires replacement. Upon resolution, our team provides feedback of the results to the user. Additionally, our team stores any lessons learned in a knowledge database for future reference. This allows for efficiencies when a repeat occurrence happens in the future. Our AV/VTC team also performs a root cause analysis to determine if there are any underlying issues to prevent future problem recurrence. This analysis is an iterative process that provides continuous process improvement and a proactive approach in solving issues.

2.4.2 AV / VTC Monitoring & Maintenance Support

2.4.2.1 Preventative Maintenance

The second tier of our AV/VTC approach includes the maintenance and support for all AV/VTC systems. Our AV/VTC team will ensure that all equipment is functional and readily available for USTRANSCOM meetings and VTCs. We perform preventative maintenance inspections as prescribed by the equipment manufacturer and will establish a timeline and schedule as agreed to

by the Government. Preventative maintenance on the AV and VTC equipment eliminates surprises and any added expenses that result from unexpected downtime. Our preventative maintenance support includes at a minimum, cleaning, adjusting, aligning, and checking all functions of each component within the system. We remove and clean all equipment as prescribed by the manufacturer's recommendations and replace the bulbs or LCD lamps as required. Examples of such equipment repair during preventative maintenance may also include:

- Replacement of project lamps, external fuses, batteries, video and audio tape, software, accessories, wiring, connectors, etc.
- Equipment alignments, calibrations, and system/firmware updates

During preventative maintenance, we also verify the operation of the system as a whole and make any minor adjustments as necessary. If any major adjustments are required, we will schedule the required downtime to complete maintenance activity upon approval of the Government. Depending on the nature of the issue, we would also provide a temporary working solution to minimize the impact to the user community. Upon completion of the repair, we reinstall the equipment and ensure it is working properly. We will serve as the focal point for any repairs that are beyond in-house capabilities and will function as the liaison for interfacing with equipment manufacturers and other 3rd party organizations. If it is determined that replacement for equipment is required, we will replace with equipment that is kept in our inventory storage or contact the manufacturer for any specialized component. We will also track our equipment inventory levels and coordinate with the manufacturer for restocking to reduce any unexpected downtime.

2.4.2.2 Usage and Performance Metrics

TEAM WDC will execute, track, and archive Call Detail Reports (CDR) which provide usage and performance metrics on a monthly and annual basis. The CDR captures VTC usage by the time of day and by the number of VTCs per hour per day. In addition, the CDR provides metrics for denials due to personnel and room shortage per hour of the day. Each of our metrics can be traced directly back to a VTC request through our knowledge database. *TEAM WDC* will ensure that monthly CDRs are provided to the government no later than the 5th business day of the following month and annual metrics will be provided no later than the 10th business day of January for each period of performance.

2.4.3 AV/VTC Configuration and Administration Support

In the third tier of our approach, our AV/VTC Team will provide configuration and administration support for USTRANSCOM. *TEAM WDC* will ensure that all AV/VTC related operational documents, SOPs, and associated job aids are current and properly maintained through industry's best practice version control processes. In addition, we will document and publish operator level instructions for USTRANSCOM AV systems within 20 business days of any changes or upgrades that may have occurred. *TEAM WDC* will provide hand-on operational training and problem resolution assistance for all USTRANSCOM AV/VTC related equipment and AV customers as needed. Our Team will schedule, administer, and monitor VTC conferences for hosted events and will resolve VTC studio scheduling conflicts by position or rank of the requiring authority. The AV/VTC Team will document and maintain a stringent configuration baseline archive that captures the configuration profile of all AV/VTC components to include firmware revisions, set-up profiles and associate end-user equipment configurations.

The asset configuration archive will be administered, hosted and sustained within the knowledge base platform.

2.4.3.1 On-Site AV and VTC Support

Our VTC support encompasses point-to-point and multi-point conferencing with audio and video capability in both a secure and non-secure mode. We will support AV equipment checkout for limited overheads, projectors, screens, etc. Our AV/VTC on-site support will provide 100% briefing assistance for all USTRANSCOM Commander (TCCC), USTRANSCOM Deputy Commander (TCDC), and USTRANSCOM Chief of Staff (TCCS) attended briefing events at Scott Air Force Base. Additionally, we will provide on-site AV support and briefing assistance for all events in the Seay Auditorium and Heritage Hall video wall. One individual from our team will be designated for support to the Seay Auditorium with a backup as needed. For unclassified VTC support, we will utilize the portable VTC units (1961 and 1900E).

2.4.3.2 Classified VTC Support

Classified VTC Support is limited to Room 261, the Balcony, the Honor Hall, Room 2093, Room 2064, and the J6-MR. We will designate a primary and alternate CRO to manage all COMSEC material necessary for classified AV/VTC communication encryption within the AV/VTC support team. Prior to conducting a classified VTC, our AV/VTC Team will proactively conduct a system check of components to include the codec, IMUX, camera, and the audio system to ensure they are fully operational and ready for use. All members of the AV/VTC team will have clearances at the Secret level as required in the PWS and per National Industrial Security Program Operating Manual (NISPOM) contractual requirements. Prior to the classified meeting, our technician will provide a security administration instruction that reminds participants of the level of classified discussions. This allows participants to be mindful of the technician's clearance level prior to discussion at a higher classified level. In the event that at the conclusion of a classified VTC participants engage in discussions that are at the TS level, our technicians will leave the room. *TEAM WDC* will be prepared to upgrade any clearances if the Government deems necessary based on these situations.

2.4.4 Schedule Management

Our AV/VTC Team will function as the channel of communication for all scheduling management support. Our AV/VTC Team will receive initial requests via email, telephone or in person. Upon AV/VTC requests, we will provide a form to the requestor that includes the detailed information (e.g., date, state/end time, subject, classification, reserved room, host/participant, highest ranking participant, etc.) required for seamless VTC support. This form will also require the requestor to provide a functional point of contact (POC) and a VTC technician from each VTC location. As part of our knowledge database, we will keep a POC list of VTC technicians from different locations based on previous VTC support and provide this type of information to the requestor if needed. After review of the request form, we will then provide the requestor with confirmation of their reservation summarizing their request. All AV/VTC request information will be kept in our knowledge database and assigned to one of our AV/VTC technicians. Each morning, we will post an updated schedule of events for that day that includes the individual assigned to support, and any specialized technical requirements that may be required.

2.4.4.1 Resolve VTC Studio Schedule Conflicts

In the event of a scheduling conflict, our team will advise the requestors and begin to resolve through coordination among authorities. Additionally, resolution will be made by position or rank of the requiring authority.

2.4.5 Operational Training

Our AV/VTC Team will also provide instruction for users in accordance with the USTRANSCOM Instruction 33-7 publication. Instruction will include VTC participation professionalism, microphone operation and hazards, general VTC etiquette, and camera presence. Instructions will be provided to the VTC requestor with confirmation of the request and also posted within each of the conference rooms. Additionally, *TEAM WDC* will develop, maintain, and publish AV/VTC checklists and operator level instructions which provide a complete guide for a technician to operate the system. The guide will include step by step instructions, floor plans, diagrams, and screen shots to ensure ease of use at the novice technician level. We will update the guide within 20 business days of any system changes or upgrades.

We understand that the USTRANSCOM Tandberg units are becoming a more prevalent and efficient access to VTC support. As a value added to our customers, our AV/VTC Team will attend training by Tandberg (at no cost to the Government) and provide a checklist and quick reference guide to Tandberg users. We will also provide over-the-shoulder assistance, as needed. Our partner, SRA, is a certified Tandberg reseller; this inside channel provides an advantageous support vehicle from the manufacturer. In addition, it offers reach-back within the corporate support structure while leveraging a greater pool of internal resources and pricing discounts.

2.4.6 Server and Multipoint Control Unit (MCU) VTC Support

TEAM WDC will provide day-to-day operational and maintenance support functions of all managed AV/VTC components to include: VTC Multipoint Control Units (MCUs), network traversal system and VTC suite management platforms. Our AV/VTC Team will proactively manage core components and ensure that all peripherals are utilizing the latest firmware releases approved for DOD use. In addition, our AV/VTC Team will utilize best practice VTC techniques such as conference templates, auto-negotiation and video-switching to enhance the day to day support posture and overall user experience. All members of our AV/VTC Team supporting the Server and Multipoint Control Unit VTC Support functions will be DVS VTC Resident Phase Facilitator certified.

2.5 IMPLEMENTATION

TEAM WDC Significant Strength: _TEAM WDC_ has introduced Critical Success Factors, Risk Mitigation approaches, and a seasoned Implementation Team to strengthen its Implementation Planning process
Customer Benefit: Eliminates any degradation of service during cutover, resulting in rapid assumption of program responsibilities which reduces overall operational risk for TCJ6.

A successful implementation depends on communication, cooperation, and collaboration within our team and among transitioning parties. We understand that contract transition can be a period of significant risk to TCJ6, and have addressed these risks in Proposal Section 2.5.3., Our proposed Implementation Manager (IM) also minimizes risk by leveraging his considerable experience in transitioning large IT programs in the US Navy and the Department of State. The following proposal subsections detail our Implementation Plan for TCJ6, including details about

our proposed Implementation Team, activities associated with our three-phased Implementation Methodology, and a detailed analysis of the risks associated with implementation of a project of this size and scope.

2.5.1 Implementation Team

We have formed a structured Implementation Team that will work together to ensure "business as usual" during contract implementation. *TEAM WDC's* Implementation Team will consist of a staff of experts in human resources, security, quality assurance, engineering, and technical support services, including members of our established Program Management Office (PMO). Our dedicated Implementation Team will perform all aspects of the transition and facilitate communications across all levels throughout the implementation lifecycle. Roles and responsibilities of the members of our Implementation Team are outlined in Figure **2-13**.

Implementation Team	
Role	**Responsibilities**
Implementation Manager (IM)	• Initiate immediate and continuous communication with TCJ6 leadership critical incumbents • Nurture critical staff relationships • Identify, plan, and coordinate critical transition activities early (tasks, workload, security, etc.) • Meet weekly with TCJ6 leadership to review and measure progress • Develop and present draft Implementation Plan to the TCJ6 CSS: SS Task Manager, Contracting Officer (CO), and Contracting Officer's Representative (COR) immediately upon contract award for review and approval before proceeding with implementation activities. • Define customer-required deliverables, in-process tasks, and TCJ6 priority projects and services at kick-off • Deliver the employee roster, on-call roster, and kick-off minutes
Human Resources Manager	• Coordinate and schedule recruiting activities to include job fairs, identification of key incumbent personnel, and identification of other qualified candidates for hire • Establish employee certification date database
PMO Support	• Provides back office support to the TM. Supports TM in support of government budget, finance, quality assurance, and programmatic issues.
Security Manager	• Process security documentation (clearance initiation) • Identify security training requirements and coordinate training activities

Figure 2-13. *TEAM WDC* Implementation Team. *Our team of qualified professionals is in place today and working to ensure successful transition on* ***Day 1.***

2.5.2 Implementation Methodology

TEAM WDC HAS A STRONG RECORD OF SUCCESSFUL TRANSITION
• **WDC- Department of the Navy, Office of Information Technology DON/AA, ITD SECNAV:** Ramped up staffing from zero to 32 FTE in less than 1 week. Developed task issuance process and established Task Review Board to expediate senior management prioirty tasks during implementation phase.
• **WDC- Defense Advanced Research Projects Agency (DARPA):** Instrumental in staffing emergency ramp up of cyber/IA support personnel to thwart "state-sponsored " attack on the agency.
• **SRA- Advanced Information Technology Services (AITS)** for US Army PEO EIS: Completed transition of system sustainment and deployment activities from incumbent for worldwide support of more than 40,000 users.
• **SRA- Military Sealift Command (MSC) Afloat Information Technology Operations Support:** Staffed project with more than 100 personnel within three weeks to support worldwide operations.
• **SRA- Army National Guard Enterprise Network Support (GuardNet XXI):** Completed transition from incumbent 10 days early with no degradation of service to support responses to September 11, 2001 attacks.
• **SRA- Puget Sound Naval Shipyard:** Delivered seamless IT support to 6,500 users after previous incumbents walked off job.
• **SRA- U.S. Agency for International Development (USAID) Principal Resource for Information Management Enterprise-Wide (PRIME 2.2):** Transitioned 6,000 users across more than 90 locations worldwide with no loss of service. Staffed more than 160 cleared personnel in 60 days during the Thanksgiving through New Year holiday season.

TEAM WDC has a long history successfully transitioning large, complex IT projects with seamless and no degradation of performance levels as shown in the table above. Our implementation methodology is based upon a **Day 1** "do no harm" approach— meaning we will ensure that there is no degradation to the mission and no interruption to mission critical services. We will develop a detailed event dependencies chart and a revised work breakdown structure to ensure we have considered current operational conditions. Proposal Section 2.7.2, Schedule describes how the TM will develop this deliverable. The benefits of *TEAM WDC's* implementation methodology are characterized by:

- Experience in executing seamless transition plans – promoting operational excellence
- The identification of Critical Success Factors – targeting implementation critical path milestones and interdependencies
- Risk mitigation that addresses potential problems and provides fallback scenarios – reducing programmatic and operational impediments
- A team with extensive experience partnering with USTRANSCOM – customer intimacy fosters smooth and seamless implementation
- Cross leveled staffing plan (i.e., supporting functionality and skills) that mitigates and prevents interruption in services. A Most Efficient Organization (MEO) model provides TCJ6 an optimal, cost effective staffing plan

Our methodology consists of three phases: (1) Pre-Award, (2) Post-Award, and (3) Contract Start-Up. Figure **2-14** depicts the *TEAM WDC* implementation recruiting process.

TEAM WDC Implementation Recruiting Process	
Identify Candidates	Based on our proposal staffing plan, we identify candidates based on internal contractor personnel we will assign to the project, selected incumbent contractor personnel, qualified personnel identified through our supporting staff provider (TEKsystems) and through job fairs.
Review Resumes	Resumes from potential candidates are reviewed to ensure they possess the appropriate education, skills sets, certification and qualifications, security clearance, and experience to perform in the specified labor category.
Open House	*TEAM WDC* will hold an open house to speak with key personnel and other candidates about team benefits, discuss their skills and capabilities, and familiarize them with our procedures. *TEAM WDC's* principals will determine where the best fit for positions is among the Team. The decisions will be based on providing the best skills and core competency

(b)(4)

Figure (b)(4)

(b)(4)

2.5.2.1 Pre-Award Activities

A successful transition begins now. *TEAM WDC* is already in the process of completing several activities associated with successful and seamless contract transition, as described in Figure **2-15**.

(b)(4)

Figure 2-15. (b)(4)

(b)(4)

To ensure continuity of operations, we will continue to implement our established recruiting plan. A key activity within our pre-award phase is the identification of qualified candidates. Through our approach, we are focused on filling positions with qualified candidates prior to contract award. We look for these qualified candidates both internally and externally and provide contingent offers, once the right candidates are identified. Our IM will perform a detailed analysis to identify skill requirements, organizational sourcing, and validate qualified personnel required for **Day 1** implementation. *TEAM WDC* follows a detailed process to vett candidates. This process is shown in Figure **2-16**.

To supplement this process we use a number of additional recruiting methods, including employee referrals, job fairs, customer recommendations of key contract incumbents, and TEKsystems staffing agency in St. Louis, Missouri. TEKsystems is a subcontractor to WDC on the NMCI contract and also supports SRA's external recruiting. TEKsystems is the nation's largest technology staffing services firm with offices in over 90 cities and over 20,000 consultants on staff. Their St. Louis office regularly provides our partner, SRA's local office, with temp to perm staffing support for USTRANSCOM, SDDC, and Air Mobility Command (AMC) projects.

Candidates are also recruited through our corporate websites, www.websterdata.com and www.sra.com, and external internet job services such as Monster, LinkedIn, Dice, Clearance Jobs, and others. *TEAM WDC's* participation in industry organizations and professional associations provides additional sources. Our knowledge of the current St. Louis metro-area labor market, our involvement with the USTRANSCOM community, and our superior reputation within the local Scott Air Force Base area also assist in attracting qualified personnel to meet

task requirements. Our Implementation Team will also build on the implementation activities described below to develop a more detailed implementation and task order management plan.

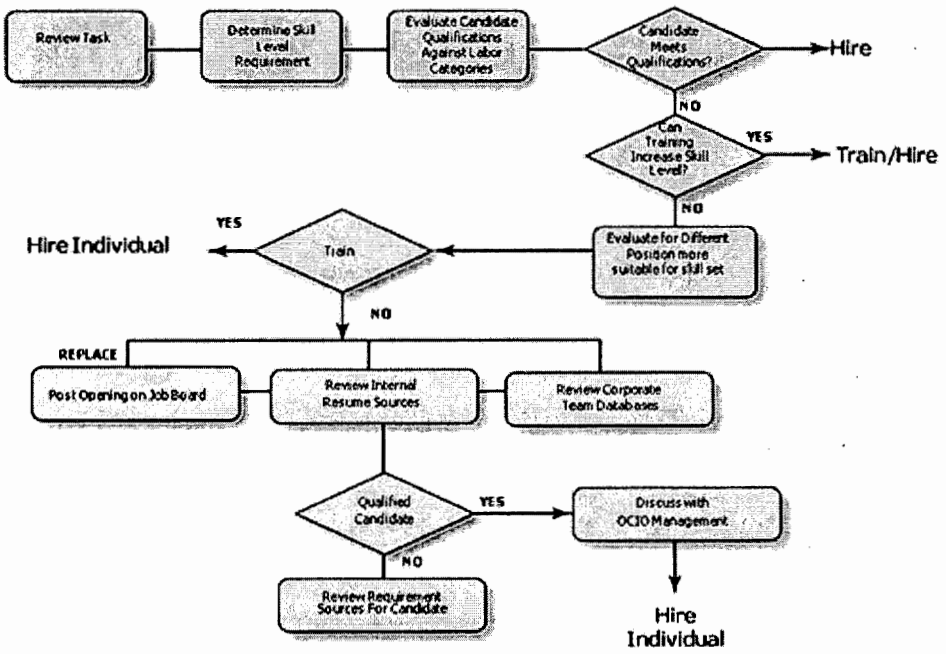


Figure 2-16: Personnel Vetting Model. *A well-defined personnel vetting procedure ensures standards are managed and upheld in the recruiting process.*

2.5.2.2 Post-Award Activities

The key to ensuring a mutual understanding of implementation goals, roles, schedule, and workflow management across all stakeholders is clear, consistent communication. Upon contract award, we will engage in a partnership with the Government and incumbent contractor to validate implementation activities and make necessary adjustments to ensure coordinated transition execution. Our goal is to immediately assess the organization's "As Is" state and then perform the activities identified in Figure **2-17**.

During this phase, our Implementation Team will conduct an initial kickoff meeting with the Contracting Officer Representative (COR) and incumbent contractor management to review the projected turnover of work, validate the scope, status, and milestones, and coordinate with POCs within the incumbent team for each task area. A key kickoff meeting activity is to review the transition plan and schedule with the Government. *TEAM WDC* will continue to manage and review the implementation Work Breakdown Schedule (WBS). We will use our implementation schedule to monitor and evaluate the integration process. During this phase, we will conduct daily, weekly, and ad-hoc implementation meetings between the incumbent contractor and the *TEAM WDC* Implementation Team to ensure continuity. For each task area, our Implementation Team will meet with the identified POCs of the incumbent staff or Government to review pertinent documentation and distill further details of current and other institutional knowledge. *TEAM WDC* will use this review to analyze current processes and procedures and determine potential areas for efficiencies. Any recommendations will be provided to the Government in an

Implementation After Action Report (AAR). During this phase, if required, we will continue our recruiting activities as discussed in paragraph 2.5.2.1.

Our security manager will begin the security process in coordination with recruiting and Human Resources (HR) and begin initiating clearances for those employees that need them immediately upon contract award. Our security team is extremely familiar with USTRANSCOM's policy for issuing common access cards (CACs) and line badges to only those with interim clearances that have an opened investigation. Our security manager will proactively work with Defense Industrial Security Clearance Office (DISCO) and expedite security clearances if needed. In addition to this, we will perform the activities outlined in Figure **2-17** following contract award.

(b)(4)

Figure 2-17. (b)(4)
(b)(4)

2.5.2.3 Contract Start-Up

Upon contract start on 1 October 2011, our team will be in place and ready to execute contract tasks. Members of our Implementation Team will remain on board to continue to ensure a seamless transition from implementation to execution. *TEAM WDC* knows that personnel issues will need immediate and undivided attention as successful Change Management is implemented. We will begin operations on **Day 1** with a staff composed of WDC and SRA employees that includes SRA incumbent personnel that are currently working on the J6 contract, and selected personnel that have left other incumbent contracts and joined the WDC Team. Our staffing plan (Proposal Section 2.6, Staffing) demonstrates how we map critical personnel to the WBS and the CLIN structure of the contract, and our personnel retention practices are described in Proposal Section 2.6.3, Personnel Retention Plan. The Implementation Team's objective is to ensure personnel are assigned based on a best athlete approach and that we retain the "best of the best".

2.5.3 Implementation Risks

Considering the factors critical to a successful implementation, we have developed risk mitigation plans to ensure any concerns that arise in the execution of the activities described above are addressed. The benefit of this approach is to give TCJ6 confidence that *TEAM WDC* has a framework in place to reduce any implementation risk normally associated with phasing in large IT enterprise programs. Our Risk Mitigation Framework is detailed in Figure **2-18**.

(b)(4)

(b)(4)

Figure 2-18: (b)(4)

(b)(4)

2.6 STAFFING

(b)(4)

(b)(4)

(b)(4)

2.6.1 Staffing Matrix

(b)(4)

2.6.2 On-Call Staffing Approach

(b)(4)

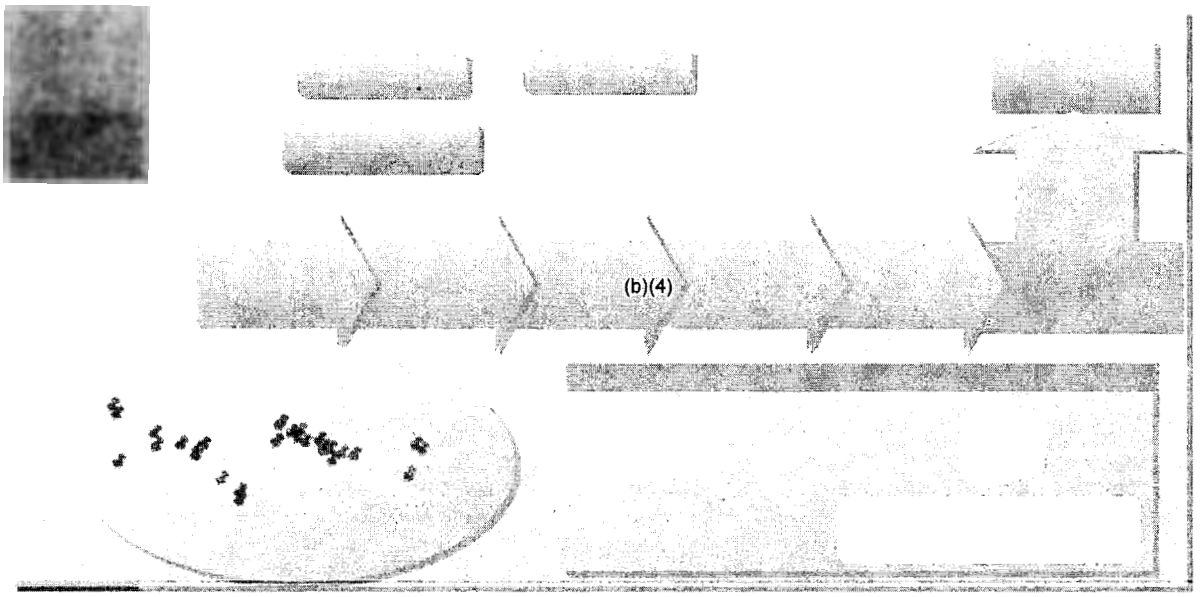


Figure 2-19. (b)(4)

(b)(4)

2.6.3 Personnel Retention Plan

TEAM WDC's retention plan is founded on established recruiting and retention initiatives designed to not only hire, but to retain highly skilled IT professionals. *TEAM WDC* has a successful record of retaining a professional workforce of dedicated IT professionals. WDC exceeds its DCAA Submission rates for fringe benefits to its employees to minimize turnover and ensure high retention rates. As an addition to the existing fringe benefits base, WDC will offer key TCJ6 incumbent staff "Stay Put" retention bonuses to incentivize employees and assure retention rates remain high throughout the contract period of performance. Team member SRA has long been considered an employer of choice within the Federal IT services provider market as evidenced by such awards as "100 Best Companies to Work For." These retention initiatives, coupled with SRA's accolades, make *TEAM WDC* an employer of choice. *TEAM WDC's* strategy for retaining staff is to hire staff aligned with their corporate culture, enable staff to use their expertise, and provide training and growth opportunities toward keeping staff challenged, as depicted in Figure **2-20**.

Figure 2-20. *TEAM WDC's core values are at the heart of our commitment to retain quality staff.*

As a part of our retention plan, WDC provides the necessary training to entice and challenge the technical intellect of our IT professionals. We recognize that it is important to place staff in positions suited to their interests and goals as well as their skill set. *TEAM WDC* works diligently to give their employees the opportunity to do work that is meaningful to them. We offer diverse career options to give staff the opportunity to grow in support of USTRANSCOM's mission. We also mentor staff and encourage them to expand their knowledge. We encourage our technical staff to gain certifications that will enhance their careers while benefiting the customer by delivering a higher level of service often resulting in operational improvements and higher productivity. For example, on our DARPA contract, our IT professionals exceeded DoD 8570 certification standards by attaining certifications in specific IT skills, in addition to the required IAT and IAM Level II/III certification, to enhance their service delivery to the customer. In another example, our C&A professionals on the DON/AA ITD program not only possess CISSPs but are also certified Certification & Accreditation Professionals (CAP). *TEAM WDC* will provide the same level of commitment to training and certification excellence as we demonstrate in our work at DARPA and SECNAV.

TEAM WDC employs a full complement of full-time technical recruiters who possess an in-depth understanding of job markets across the United States. To optimize retention, our technical recruiters use innovative recruiting methods such as social media and automated recruiting tool tools such as *Taleo*® to provide the flexibility and agility to recruit for highly-specialized positions. Taleo's® seven modules—*Recruiting*, *Talent Development*, *Sourcing*, *On Boarding*, *Compensation*, *Performance Reviews*, and *Succession*—enable our technical recruiters to manage the entire recruiting and retention lifecycle.

Retention through Stellar Benefits

WDC uses our existing robust benefits and compensation program as leverage to retain employees. We have learned that our benefits in many ways mirror the benefits program of companies much larger than WDC. WDC's salary and compensation packages are in line with several national salary surveys (i.e., Watson Wyatt, Western Management Group Salary, and the Society for Human Resource Management's [SHRM] 2010 Government Contractor Compensation Survey Report). These national surveys and reports validate that our benefits and compensation packages are consistent with and, in some cases better than, companies within our size standard. At DARPA, our retention rate consistently remained at 98 percent. To maximize retention and employee satisfaction, WDC offers a leading compensation plan consisting of salary, fringe benefits, performance bonuses, and awards. A typical *TEAM WDC* employee's benefits package includes paid time off, paid holidays, training, military reserve leave, jury/court

duty leave, a 401(k) plan, health, dental and vision insurance, short- and long-term disability and life insurance, as well as dependent care and medical flexible spending accounts. In addition to these standard benefits, WDC also provides the benefits outlined in Figure **2-21**.

Benefit	Description
Summer Gas Program	Summer is a time when we all drive more, but gas prices can be expensive. In the months of July and August, WDC reimburses our employees for two fill-ups per month.
PTO Buy-Back Program	WDC encourages all staff to use as much of their PTO as possible. However, if special circumstances do not allow an employee to use all of his/her earned vacation time, WDC offers to buy back unused paid time off (PTO) twice a year.
Company-Wide PTO pool	Life is unpredictable. Should an emergency arrive and a fellow employee has not accrued the sufficient amount of paid leave to take time off, we have an established Company-Wide PTO Pool. This collaboration allows any employee to donate their accrued PTO hours to the co-worker in need.
Worldwide Emergency Travel Assistance	Through our Emergency Travel Assistance program, employees and their families are provided with assistance in a travel emergency in a foreign country of 100 miles or more away from home.
Working Advantage® Corporate Discounts	All employees are immediately eligible to participate in our discount program provided through Working Advantage®. Working Advantage® is an online resource that provides up to 60% discounts to all members on tickets, travel, shopping, and more.
Supplemental Health Insurance	WDC offers its employees optional health insurance through Aflac. Major medical insurance pays for doctors and hospitals. Aflac is insurance for daily living. It pays cash benefits directly to policyholders, unless otherwise assigned, to help with daily expenses when they become sick or hurt.

Figure 2-21. WDC's Extensive Benefits Package. *We help to retain personnel by offering a comprehensive benefits package.*

Career Development Strategy for Retention

In addition to our benefits package, our program managers and supervisors conduct annual performance reviews and are required to develop a Career Development Strategy (Figure **2-22**) for each IT professional which prioritizes the employee's development needs, and lists suggested development actions to be taken over the next 12 months. Through our certification reimbursement program, we encourage our employees to continue their education. This further increases our retention rates by allowing employees to feel as though their future educational needs are taken care of.

PRIORITY	DEVELOPMENT NEEDS	SUGGESTED DEVELOPMENT ACTIONS	DATE RESULTS EXPECTED
High	CISSP Certification	Attend SANS CISSP course; take Prep Exam; Complete CISSP examination	4th Qtr 2011
High	Sec+ Training/Certification	Sign up for On line preparatory course work; Take Final Exam	3rd Qtr 2011

Figure 2-22. Career Development Strategy Chart. *Increasing retention through proactive career development strategies.*

TEAM WDC's subcontractor documents their personnel's goals and objectives in a Personal Development Plan (PDP). Employees meet with their supervisors on a semi-annual basis to discuss and document specific actions to help them achieve these goals. SRA also provides mentorship to help personnel develop soft skills like effective communication and personnel management. Diverse and thorough training opportunities are another component to develop their team's skills, expertise, and certifications.

2.6.4 DOD Directive 8570 Compliance

As 95% of our contracts are in DoD, we successfully operate in an environment in which it is necessary to recruit, train, and retain certified and cleared employees. *TEAM WDC* is dedicated to ensuring our personnel comply with all IA/DoD Directive 8570 requirements. We will utilize

a set of proven and disciplined methodologies, as described below, to ensure all USTRANSCOM DoD 8570 requirements are fully met. Upon award, we will ensure employees assigned to the IA positions within this contract are certified to the appropriate level prior to being engaged on the contract per DoD 8570.01-M. Compliance with the 8570.01-M directive begins during the recruiting process. Working as an integrated team, WDC and SRA maintain dedicated recruiting organizations to implement the necessary recruiting processes for our team to provide the most qualified resources. Our recruiting teams will ensure and verify education and certifications through the appropriate educational and technical certification institutions.

In addition to our dedicated recruiting teams, *TEAM WDC* uses *MindLeaders®*, an online training portal which enables us to comply with DoD 8570.01-M's computer certification training. Our employees receive training in security Network+, MCSE, MCSA, MCP, COMPTIA A+, N+, and CCNA. *MindLeaders®* gives our PMO an embedded training management module which provides course utilization reports that offers insight into student goals, motivations, and test results. We have visibility over which employees use the tool; the number of employees who have completed training; what courses were taken; the employee's mastery of the coursework (a visible grading system); and who is prepared for certification. WDC and SRA budget and provide reimbursement for our project managers and IT professionals to take their certification tests. We maintain operational excellence by ensuring our IT professionals are trained and certified. Individual Training Development (ITD) plans ensure all employees receive security training as required by the Defense Security Service. Our ITD plans encourage employees to enter into continuing education programs during the life of their certification. Based on the employee's certification expiration dates, the HR manager will notify the employee within a year advance of expiration to begin preparation for recertification. Our TM will continually work with the employees to ensure they are on track for recertification within three months of the expiration of their current certification.

TEAM WDC also offers a DoD 8570 Learning Resource Center that provides information on certification paths, certification prep programs, and continuing education FAQs. Individuals can access courses through our online library of prep training courses to help prepare for certification exams and also provide refresh for continuing education. Our teammate, SRA, has qualified instructors that will provide "just-in-time" certification training for *TEAM WDC* staff. The SRA Security+ Certification Boot Camp is a 5-day course that includes completion of the certification examination on the last day of class. The materials are developed and ready for distribution. The boot camp has a mobile test center activated and ready to go "on the road" with a certified proctor available to support mobile training/exams. All employees receive certification reimbursement under our Certification Assistance program. Our certification process will ensure 100% compliance with the DoD Directive 8570 requirements throughout the life of the CSS: SS contract. We reward outstanding performance through spot, annual, short-term, and long-term incentive bonuses.

2.6.5 Cyber Security Requirements

TEAM WDC, through our partner SRA, has established a comprehensive Cyber Security (CS) and Privacy Solutions (CS&PS) practice to provide DoD with CS IT capabilities including CS technical solutions, CS managerial expertise, CS enabling products, and professional services that ensure the availability, integrity, authentication, confidentiality, and non-repudiation of government Information Systems (IS). During the last ten years, SRA has established a long history of extensive CS and DIACAP experience with numerous DoD clients including the Army

National Guard Bureau, Defense Logistics Agency, Portsmouth Naval Yard, Pentagon Force Protection Agency, and the Missile Defense Agency and possesses a thorough understanding of the discipline that will enable effective support of this activity.

In addition to the IA support in Task Area 7, WDC and SRA will leverage their respective existing corporate security programs. Upon beginning work on this contract, all individuals assigned to *TEAM WDC* will possess at minimum a valid Secret clearance and will ensure that all personnel assigned to the project are appropriately cleared, authorized to work and abide by all applicable security requirements. *TEAM WDC* understands that we may have access to sensitive, non-public information during the performance of this contract, and agrees to comply with all requirements pertaining to the handling of non-public information identified in PWS Section 5.1. *TEAM WDC* assumes the following security requirements are applicable and will comply with the requirements identified in PWS Section 5.0, as required.

For the mandated security requirements for contractor provision of a security plan and IA controls, the CS Team will leverage and modify our existing IA program to implement and sustain appropriate IA management, operational, and technical controls and processes required to safeguard DOD non-public information resident on or transiting *TEAM WDC's* unclassified information systems from unauthorized access and disclosure and document this program in compliant security plan as part of a DIACAP package, if required. *TEAM WDC* will authorize periodic government inspections and reviews, to assure compliance with DOD IA requirements throughout the contract performance period, and will be responsible for taking corrective action based upon the impact and severity of identified weaknesses. We understand the DoD 8570.01-M IAWIP certification requirements, and how critical training, certification, and management of the DoD workforce conducting IA functions in assigned duty positions is to the overall security.

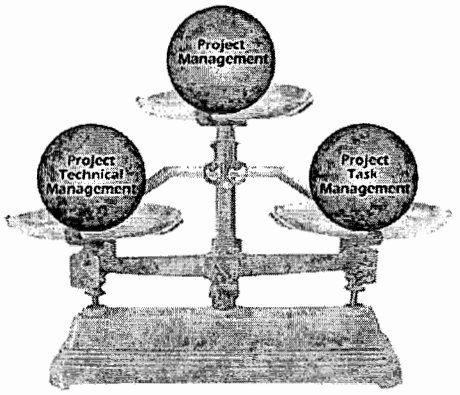
We will fill the government-designated IAT, IAM, and/or IA Workforce System Architecture and Engineering (IASAE) with appropriate personnel and be prepared to provide backup documentation of the certification status. *TEAM WDC* will comply with the security requirements regarding stated physical security, personnel security, information security, anti-terrorism/force protection, and industrial security requirements. We plan to accomplish meeting these requirements by leverage our existing corporate security program, policies, processes, and procedures and to locally modify them to meet any specific requirements in these areas.

TEAM WDC is prepared to support the optional security requirements after authorization from the government. For the remote access requirement, we will comply with the requirements that all contractor furnished equipment (CFE) employed for remote access to a Government network will meet equivalent Government furnished equipment (GFE) IA computing requirements. For detect, analyze, and respond requirements, we will comply with the identified requirements for incident response, reporting, submission, and, coordination. For law enforcement and counterintelligence requirements, *TEAM WDC* will comply with the identified requirements for contractor support of incident investigation. For information sharing requirements, we understand and will comply with the identified conditions for information sharing. For confidentiality and non-attribution statement requirements, *TEAM WDC* understands and will comply with the identified conditions for confidentiality and non-attribution of contractor provided information. For developer environment, MAC, and CL requirements, we understand that a development environment would be physically and logically isolated from other *TEAM WDC* networks which would be compliant with NIST SP 800-53 Revision 3 and documented

accordingly by the CS Team. For system design, information system security engineering (ISSE) principles requirements, we will comply with the identified requirements for ISSE and CM support. We are "Innovation Leaders" as shown by our authoring the upcoming "NSA Systems Security Engineering Process" document that is becoming a NIST SP providing the standard by with all other organizations will apply a strong process for building secure information systems. This sound Systems Security Engineering (SSE) process matches secure IT products with proven system architectural designs in order to protect the overall business/mission as part of a comprehensive risk management strategy, extending throughout the entire system development life cycle (SDLC). For DIACAP requirements, we will comply with the identified requirements for DIACAP including review and development of the applicable package. Our partner, SRA, has significant experience supporting DoD customers in the areas of expertise, and has helped more than 400 federal IT systems achieve C&A through the DIACAP and NIST-based processes. For software development related-tasks requirements, we understand and will comply with the identified requirements for software assurance and security engineering practices, non-secure software, malicious code warranty, and source code configuration control (versioning), as required. The CS Team will support these requirements by requesting and coordinating obtaining the appropriate staff by utilizing the our large, pool of CS SMEs with various types of "on demand" expertise such as IT contingency planning, specific technologies or software, and technology specific implementations that enhances our ability to deal with legacy or special or new platform environments or technologies quickly and cost-effectively.

2.7 TASK ORDER MANAGEMENT PLAN (TOMP)

Our task order management excellence starts with offering TCJ6 a high-performance team with a deep knowledge of the TCJ6 and USTRANSCOM IT environment. To complement the depth and breadth of WDC's capabilities, we have chosen SRA whose technical expertise and experience directly augments the quality of our team's depth of understanding of the requirements within the PWS.



- System Engineering Management
- Requirements Management
- Requirements Analysis
- Requirements Audit
- Interface Control
- Risk Management
- Performance Management
- Task Planning
- Cost Management
- Schedule Management
- Contracts Management
- Data Management
- Configuration Management
- Subcontractor Management
- Administrative Management
- Security

TEAM WDC provides the TCJ6 an experienced prime contractor with seasoned leadership and knowledgeable staff to effectively manage and administer TCJ6 Support Services. Through our Program Management Office (PMO), we will provide the government with contract level and task visibility, quality-monitored performance, and services delivered on time and within budget. *TEAM WDC* recognizes that on-time delivery of superior quality technical support services/deliverables is essential to achieving customer satisfaction. *TEAM WDC* has deep experience providing services and products, ensuring quality, controlling costs, and meeting schedule commitments for national security and classified IT support contracts.

2.7.1 Task Order Management Approach

TEAM WDC offers TCJ6 a management approach that leverages an effective management structure customized to manage specific requirements of the contract. We will establish a PMO, at no additional direct cost, to assist the *TEAM WDC* Task Manager (TM) successfully manage the program. *TEAM WDC* has local presence in the vicinity of USTRANSCOM's headquarters and will use those resources to enhance our PMO capability. Our PMO model is already in operation today supporting the high velocity demands of our customers on our Department of the Navy, Assistant for Administration (DON/AA) Information Technology Division (ITD) prime contract and our Navy-Marine Corps Intranet (NMCI) subcontract. The *TEAM WDC* PMO consists of a back office to support program level functions (i.e., finance, accounting, human resources, and administrative staff) and an on-site TM to plan, receive, execute, and track tasks. The PMO is structured to efficiently manage essential functions such as quality assurance, task execution, risk mitigation, performance monitoring, and cost/schedule balance. Our streamlined process has Web portal workflow management and communication connectivity that expedites our response process.

TEAM WDC's Project Management Methodology (PMM) is a management framework (see Figure **2-23**) that addresses external factors affecting the TM's success in meeting the customer's expectations. *TEAM WDC's* approach incorporates the use of appropriate tools (e.g., MS Project, Deltek, *Balanced Scorecard*, *ShareMethods*®, etc.) and industry best practices. Effective Task Order Management encompasses the full project lifecycle from initiation and planning to execution and closeout. WDC's approach employs the right competencies (i.e., leadership,

management, and risk management) while also addressing external factors (i.e., stakeholders and end users). Our PMM is based upon a PMBOK® project lifecycle model and emphasizes process metrics (i.e., earned value management, service level objectives, and quality assurance), continuous customer collaboration, and strong communication strategies at appropriate levels to ensure we meet or exceed the expectations of the TCJ6 staff and end users.

(b)(4)

Figure 2-23. (b)(4)

TEAM WDC meets management performance standards by controlling task schedules and deliverables, using project management control and measurement processes, monitoring and measuring continual improvement, conducting in-program technical status reviews, and tracking task status. *TEAM WDC* uses project management tools (e.g., MS Project, Excel, Gantt Charts, etc.) and project control techniques to schedule activities at the contract and task level. We believe that complex projects with many activities that have dependencies and linkages require the critical path method (CPM) as a schedule technique. CPM allows the TM to assess the sequence of these activities and calculate the minimum completion time for a project along with the possible start and finish times for the project activities. Our cross-functional staffing approach and ability to fine tune project scheduling reduces operational and project risk. *TEAM WDC* will implement project administration and control processes (e.g., monitoring Deltek's Job Summary Reports, weekly and monthly program review meetings, etc.) to ensure project tracking is completed effectively and on time. Developing concise WBSs and project schedules with milestones and dependencies enables the management team to define specific metrics for which reports can be generated and which can effectively measure project status.

TEAM WDC's PMO provides effective program oversight and visibility to USTRANSCOM and a single POC backed by *TEAM WDC's* corporate infrastructure to effectively administer the

contract. *TEAM WDC's* TM will work collaboratively to ensure common processes, procedures, and best practices are used. Our management approach provides the framework to organize and integrate our core competencies and resources to meet the varying complexity and specialized requirements of each task area. The PMO will orchestrate document collaboration for all programs as well as project and task execution. To facilitate task execution and management, our TM, task leads, team members, and back office support staff will use ShareMethods®, an on-demand workflow portal tool that interfaces seamlessly with other technology tools used by the PMO (i.e., *Taleo*®, a recruiting and résumé repository; and Deltek® *GCS,* a Defense Contracting Auditing Agency approved *Finance and Accounting* tool). This workflow portal allows us to effectively manage contract level and task level projects, tasks, and activities.

TEAM WDC uses contract management tools and techniques such as the "S-Curve" and Earned Value Analysis to measure actual cost against budgeted cost over time. The TM will schedule Program Status Reviews, where detailed project progress reporting will occur. We know our ability to take corrective action depends on the quality of the data available; consequently, progress will be measured relative to the agreed upon project baseline. Quarterly corporate contract reviews will encompass analysis of all cost elements, technical progress, and evaluation of management quality. Our cost control system, Deltek GCS Premier, provides timely and detailed summaries of information on labor, other direct costs, travel, and subcontractor costs. We will analyze this data to predict the potential for cost overruns and develop mitigation approaches. We will control cost by limiting authority for approving charges, among other techniques. Only the TM can authorize assignment of personnel and other direct charges to a task.

"Webster Data's cost and invoice processes are outstanding. Daniel Yuly, your Controller, is a financial wiz, he always delivers detailed and accurate cost reports"

-Kelley McGrath, DON/AA COR

2.7.2 Schedule

(b)(4)

(b)(4)

Figure 2-24a.

(b)(4)

(b)(4)

Figure 2-24b. (b)(4)

2.7.3 Team Organization

TEAM WDC's organization (see Figure **2-25**) is structured to provide proactive support and management oversight. WDC's executive management is committed to ensuring our on-site TM has the authority and resources necessary to support the CSS: SS contract.

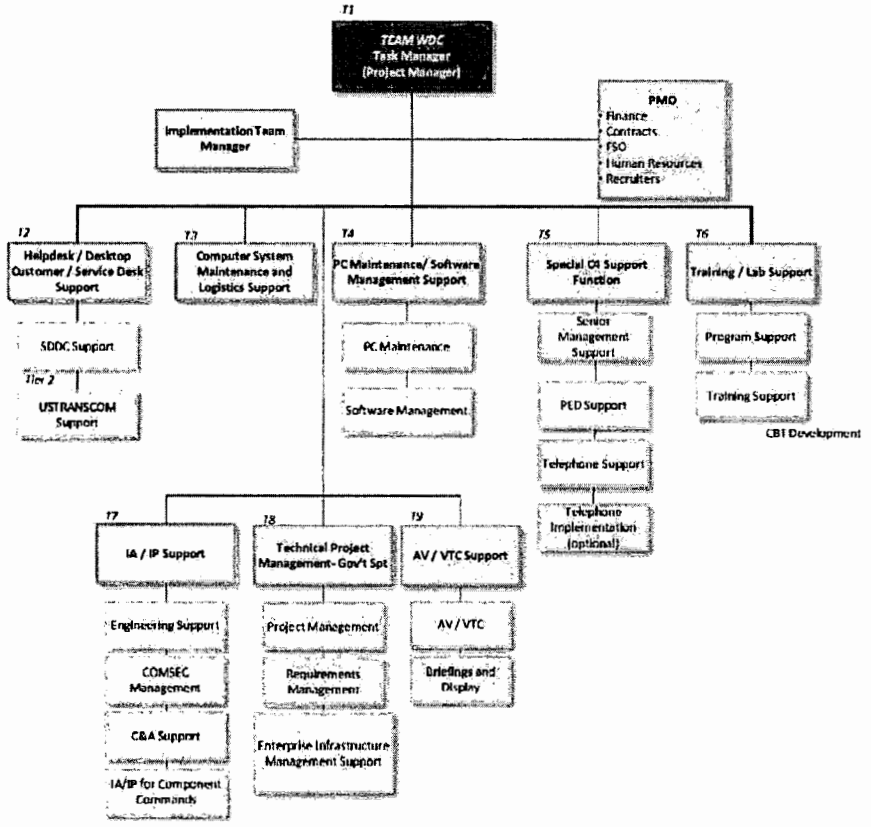


Figure 2-25. *TEAM WDC's* Organization. *TEAM WDC's PMO will support TCJ6's mission through efficient and scalable project management.*

TEAM WDC's project management structure aligns to the CSS: SS PWS requirements and will integrate all stakeholders, USTRANSCOM and other agencies, into one team. Our goal is not to be viewed as *contractors* but rather as full partners of the TCJ6 CSS: SS enterprise team. The TM reports directly to the Chief Executive Officer (CEO) of WDC to ensure all corporate assets are made available to support this contract. WDC's CEO will monitor *TEAM WDC* performance against key program metrics monthly to ensure resources are applied when needed. Our PMO (see Figure **2-26**) is structured to manage such essential functions as QA, subcontractor management, and TO management to ensure continuous monitoring of cost/schedule, resources, risk, performance, knowledge, and strategic development issues.

Role	Responsibilities
Task Manager	Located on site at Scott AFB and serves as a single point of accountability to ensure *TEAM WDC* provides high-quality, responsive support. Makes executive decisions for the entire team and has the full support of WDC's corporate resources. Areas of responsibility include quality, finance and accounting, and human resources.
Human Resources Staff	Recruits, trains, and provides staff as TOs are awarded and for surge requirements.
Accounting Staff	Produces accurate invoices in a timely manner.
Facilities Security	Ensures the timely and accurate processing of personnel security clearances and adherence to all program security requirements.
Quality Control	Ensures quality and performance adherence to service levels, and overall TCJ6 satisfaction with the quality of service. QA staff provides corporate-level oversight and participates in process reviews and

Role	Responsibilities
	quarterly program reviews.
Financial Management Staff	Responsible for accurate program setup and account administration of Deltek system for *Program Administration*, *Timesheets* and *Job Summary Reports;* and for accurate task financials and ensuring complete, auditable cost accounting, reporting, and billing to meet contract deliverables.

Figure 2-26. Management Roles and Responsibilities. *TEAM WDC's management structure facilitates IT governance, implements standardized processes enterprise wide, and enables the TCJ6 mission.*

2.7.4 Technical/Engineering Approach

The following subsections provide a high-level summary of our approach for performing all major task areas. *TEAM WDC's* contract level and task order management support approach is founded on the tenets of PMI's Program Management Body of Knowledge (PMBOK®) offering TCJ6 visibility of the program's Acceptable Quality Levels.

2.7.4.1 Task 1: Contract Level and Task Order Management

TEAM WDC's contract level and task order management methodology consists of a management plan which provides interdependencies analyses of project events, initiatives, programs, and project-related activities associated with TCJ6 business areas. Our PMO manages contractor personnel, administrative and documentation functions, and all projects, tasks, and activities associated with this contract. We will use the TOMP to define and reflect priorities of initiatives and programs. It will also enable us to project budget necessities for recurring costs and warranty information for budgeting and risk management purposes. *TEAM WDC* will maintain the TOMP within our PMO and provide an updated version of the TOMP to the government within fifteen (15) business days of the task start date. We will also review the WBS component of the updated TOMP during In-Process Reviews (IPRs) or as USTRANSCOM priorities change for status reporting and modifications. Each month, our TM will prepare a Monthly Status Report (MSR) for distribution to our client and contracting agency managers. The report corresponds directly to the TOMP's WBS. The MSR report will be prepared for QA, reviewed by our contract team for QA, and delivered no later than the 15th of the month.

Our PMO staff and TCJ6 management will meet quarterly for government-scheduled IPRs of the program status along with a formal planning session for new activities that may be upcoming. Our TM will prepare a formal agenda addressing specific issues regarding financial statuses, performance metrics and risk mitigation plans for underperforming areas. We will use a Balanced Score Card (BSC) approach to report and rate progress (based on a red, yellow, or green light rating). We will tailor the BSCs to the objectives and desired outcomes of each business area, and our approach will include targets for individual functions and processes as a means for achieving increased value. *TEAM WDC* will also prepare trip reports within five (5) business days of travel and meeting minutes within two (two business days of meetings attended by *TEAM WDC* personnel in accordance with PWS requirements.

2.7.4.2 Task 2: Helpdesk, Desktop Customer, and Service Desk Support

TEAM WDC's process for issue resolution uses an ITIL Framework, as discussed below, to address all issues with expediency and urgency. Our approach enables less complex issues to be resolved quickly while escalating more complex issues to the level of service necessary for quick and timely issue resolution. Figure **2-27** illustrates the fundamentals of *TEAM WDC's* incident management process. Once the ticket is marked as completed, quality control (QC) personnel can verify that the ticket is closed. If appropriate, quality assurance (QA) personnel can verify

the resolution and provide users with the capability to complete a customer survey. After QA, the ticket can be closed within the ticketing system.

(b)(4)

Figure 2-27: I (b)(4)

(b)(4)

Efficient and Effective Issue Resolution

We will provide issue resolution to customers expeditiously and with urgency. As issues move up the Tier structure, *TEAM WDC* separates them into categories by complexity and priority. We will first prioritize issues as either High (Priority 1), Medium (Priority 2-3), or Low (Priority 4). High Priority incidents are received from senior executives or activities, tasks, or issues associated with immediate operational requirements. Medium Priority incidents are routine activities, tasks, or issues associated with day-to-day operations. Low Priority incidents are activities, tasks, or issues for which immediate attention or resolution is not required. *TEAM WDC* will introduce a process to log and resolve incidents and issues. *TEAM WDC* will conduct internal and project status meetings quarterly to ensure we close all tickets efficiently and effectively and coordinate effectively between the TCJ6 staff, the COTR and our technical staff.

As issues are prioritized, Priority 2 incidents requiring greater expertise to resolve are escalated to supervisor or appropriate next level support technician who then allocates the required resources for its immediate resolution. Issue resolution by category has three effects: (1) issues are quickly sent to their appropriate level of resolution; (2) simpler issues are sorted out and resolved expeditiously; and (3) more difficult issues are promptly identified so that resources can be properly focused. This process enables the rapid resolution of routine issues, at the right level,

with the right skill set and gives our senior technicians time to resolve more complex-higher priority more effectively and efficiently.

A representative sample of the Service Level Agreements and performance metrics for Help Desk is provided in Figure **2-28.**

(b)(4)

Figure 2-28. (b)(4)

(b)(4)

TEAM WDC provides technical and exper (b)(4) support to senior executive service officials and Flag/Generals officers for Defense Advanced Research Projects Agency (DARPA) and the Secretary of the Navy (SECNAV). DARPA, a customer with exceedingly high response requirements for its executives, demanded that our " (b)(4) technicians exceed the 2 hour SLA response requirement by responding within 15 minutes. We routinely met that expectation as evident in our quarterly award fee ratings, which averaged 96 percent and higher. At SECNAV, *TEAM WDC* supports senior and executive management and staff which includes career Senior Executive Service, Presidential Political Appointees, Flag and General officers who manage various Secretariat offices. Because these executives are highly placed and their mission exceptionally sensitive (national security implications) our technicians are extremely professional and always succeeds in a "low tolerance-high risk" environment.

(b)(4) service and support will be established to provide immediate service to designated VIPs at TCJ6 and its customers. (b)(4) supersedes normal customer support, resolving issues in the minimum amount of time. "White Glove" incidents and issues are considered 'urgent' Priority 1 incidents and issues. Designated Tier 2 technicians on the SDDC service desk and end-user support program will be identified as "White Glove" support technicians for USTRANSCOM VIPs and executives. Our designated Tier 2 technicians will respond to Priority 1 incidents and issues to bring immediate resolution for senior executives. WDC will request a list of VIPs by name from the COR. Our "White Glove" process will be as follows:

- An e-mail or call is received from a designated "White Glove" VIP

  - VIPs have a separate phone number to use for reporting incidents/issues
  - VIPs also have a separate email address that is monitored by all members of the "White Glove" team
- A trouble ticket will be created under the VIP's name
- The requestor is contacted within 15 minutes if not immediately
- A trouble ticket will be marked resolved when the action has been completed and the VIP is satisfied

We will accurately escalate incidents (trouble tickets) from Tier 1 to Tier 2 following the procedures outlined in Figure 2-25. The combination of this approach with improved training of service desk personnel will help reduce time lost because of misrouting of tickets. The TCJ6 service desk will automatically escalate trouble calls to higher level technicians after 10 minutes or immediately after determining that the issue cannot be resolved by the service desk. *TEAM WDC* will keep customers informed about incident status at regular intervals by making a personal telephone call or sending an email.

2.7.4.3 Task 3: Computer System Maintenance and Logistics Support

TEAM WDC will perform an initial assessment of the TCJ6 legacy network to develop and manage a comprehensive life cycle maintenance program, as required, supporting TCJ6's network infrastructure with continuous monitoring, notifications, and on-call services achieving 24/7/365 network operability. *TEAM WDC* will begin by establishing a baseline inventory as well as identifying and documenting the most common problems throughout the network infrastructure. This is done by analyzing trouble ticket history, event logs, performance baselines, and monitoring tool data. We will quickly identify and resolve any recurring problems, resulting in increased service availability and performance. We will capture, document, and categorize performance baseline data for each network including Local Area Network (LAN), Wide Area Network (WAN), Wireless, and Remote Access, and retain this data in a central repository and analyze it for performance, troubleshooting, and capacity planning. The inventory assists *TEAM WDC* technicians in providing life cycle support for unclassified and classified USTRANSCOM infrastructure located both at Scott AFB and the DECC-St. Louis site. *TEAM WDC* will maintain the B-3 list of equipment in use beyond warranty. As described in Proposal Section 2.6.2, On-Call Staffing Approach, we are poised to deliver services within the allocated 24 hour response times on location. We will ensure restoral within 48 hours after work start.

2.7.4.4 Task 4: PC Maintenance and Software Management Support

TEAM WDC will provide support services associated with the maintenance and accountability of all USTRANSCOM client level (Tier 1) IT assets including but not limited to Government owned/purchased hardware and software. Support includes maintenance, installation, repair, and replacement of client workstations; inventory management for all warranty and maintenance contracts; configuration management of USTRANSCOM's software inventory; and management of USTRANSCOM's software library. Support also includes interface, participation, and preparation of minutes from attendance at meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government. Meeting minutes detailing results and impact of the meetings/conferences will be provided IAW PWS paragraph 1.3.1.5.

Our team's approach provides processes and structure around Configuration Management (CM) and Asset Management. Our process driven approach is aligned to establish, receive, track, and maintain assets from acquisition through disposal. In establishing, receiving, and tracking assets,

our dedicated Asset Manager initiates and maintains a baseline configuration, reports hardware/software license status, and tracks vendor licenses within our Configuration Management Database (CMDB). As the asset lifecycle progresses, ordered steps are performed to ensure delivery of effective and reliable maintenance that that will minimize and prevent problems. Our approach combines change management best practices with release, and deployment management processes to identify the need, configure, test, deploy and maintain the asset within the production environment (See Figure **2-29** for details).

(b)(4)

Figure 2-29: (b)(4)

(b)(4)

2.7.4.5 Task 5: Special C4 Support Function

TEAM WDC's Special C4 Support Team establishes multi-disciplined technicians that can support a range of desk side service and diverse technologies. We leverage a predictive and proactive monitoring approach through our "White Glove" program to ensure timely receipt, management, and resolution of executive customer support

TEAM WDC will provide 24/7 support services as described in PWS paragraph 1.3.5 to implement and maintain C4 executive-level information technology services. This support includes but is not limited to mobile/wireless computing support and telecommunication support to USTRANSCOM and SDDC senior-level executives, their immediate support staff, USTRANSCOM Liaison Officers located at various Combatant Commands, and other senior managers approved by the USTRANSCOM Chief Information Officer. Support also includes interface, participation, and preparation of minutes from attendance at meetings or conferences held at USTRANSCOM, SDDC, or other locations as identified by the Government. Meeting minutes detailing results and impact of the meetings/conferences will be provided IAW PWS paragraph 1.3.1.5.

Our team will provide 24/7/365 dedicated support to stakeholders as identified in the paragraph above. We will use our "White Glove" program in this support area. Our plan provides on-site

coverage for 12 consecutive hours Monday to Friday by implementing overlapping shifts. For the remainder of the duty day (after hours), weekends, and holidays we will utilize our "24/7 Mobile Command Post (MCP)." (as discussed in Proposal Section 2.6.2, On-Call Staffing Approach). In addressing some of the high level key activities described in the SOP, our approach delivers:

- Multi-disciplined technicians to support a range of desk side services (moves/adds/changes, user assistance and training, etc.) and diverse technologies (workstation, VTC, telephones, cell phones, personal data assistants, etc.)
- Processes to leverage existing enterprise management and trouble ticketing technologies, along with complementary procedures
- Incident escalation and close-out procedures that ensure appropriate coordination between the Desk Side Support Team and the Consolidated Help Desk

Upon incident resolution, the Service Desk will verify with the end-user that the incident has been resolved and the ticket will be closed.

2.7.4.6 Task 6: Training/Lab Function

Team Member SRA's IT Software Application Training Team received a 4.75 rating on a 5 point scale on its recent customer satisfaction survey.

TEAM WDC, through its SRA Team Member, has extensive experience developing, updating, presenting and maintaining USTRANSCOM training material, curricula and critiques. Our Training and Software Support team is currently on contract within the TCJ6 and is performing training tasks in support of USTRANSCOM. Our Team members are all Microsoft Office Specialist Certified. Additionally, our Task Lead is a Microsoft Certified Trainer (MCT), Certified Technical Trainer (CTT+), and is A+ Certified. We developed the courseware and provide instruction for the USTRANSCOM Microsoft Office Suite of Applications (COTS) as well as applications that are uniquely inherent to USTRANSCOM.

The WDC Training Team will continue to proactively update and modify training materials and methodology based on USTRANSCOM needs. The Team works closely with Subject Matter Experts (SME's), stakeholders, and industry partners to ensure training is up to date, effective, and realistic. Feedback will continue to be solicited from each class through the use of written critiques. This process enables continuous assessment of training team effectiveness and often drives adjustments to training materials and presentation methods.

TEAM WDC successes in providing training plans and training curriculum are based on a sound and repeatable methodology for developing courseware based on the proven Instructional Systems Design (ISD) model, ADDIE. We will continue to use this approach, as summarized below.

- **A**nalysis –Perform a thorough assessment which includes clarifying the instructional problem, establishing the learning goals, objectives, and learning environment, and identifying the learner's existing knowledge and skills.
- **D**esign – Assess the learning objectives, exercises, assessment instruments, and content. Perform a thorough subject matter analysis to support lesson planning and media selection.

- **D**evelopment –Depending on the media type selected, begin developing the Training Plan/Curriculum. Concurrent with this activity, *TEAM WDC* instructors learn the application thoroughly enough to be considered SMEs
- **I**mplementation –Instructors begin facilitating the learning process and adapting their teaching methodologies to ensure students learns in a manner that enhances retention.
- **E**valuation- SRA instructors continually observe students for non-verbal clues to ensure that each student understands the training and is an active learner. Verbal feedback is constantly solicited throughout the training class. A formal, written critique using the Likert scale will be completed by each student at course completion.

TEAM WDC will also provide program support to USTRANSCOM by helping to assess, evaluate, and test software against functional requirements prior to sending the software to the Test Center for testing. As an example, the WDC Training Team performed a detailed evaluation of Office 2007 Software which identified several functional deficiencies. The defects were subsequently corrected prior to making Office 2007 available on the USTRANSCOM network. Our Team is currently preparing to instruct iDistribute.mil and Microsoft Office 2010 Suite of applications.

Team Member SRA has over 30 years of experience developing learning solutions, including videos and CBTs using ISD standards such as Air Force Handbook 36-2235. Our approach to learning is founded in years of experience and research, including 140,000 data hours of research for the USAF Research Laboratory, providing a solid foundation for our learning solutions. Using the ISD process in accordance with AFH 36-2235 as our framework and the video production steps outlined in Figure **2-30** we will deliver draft videos and computer based training (CBT) within 40 business days of their request and we will be able to go final within 10 business days of receiving comments. We can effectively respond on short notice by reaching back into over 90 training professionals in our Emerging Learning Technologies group, including retired USAF and Air Guard "on air" personalities who are intimately familiar with the video process both in front of and behind the camera.

Video Production Methodology
• **Concept Development** – brainstorming with the customer and stakeholders
• **Storyboarding and Scriptwriting** – capturing the ideas and validating them with the customer
• **Production Planning (Pre-production)** – arranging shooting site, interviews, actors and other logistics
• **Videography (Shoot)** – get the needed video footage, including B-roll with a minimally invasive approach
• **Graphics Design & Creation** – editing using software such as Adobe Illustrator, PhotoShop and After Effects
• **Voice Talent Recording** – using on site or SRAs sound booth
• **Original Music or Library Music tracks** – using Apple Sound Track and Garage band as well as Amadeus Pro
• **Editing** – using iMovie for rough cut versions
• **Motion Graphics & Special Effects** – using Apple Motion, Shake, Combustion and Commotion
• **Animation** – with Newtek Lightwave and 3D Studio Max
• **Final Edit, Mix, and Master** - using Media 100i with Boris FX, and Final Cut Pro with Boris FX
• **Compression** – using Apple Compressor, Squeeze and Toast Titanium
• **Authoring** - Apple DVD Studio Pro, DVCPro50
• **Standards conversion** - for worldwide distribution (e.g. PAL, Region Codes)
• **Dubs (Copies) or other Distribution**

Figure 2-30. *TEAM WDC's* Standard Video Production Methodology.

"I want to take the opportunity to tell you how professional your TCJ6-C4S Training and Software Support team is a pleasure to work with. Not only have they taken the time to thoroughly and patiently explain applications to me, but also come to my desk and walked me through my application tasking(s). Their knowledge and patience has been appreciated more then they know. Please extend my heartfelt gratitude to them for always being there ready-and-willing to assist me."

Diane Berkebile
GTN/IGC Functional Data Base Manager

2.7.4.7 Task 7: USTRANSCOM Information Assurance and Information Protection (IA/IP)

OUR TEAM'S SPECIALIZED EXPERTISE BRINGS HIGH CONFIDENCE, LOW RISK, AND IMMEDIATE RESULTS

- WDC's Cyber Support Team led DARPA to their first Outstanding rating in it's Command Cyber Readiness Inspection (CCRI) audit
- WDC's C&A Team successfully implemented an aggressive C&A plan at SECNAV to expeditiously get the 20 out of 68 systems with expiring IATOs to either IATO or Authorization to Proceed (ATO) status within 90 days
- Team Member SRA is one of only six organizations—and the only systems integrator—to be rated against the NSA's latest and more rigorous IA-CMM rating profile—Full lifecycle IA methodology is evaluated at NSA-CMM Level 3
- Team Member SRA has fielded a dedicated IA and Privacy Practice since 1999 with more than 300 dedicated IA personnel and 600+ staff supporting the IA lifecycle on DoD and Federal projects
- IA industry leadership includes support for the development of the National Strategy for the Physical Protection of Critical Infrastructures and Key Asset, the Industry Compendium to the National Strategy to Secure Cyberspace, and the establishment of NSA CoE requirements for Information Security Education

TEAM WDC's approach to providing CND and IA services, as part of our "Defense-in-Depth" strategy, integrates the capabilities of personnel, operations, and technology to provide USTRANSCOM confidence in the integrity and availability of information to achieve mission readiness, while providing decision makers a seamless, enterprise-wide and common view of data to facilitate their collaborative decision making processes. Our CND and IA processes align with the Net-Ready criteria to support mission accomplishment in a Net-Centric environment and are continually improved to accommodate rapidly changing requirements and enhancements.

As required, *TEAM WDC* will develop new and maintain existing DIACAP and security documentation for each USTRANSCOM C2, Transportation, and Financial program in accordance with DoDI 8510.01 and AFI 33-210. We will provide guidance and support to all USTRANSCOM customers within our area of responsibility in developing new, updated and optional documentation to complete or maintain a fully defined Enterprise Mission Assurance Support Service (eMASS) Comprehensive package. We will attend and offer advice during Program Design Reviews and Configuration Control Board (CCB) meetings to ensure system changes are documented and do not adversely change the security posture of the system. We will evaluate the results from the test team and determine the information system's residual risk based on its reliability and viability with respect to the larger USTRANSCOM operating environment. We will monitor this activity to ensure the CA is provided all the necessary information to keep the certification process moving forward. The CA notifies the DAA of the certification determination for consideration in the accreditation decision. The DAA determines

whether the system should receive one of four approvals: ATO, Interim ATO (IATO), Interim Approval to Test (IATT), or Denial of ATO (DATO).

C&A Verification and Configuration/Vulnerability Management Support

As identified in the PWS, our team will perform security assessments of DoD security controls for USTRANSCOM systems to measure the effectiveness of the total system security using the security validation procedures listed on the DIACAP KS and DISA IA Control Checklists. We are intimately familiar with the IA control subject areas of DoD Instruction 8500.2, and we have spent many years managing IA offices supporting and assessing DoD automated information system (AIS) applications, stand-alone systems, local-area and enterprise-wide-area enclaves, outsourced IT-based processes and platform dependent IT interconnections. Security Test and Evaluation (ST&E), Figure **2-31**, is the validation arm of the DIACAP program currently being implemented by the AFNIC.

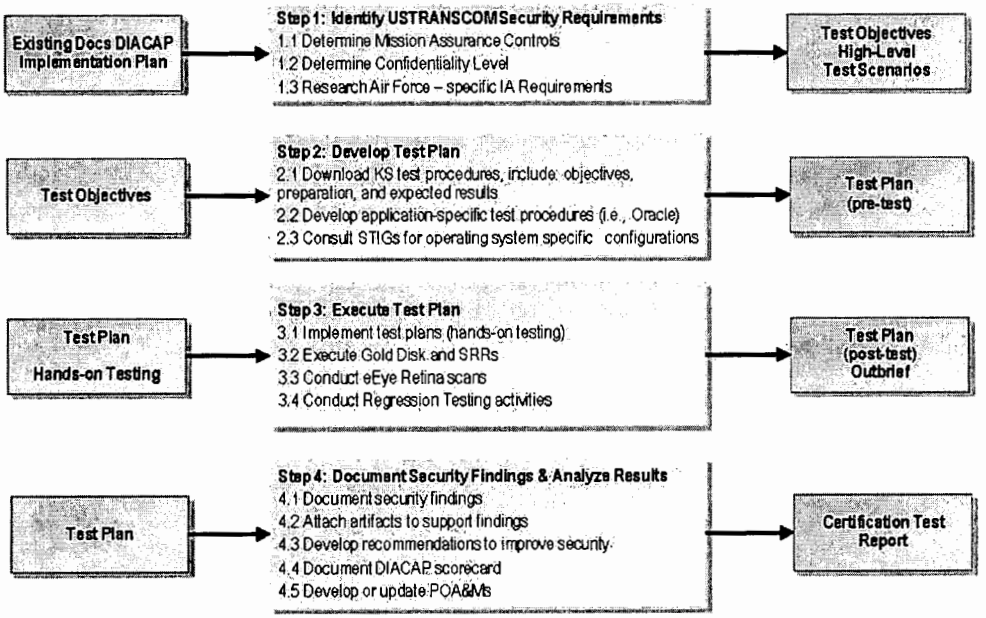


Figure 2-31 ***TEAM WDC's* ST&E Process.** *TEAM WDC's ST&E Process assures accurate and complete C&A results.*

The goal is to identify software/hardware defects and policy/procedure inconsistencies before they introduce vulnerabilities into the network. We use a variety of technical and non-technical techniques to verify an information system's or enclave's compliance with its DIP, including interviews, examination, observation, and technical testing. We will incorporate the DISA Security Technical Implementation Guides (STIG), Checklists, System Requirements Reviews (SRRs) and DISA Gold Disk Program to obtain optimal level of security and compliance with physical, administrative, personnel, computer, network and communications security on USTRANSCOM systems.

2.7.4.8 Task 8: Project and Program Management

(b)(4)

(b)(4)

(b)(4)

Figure 2-32. Task Review Board Process.

2.7.4.9 Task 9: Audiovisual and Video Teleconferencing Support

The end result of implementing our proven AV/ VTC support approach and flexible staffing is a seamless integration of AV/VTC services and improved responsiveness to customer needs.

TEAM WDC will provide trained and certified communication specialists from our VTC and Briefings and Display Teams to support USTRANSCOM AV/VTC requirements. Several of the team members will also be trained and qualified to perform as primary and alternate COMSEC Responsible Officers (CRO) and Secure Voice Responsible Officers (SVRO). We will also designate an ADPE Equipment Custodian and perform FACCSM duties. Our support methodology objective is designed to provide preventative maintenance, operator instructions, and on-site TCCC, TCDC, and TCCS deliverables IAW established performance thresholds. Our approach to providing successful AV/VTC support is comprised of three major activity sets as described below.

- **AV/VTC Support.** Includes incident investigation and analysis, root cause analysis, problem resolution, lessons learned, and customer feedback
- **AV/VTC Monitoring and Maintenance.** Maintenance and preventive maintenance activities (alignment, calibration, bulb/lamp replacement, system updates) performance and usage metrics and compliance monitoring (STIG and IAVA compliance)
- **AV/VTC Configuration and Management.** Focuses on setup management, VTC conference scheduling and de-confliction, on-site support, document maintenance, hardware baseline management and software revision control.

In addition to the above support activities, *TEAM WDC* has experience in AV/VTC design support through current contracts (e.g., USECUOM, Army National Guard, FDIC) and possesses the expertise to provide AV/VTC equipment upgrade and migration strategy recommendations.

A critical part of our management strategy is to cross train the ITV and Briefing and Analysis team members to provide more flexibility and efficiencies in meeting AV/ITC requirements.

2.7.5 Risk Management

TEAM WDC's risk management process provides for a continuous, rigorous process of risk identification, assessment, and mitigation. Our risk management process also provides a means for identifying risk "triggers" and monitoring risks, as well as a means for implementing metrics required by performance-based contracts. Our risk assessment methodology is designed for early identification of risk triggers, provides a means to mitigate risk and lower programmatic slippages, and minimizes operational disruptions. Our overall objective is to minimize the effects of project risks by defining systematic risk management processes to address technical, managerial, performance, and cost issues. We define "risk" as any event with some probability of adverse impact on a project's cost, schedule, or technical accomplishment. Effective risk management supports the program's ability to meet its objectives on time and on budget. We will assist TCJ6 in determining technical risk associated with proficient execution of assigned tasks. We will work with TCJ6 to weigh risk factors to systematically prioritize the task activities and reduce risks through aggressive mitigation activities. Our risk management process consists of six elements shown in Figure **2-33**.

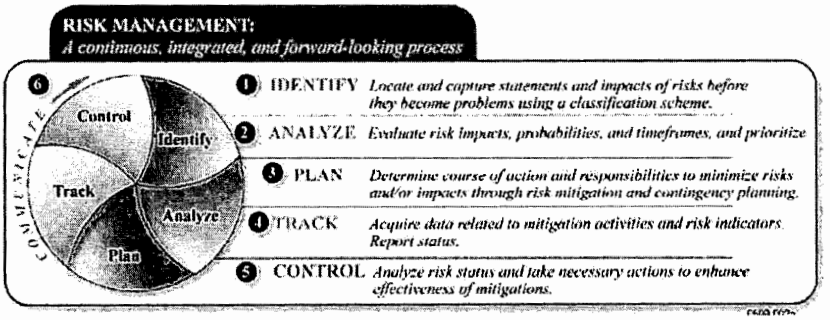


Figure 2-33: *TEAM WDC's* aggressive risk management methodology

We have a structured approach for identifying and managing risks on every project; this prevents the need for undue delay or inconvenience. We perform a wide range of Capability Model Maturity Integration (CMMI)-based risk identification and mitigation activities, including—

- Evaluation by senior staff of proposed approaches for feasibility and suitability
- Project staffing with the right mix of specialists, and ensuring breadth of coverage so that no one team member is indispensable
- Aggressive requirements gathering and tracking to make sure that all requirements are clearly defined, measurable, and testable
- Day-to-day management and oversight infrastructure to ensure that solid QA and configuration management programs are in place and in use from the start of the program. We use online risk tracking tools to help track risks from the time they are identified to when closed
- Timely reporting of activities to the customer and the team's senior management

By aggressively managing risk from the start of all projects, we have continuously and successfully minimized risk to our customers. Successful past performance, solid risk management methodology, and our highly experienced IT staff ideally positions our team to easily recognize any potential for technical risk up front. Once we have identified the potential

for risk we can then assess it, track it, and mitigate the risk factor to a manageable level. We have also listed, in our risk factors table in Proposal Section 2.5.3, Implementation Risks, and samples of actions we have taken to mitigate or remediate risk factors in the past.

2.7.6 Communications Plan

Our Communications Plan provides methods and identifies technology for accurate and timely information exchange and cooperative sharing among TCJ6's customers, stakeholders, and support staff. Our plan emphasizes bi-directional communication through direct and frequent interaction at staff, management, and executive levels; is supported by tools that facilitate information and knowledge capture, analysis, dissemination, archiving, and retrieval; and aligns with Project Management Institute (PMI) standard practices. We promote awareness and information distribution through easily accessible, hierarchical visibility into program status and performance against program service level objectives (SLOs) and metrics, advance knowledge of scheduled events and rapid notification of unscheduled events, and robust and effective feedback channels and techniques that result in a no-surprises environment that enables continuous process improvement.

Our Team understands the importance of clear, concise, and bi-directional communications as well as open access to all pertinent programmatic and contractual information. *TEAM WDC* is committed to full and open communication with TCJ6 representatives, including the TCJ6 Contracting Officer (CO), TM, and COTR. *TEAM WDC* will facilitate communication among the CO, COTR, *TEAM WDC*, and TCJ6 functional experts and end users to enhance coordination, and will convene weekly internal management meetings to discuss quality, resources, and technical issues. Our Communication Plan provides *TEAM WDC* a forum for discussing and resolving issues surrounding the design, implementation, delivery, and integration of services.

While we strive to identify and resolve issues at the lowest possible level, the final authority for resolution rests with the TM. Our escalation procedures for problem resolution have been developed to prevent problems. However, we build appropriate feedback loops and mechanisms into our technical solutions and management plans to provide clear channels for communicating and escalating problems. In those rare instances where problems arise, *TEAM WDC* has procedures in place to immediately respond to our client's concerns.

Our Voice of the Customer (VOC) process implemented across our SECNAV program is a quality-based communication method we will introduce to the CSS: SS contract. The VOC process is used to identify customer concerns and desires before they become problematic. Action plans are developed for each issue. All actions are tracked and given attention until ultimate closure is achieved. We will develop an online VOC database that includes a set of queries that can easily identify items such as pending issues, due dates, issues within a subtask, or customer issues. The VOC process is used to identify ongoing problems and trends. We can also track closure times and effectiveness. Ease of use and constant monitoring by our Quality professionals has assured our customers of consistent follow-through on actions.

We implemented a robust and redundant, rapid notification framework to alert organizations or individuals of unplanned events to minimize impact to daily operations. Figure **2-34** summarizes our regularly scheduled meetings that are conducted at appropriate levels and frequency for the efficient dissemination of information necessary to meet program objectives and schedules, monitor progress, and develop and implement remediation plans, if necessary. All required

contract, task and project reports will be prepared and available for distribution in hard copy form and posted on-line (with Government concurrence) in the Knowledge Corner.

Type	Frequency	Attendees	Purpose	Outcomes
Stand-up Meetings	Daily	COR and TM	Update ongoing activities Preview day's activities and goals	Agreement on priorities for ongoing work
Status Meetings	Weekly	COR, TM and Mgrs	Review current activities Preview upcoming week Plan near-term actions	Priority re-evaluation Reassign resources Rolling labor forecast
Program Reviews	Monthly	CO, COR, TM, Mgrs, task leads	Review program metrics Present risks, impacts, and mitigation plan Preview upcoming goals	At-risk progress and funding identified New resource needs identified
IPR	Quarterly	CO, COR, M, SVP	Summarize status, progress, recommendations, and concerns in development of any tasks or documentation	Understanding of Status Resolution to concerns

Figure 2-34. TCJ6 schedule of meetings ensures bi-directional communication and early problem resolution

We have an in-place notification hierarchy to quickly respond to any unplanned events or emergencies, for both contractor staff and TCJ6. Our staff has clear instructions on who to contact for any unforeseen operational situations. Our framework has a defined escalation process regarding or identifying whom within our management hierarchy and TCJ6 to contact if a situation is not resolved within a predetermined time-limit. The on-site escalation terminates with our 24x7 accessible PMO and TM, who has direct contact with corporate resources and executives and authority to bring in additional resources as necessary. During the entire unplanned event, USTRANSCOM will be notified of our plans, actions, and estimated time to resolve.

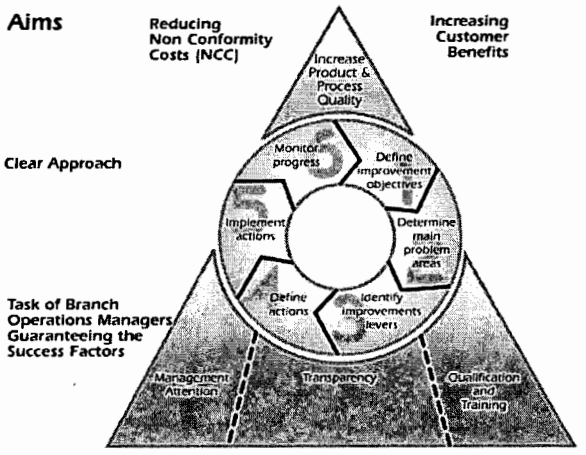
2.7.7 Quality Control

TEAM WDC is a customer-centered company focused on providing quality and responsive information technology support. *TEAM WDC* adheres to ISO 9001:2000 International Standard (Quality Management System – Requirements) requirements for a quality management system to consistently provide products and services that meet customer and applicable regulatory requirements. The aim of the quality management system used by *TEAM WDC* is to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable regulatory requirements. We meet SLOs outlines in the PWS through the use of an automated tool, such as Privia, which sends alerts to our PRM and management staff as due dates and milestones arise. We enhance customer satisfaction through the effective application of quality management, including processes for continual system improvement and assurance of conformity to customer and applicable Government guidance and requirements.

TEAM WDC's QC ensures that services exceed the Performance Work Statement (PWS) requirements. This is accomplished by requiring that all deliverables are reviewed, quality checked, and approved by the QC Specialist located in the PMO. The QC techniques used may include:

- Cause and Effect Diagrams
- Control Charts
- Flowcharts
- Histograms
- Pareto Charts
- Run Charts

- Scatter Diagrams
- Statistical Sampling
- Inspection
- Defect Repair Reviews



Our QC Specialist is responsible for all QA/QC activities and reports directly to the *TEAM WDC* TM. All *TEAM WDC* personnel will be responsible for the development of deliverables according to WDC's Quality Assurance policy and procedures. *TEAM WDC* will conduct independent internal peer reviews and QA certification of all client deliverables. This certification process ensures all other verification processes were completed and is a final control point to identify products that are not ready for delivery. In addition to review and certification activities, QA personnel in the program support group conduct regular single process and full process audits of projects. These audits ensure that projects are following standard *TEAM WDC* processes, including quality control activities. QA reports audit results to the Task Order Manager for corrective action, and independently reports to *TEAM WDC* senior management through regular monthly and quarterly reports. They will ensure that any changes to deliverables are approved by the QA/QC and management functions.

2.7.8 Configuration Management

TEAM WDC is dedicated to supporting a centralized ITIL-based Configuration Management (CM) control process to include introduction of a Configuration Management Database (CMBD) tool to integrate with the Service Desk tool suite. The CMDB will identify, control, maintain, and verify configuration items (CIs) within the USTRANSCOM J6 environment. Further, the integration of CMDB with the Service Desk tool suite will directly correlate to quality assurance for accuracy and increase the efficiency and effectiveness of our *TEAM WDC* and USTRANSCOM's entire service management strategy and impacts on all areas of ITSM.

Our CM methodology will ensure maintenance of an asset inventory change history of all hardware, software, and communications infrastructure elements. The asset inventory change history will include all fixed and portable seats, wireless seats, enterprise local area network infrastructure elements, external networks, and all related software products.

The established CM program will support the IT Governance Structure as follows:

- Establish system baselines
- Maximize control and accountability
- Maximize responsiveness and minimize inefficiency
- Provide traceability and version control of IT assets
- Provide management flexibility and visibility into the IT process

ATTACHMENT 7 – STAFFING MATRIX

[Please Refer To Attached Excel File – "WDC VOL II Atch 7 – Staffing Matrix.xls"]

(b)(4)

Labor Category / Task Area	Task1	Task 2	Task 3 & Task 4	Task 5	Task 6	Task 7	Task 8	Task 9	TOTAL HOURS BY TASK/SUBTASK
Task Area 1									
Task 1, Subtask 1	(b)(4)								(b)(4)
Task 1, Subtask 2									
Task 1, Subtask 3									
Task 1, Subtask 4									
Task 1, Subtask 5									
Task Area 2									
Task 2, Subtask 1		(b)(4)							(b)(4)
Task 2, Subtask 2									
Task 2, Subtask 3 (Optional)									
Task Area 3									
Task 3									(b)(4)
Task Area 4									
Task 4, Subtask 1			(b)(4)						(b) (4)
Task 4, Subtask 2									
Task Area 5									
Task 5, Subtask 1 para 1.3.5.1.1									(b)
Task 5, Subtask 1 para 1.3.5.1.2									
Task 5, Subtask 1 para 1.3.5.1.3									(4)
Task 5, Subtask 2				(b)(4)					
Task 5, Subtask 3									
Task 5, Subtask 4 (Optional)									
Task Area 6									
Task 6, Subtask 1									(b)
Task 6, Subtask 2					(b)(4)				
Task 6, Subtask 3									(4)
Task 6, Subtask 4 (Optional)									
Task Area 7									
Task 7, Subtask 1									
Task 7, Subtask 2						(b)(4)			(b)(4)
Task 7, Subtask 3									
Task 7, Subtask 4									
Task Area 8									
Task 8, Subtask 1	(b)(4)						(b)(4)		(b)(4)
Task 8, Subtask 2									
Task Area 9									
Task 9, Subtask 1									
Task 9, Subtask 2								(b)(4)	(b)(4)
Task 9, Subtask 3									
Task 9, Subtask 4									
Task 9, Subtask 5						(b)(4)			
Task 9, Subtask 6									
Task 9, Subtask 7									
Task 9, Subtask 8								(b)(4)	

Task Area	Labor Category	None	IAT I	IAT II	IAT III	IAM I	IAM II	IAM III	Security Clearance
Task Area 2		X							
Task 2, Subtask 1									
Task 2, Subtask 1									
Task 2, Subtask 1									
Task 2, Subtask 2									
Task 2, Subtask 2									
Task 2, Subtask 2									
Task 2, Subtask 3									
Task 2, Subtask 3									
Task Area 3									
Task Area 4									
Task 4, Subtask 1									
Task 4, Subtask 2									
Task Area 5									
Task 5, Subtask 1									
Task 5, Subtask 2									
Task 5, Subtask 3									
Task 5, Subtask 4									
Task Area 6									
Task 6, Subtask 1									
Task 6, Subtask 2									
Task 6, Subtask 3									
Task 6, Subtask 4									

(b)(4)

(b)(6)

Task Area	Labor Category	None	IAT I	IAT II	IAT III	IAM I	IAM II	IAM III	Security Clearance
Task Area 7					X				
[redacted]									
Task 7, Subtask 1									
[redacted]									
Task 7, Subtask 2									
[redacted]									
Task 7, Subtask 3									
[redacted]									
Task 7, Subtask 3 para 1.3.7.3.1									
[redacted]									
Task 7, Subtask 3 para 1.3.7.3.2									
[redacted]									
Task 7, Subtask 3 para 1.3.7.3.3									
[redacted]									
Task 7, Subtask 4									
[redacted]									
Task Area 8									
[redacted]									
Task 8, Subtask 1									
[redacted]									
Task 8, Subtask 2									
[redacted]									
Task Area 9									
[redacted]									
Task 9, Subtask 1									
[redacted]									
Task 9, Subtask 2									
[redacted]									
Task 9, Subtask 3									
[redacted]									
Task 9, Subtask 4									
[redacted]									
Task 9, Subtask 5									
[redacted]									

(b)(4)

(b)(6)

Task Area	Labor Category	None	IAT I	IAT II	IAT III	IAM I	IAM II	IAM III	Security Clearance
Task 9, Subtask 6	(b)(4)								(b)(6)
Task 9, Subtask 7									
Task 9, Subtask 8									

Each Offeror shall list the labor categories applicable to each Task Area and mark the appropriate Information Assurance Certification for each labor category. In addition, the Security Clearance for each labor category should be listed in Column K

Labor Category / Paragraph	(b)(4)									Total Hours per Paragraph
Cyber Security (Optional Support Paragraphs)										
Paragraph 5.4 (Optional)										(b)(4)
Paragraph 5.5 (Optional)										
Paragraph 5.6 (Optional)										
Paragraph 5.7 (Optional)										
Paragraph 5.8 (Optional)	(b)(4)									
Paragraph 5.10 (Optional)										
Paragraph 5.11 (Optional)										
Paragraph 5.12 (Optional)										
Paragraph 5.13 (Optional)										
Paragraph 5.14 (Optional)										
Paragraph 5.15 (Optional)										
Paragraph 5.16 (Optional)										
Total Hours Per Labor Category										

Each Offeror shall list the labor categories applicable to the acquisition and list the hours per support paragraph
The hours are for the duration of one Fiscal Year