SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

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

1. REQUISITION NUMBER	PAGE 1 OF 121

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
HQ0034-07-D-1008	01-May-2007		HQ0034-07-R-1016	26-Jan-2007

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No Collect Calls)*	8. OFFER DUE DATE/LOCAL TIME
	JOHN D. HUNDLEY	703-696-3866	12:00 PM 19 Mar 2007

9. ISSUED BY CODE HQ0034

WHS, ACQUISITION & PROCUREMENT OFFICE
1155 DEFENSE PENTAGON
RPN SUITE 12063
WASHINGTON DC 20301-1155

TEL:
FAX:

10. THIS ACQUISITION IS

- [X] UNRESTRICTED
- [ ] SET ASIDE: % FOR
  - [ ] SMALL BUSINESS
  - [ ] HUBZONE SMALL BUSINESS
  - [ ] 8(A)

NAICS: 561621
SIZE STANDARD: $11.5M

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED

- [ ] SEE SCHEDULE

12. DISCOUNT TERMS

NET 30

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

13b. RATING

14. METHOD OF SOLICITATION

- [ ] RFQ
- [ ] IFB
- [X] RFP

15. DELIVER TO CODE HQ0020

PFPA
TIM DARR
PENTAGON FORCE PROTECTION AGENCY
100 BOUNDRY CHANNEL DRIVE
ARLINGTON VA 22202

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/OFFEROR CODE 2R341

DRS TECHNICAL SERVICES INC
KRIS MCKINLEY
5845 RICHMOND HWY SUITE 725
ALEXANDRIA VA 22303-1865

TEL. 703-329-9300
FACILITY CODE

18a. PAYMENT WILL BE MADE BY CODE HQ0338

DFAS-CO/SOUTH ENTITLEMENT OPERATIONS
P.O. BOX 182264
COLUMBUS OH 43218-2264

- [ ] 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)

$2,328,878.98 EST

- [ ] 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:

29. AWARD OF CONTRACT: REFERENCE

- [ ] OFFER DATED 12-Apr-2007 . 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
	Melanie Alston	30-Apr-2007

30b. NAME AND TITLE OF SIGNER *(TYPE OR PRINT)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(TYPE OR PRINT)*
		Ms. Melanie Alston / Contracting Officer TEL: 703-696-4093 EMAIL: melanie.alston@whs.mil

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS (CONTINUED)		PAGE 2 OF 121

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			Months		
	System Support FFP System support includes the Network Control Center System Administration & Engineering Support				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001AA		6	Months	(b)(4)	(b)(4)
	Pentagon Reservation FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001AB		6	Months	(b)(4)	(b)(4)
	Leased Facilities FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0002				UNDEFINED	UNDEFINED

Installation
FFP
Prices, delivery and description of services will be by individual delivery order.

	MAX NET AMT	UNDEFINED

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0003		6	Months	(b)(4)	(b)(4)

Preventive Maintenance for Pentagon Resv
FFP

	NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0004		8,000	Hours	(b)(4)	(b)(4)

Repair for the Pentagon Reservat
T&M
Repairs are for services that are not preventive maintenance.

	TOT ESTIMATED PRICE	(b)(4)
	CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005	Logistics Support FFP		Months		
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005AA	Pentagon Reservation FFP	6		(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0005AB	Leased Facilities FFP	6		(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0006		6	Months	(b)(4)	(b)(4)
	Preventive Maintenance for Leased Fac FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0007		2,000	Hours	(b)(4)	(b)(4)
	Repair for Leased Fac T&M Repairs are for services that not preventive maintenance.				
				TOT ESTIMATED PRICE	(b)(4)
				CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0008			Hours	(b)(4)	(b)(4)
	Maintenance Labor T&M Provide a composite fixed hourly rate for unforeseen support.				
				TOT ESTIMATED PRICE	
				CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001			Months		
OPTION	System Support FFP System support includes the Network Control Center System Administration & Engineering Support				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001AA		12		(b)(4)	(b)(4)
OPTION	Pentagon Resveration FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001AB		12	Months	(b)(4)	(b)(4)
OPTION	Leased Facilities FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
1002				UNDEFINED	UNDEFINED
OPTION	Installation FFP Prices, delivery and description of services will be by individual delivery order.				
				MAX NET AMT	UNDEFINED

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1003		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Pentagon Resv FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1004		12	Months		
OPTION	Repair for the Pentagon Reservat FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1005 OPTION	Logistics Support FFP		Months		
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1005AA OPTION	Pentagon Reservation FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1005AB OPTION	Leased Facilities FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1006		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Leased Fac FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1007		12	Months		
OPTION	Repair For Leased Facilities FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1008			Hours	(b)(4)	(b)(4)
OPTION	Maintenance Labor T&M This is for unforeseen support.				
				TOT ESTIMATED PRICE	
				CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001			Months		
OPTION	System Support FFP System support includes the Network Control Center System Administration & Engineering Support				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001AA		12	Months	(b)(4)	(b)(4)
OPTION	Pentagon Reservation FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001AB		12	Months	(b)(4)	(b)(4)
OPTION	Leased Facilities FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
2002				UNDEFINED	UNDEFINED
OPTION	Installation FFP Prices, delivery and description of services will be by individual delivery order.				
				MAX NET AMT	UNDEFINED

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2003		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Pentagon Resv FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2004		12	Months		
OPTION	Repair for the Pentagon Reservat FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2005 OPTION	Logistics Support FFP		Months		
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2005AA OPTION	Pentagon Reservation FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2005AB OPTION	Leased Facilities FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2006		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance For Leased Fac FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2007		12	Months		
OPTION	Repair For Leased Facilities FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2008			Hours	(b)(4)	(b)(4)
OPTION	Maintenance Labor T&M This is for unforeseen support.				
				TOT ESTIMATED PRICE	
				CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001			Months		
OPTION	System Support FFP System support includes the Network Control Center System Administration & Engineering Support				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001AA		12	Months	(b)(4)	(b)(4)
OPTION	Pentagon Reservation FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001AB		12	Months	(b)(4)	(b)(4)
OPTION	Leased Facilities FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
3002				UNDEFINED	UNDEFINED
OPTION	Installation FFP Prices, delivery and description of services will be by individual delivery order.				
				MAX NET AMT	UNDEFINED

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3003		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Pentagon Resv FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3004		6	Months		
OPTION	Repair for the Pentagon Reservat FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3005 OPTION	Logistics Support FFP		Months		
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3005AA OPTION	Pentagon Resveration FFP	12		(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3005AB OPTION	Leased Facilities FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3006		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Leased Fac FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3007		12	Months		
OPTION	Repair For Leased Facilities FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3008			Hours	(b)(4)	(b)(4)
OPTION	Maintenance Labor T&M This is for unforeseen support.				
				TOT ESTIMATED PRICE	
				CEILING PRICE	

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001			Months		
OPTION	System Support FFP System support includes the Network Control Center System Administration & Engineering Support				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001AA		12	Months	(b)(4)	(b)(4)
OPTION	Pentagon Reservation FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001AB		12	Months	(b)(4)	(b)(4)
OPTION	Leased Facilities FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
4002				UNDEFINED	UNDEFINED
OPTION	Installation FFP Prices, delivery and description of services will be by individual delivery order.				
				MAX NET AMT	UNDEFINED

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4003		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Pentagon Resv FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4004		12	Months		
OPTION	Repair for the Pentagon Reservat FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4005 OPTION	Logistics Support FFP		Months		
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4005AA OPTION	Pentagon Resveration FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4005AB OPTION	Leased Facilities FFP	12	Months	(b)(4)	(b)(4)
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4006		12	Months	(b)(4)	(b)(4)
OPTION	Preventive Maintenance for Leased Fac FFP				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4007		12	Months		
OPTION	Repair For Leased Facilities FFP Repairs are for services that are not preventive maintenance.				
				NET AMT	(b)(4)

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4008			Hours	(b)(4)	(b)(4)
OPTION	Maintenance Labor T&M This is for unforeseen support.				
				TOT ESTIMATED PRICE	
				CEILING PRICE	

CLIN MINIMUM/MAXIMUM QUANTITY AND CLIN VALUE

The minimum quantity(s) and CLIN value(s) for all orders issued against the CLIN(s) on this contract shall not be less than the minimum quantity(s) and CLIN value(s) stated in the following

table. The maximum quantity(s) and CLIN value(s) for all orders issued against the CLIN(s) on this contract shall not exceed the maximum quantity(s) and CLIN value(s) stated in the following table.

CLIN	MINIMUM QUANTITY	MINIMUM AMOUNT	MAXIMUM QUANTITY	MAXIMUM AMOUNT
0003		$336,321.00		
0004		$465,120.00		
0006		$327,481.98		
0007		$106,240.00		
1006		$674,729.88		
2006		$695,109.48		
0001AA		$491,037.00		
0005AA		$55,821.00		
0001AB		$491,037.00		
3006		$716,121.36		
1001AB		$1,018,789.08		
0005AB		$55,821.00		
1001AA		$1,018,789.08		
4006		$737,785.20		
1005AA		$114,947.64		
1005AB		$114,947.64		
2001AA		$1,049,378.88		
2001AB		$1,049,378.88		
2005AA		$118,352.28		
2005AB		$118,352.28		
3001AA		$1,080,919.20		
3001AB		$1,080,919.20		
3005AA		$121,859.04		
3005AB		$121,859.04		
4001AA		$1,113,439.56		
4001AB		$1,113,439.56		
4005AA		$125,471.04		
4005AB		$125,471.04		
1003		$692,407.92		
2003		$712,787.52		
3003		$733,212.48		
4003		$754,857.48		

CLIN DELIVERY/TASK ORDER MINIMUM/MAXIMUM QUANTITY AND CLIN ORDER VALUE

The minimum quantity and order value for the given Delivery/Task Order issued for this CLIN shall not be less than the minimum quantity and order value stated in the following table. The maximum quantity and order value for the given Delivery/Task Order issued for this CLIN shall not exceed the maximum quantity and order value stated in the following table.

CLIN	MINIMUM QUANTITY	MINIMUM AMOUNT	MAXIMUM QUANTITY	MAXIMUM AMOUNT
0001		$		$

0002	(b)(4)	(b)(4)
0003	$	$
0004	$	$
0005	$	$
0006	$	$
0007	$	$
0008	$	$
1006	$	$
1008	$	$
2006	$	$
2008	$	$
0001AA	$	$
0005AA	$	$
1007	$	$
2007	$	$
0001AB	$	$
3006	$	$
3008	$	$
1001AB	$	$
3007	$	$
0005AB	$	$
1001AA	$	$
4006	$	$
4007	$	$
4008	$	$
1005AA	$	$
1005AB	$	$

2001AA	$	$
2001AB	$	$
2005AA	$	$
2005AB	$	$
3001AA	$	$
3001AB	$	$
3005AA	$	$
3005AB	$	$
4001AA	$	$
4001AB	$	$
4005AA	$	$
4005AB	$	$
1001	$	$
1002	(b)(4)	(b)(4)
1003	$	$
1004	$	$
1005	$	$
2002	(b)(4)	(b)(4)
2004	$	$
2001	$	$
2003	$	$
2005	$	$
3001	$	$
3002	(b)(4)	(b)(4)
3004	$	$
4002	(b)(4)	(b)(4)
4004	$	$

3003	$	$
3005	$	$
4001	$	$
4003	$	$
4005	$	$

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
0001AA	N/A	N/A	N/A	Government
0001AB	N/A	N/A	N/A	Government
0002	Destination	Government	Destination	Government
0003	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
0004	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
0005	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
0005AA	N/A	N/A	N/A	Government
0005AB	N/A	N/A	N/A	Government
0006	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government

0007	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
0008	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1001	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1001AA	N/A	N/A	N/A	Government
1001AB	N/A	N/A	N/A	Government
1002	Destination	Government	Destination	Government
1003	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1004	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1005	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1005AA	N/A	N/A	N/A	Government
1005AB	N/A	N/A	N/A	Government
1006	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1007	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
1008	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2001	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government

2001AA	N/A	N/A	N/A	Government
2001AB	N/A	N/A	N/A	Government
2002	Destination	Government	Destination	Government
2003	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2004	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2005	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2005AA	N/A	N/A	N/A	Government
2005AB	N/A	N/A	N/A	Government
2006	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2007	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
2008	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3001	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3001AA	N/A	N/A	N/A	Government
3001AB	N/A	N/A	N/A	Government
3002	Destination	Government	Destination	Government
3003	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3004	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government

3005	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3005AA	N/A	N/A	N/A	Government
3005AB	N/A	N/A	N/A	Government
3006	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3007	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
3008	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4001	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4001AA	N/A	N/A	N/A	Government
4001AB	N/A	N/A	N/A	Government
4002	Destination	Government	Destination	Government
4003	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4004	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4005	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4005AA	N/A	N/A	N/A	Government
4005AB	N/A	N/A	N/A	Government
4006	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government

4007	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government
4008	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government	PFPA PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	UIC
0001	POP 01-MAY-2007 TO 31-OCT-2007	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
0001AA	N/A	N/A	N/A	N/A
0001AB	N/A	N/A	N/A	N/A
0002	N/A	N/A	N/A	N/A
0003	POP 01-MAY-2007 TO 31-OCT-2007	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
0004	POP 01-MAY-2007 TO 31-OCT-2007	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
0005	POP 01-MAY-2007 TO 31-OCT-2007	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
0005AA	N/A	N/A	N/A	N/A
0005AB	N/A	N/A	N/A	N/A

0006	POP 01-MAY-2007 TO 31-OCT-2007	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
0007	POP 01-MAY-2007 TO 31-OCT-2007	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
0008	POP 01-MAY-2007 TO 31-OCT-2007	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
1001	POP 01-NOV-2007 TO 31-OCT-2008	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
1001AA	N/A	N/A	N/A	N/A
1001AB	N/A	N/A	N/A	N/A
1002	N/A	N/A	N/A	N/A
1003	POP 01-NOV-2007 TO 31-OCT-2008	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
1004	POP 01-NOV-2007 TO 31-OCT-2008	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
1005	POP 01-NOV-2007 TO 31-OCT-2008	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
1005AA	N/A	N/A	N/A	N/A
1005AB	N/A	N/A	N/A	N/A
1006	POP 01-NOV-2007 TO 31-OCT-2008	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
1007	POP 01-NOV-2007 TO 31-OCT-2008	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020

1008	POP 01-NOV-2007 TO 31-OCT-2008	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
2001	POP 01-NOV-2008 TO 31-OCT-2009	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
2001AA	N/A	N/A	N/A	N/A
2001AB	N/A	N/A	N/A	N/A
2002	N/A	N/A	N/A	N/A
2003	POP 01-NOV-2008 TO 31-OCT-2009	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
2004	POP 01-NOV-2008 TO 31-OCT-2009	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
2005	POP 01-NOV-2008 TO 31-OCT-2009	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
2005AA	N/A	N/A	N/A	N/A
2005AB	N/A	N/A	N/A	N/A
2006	POP 01-NOV-2008 TO 31-OCT-2009	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
2007	POP 01-NOV-2008 TO 31-OCT-2009	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
2008	POP 01-NOV-2008 TO 31-OCT-2009	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
3001	POP 01-NOV-2009 TO 31-OCT-2010	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
3001AA	N/A	N/A	N/A	N/A
3001AB	N/A	N/A	N/A	N/A
3002	N/A	N/A	N/A	N/A

3003	POP 01-NOV-2009 TO 31-OCT-2010	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
3004	POP 01-NOV-2009 TO 31-OCT-2010	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
3005	POP 01-NOV-2009 TO 31-OCT-2010	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
3005AA	N/A	N/A	N/A	N/A
3005AB	N/A	N/A	N/A	N/A
3006	POP 01-NOV-2009 TO 31-OCT-2010	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
3007	POP 01-NOV-2009 TO 31-OCT-2010	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
3008	POP 01-NOV-2009 TO 31-OCT-2010	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
4001	POP 01-NOV-2010 TO 31-OCT-2011	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
4001AA	N/A	N/A	N/A	N/A
4001AB	N/A	N/A	N/A	N/A
4002	N/A	N/A	N/A	N/A
4003	POP 01-NOV-2010 TO 31-OCT-2011	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
4004	POP 01-NOV-2010 TO 31-OCT-2011	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020

4005	POP 01-NOV-2010 TO 31-OCT-2011	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
4005AA	N/A	N/A	N/A	N/A
4005AB	N/A	N/A	N/A	N/A
4006	POP 01-NOV-2010 TO 31-OCT-2011	N/A	PFPA TIM DARR PENTAGON FORCE PROTECTION AGENCY 100 BOUNDRY CHANNEL DRIVE ARLINGTON VA 22202 703-601-2396/97 FOB: Destination	HQ0020
4007	POP 01-NOV-2010 TO 31-OCT-2011	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020
4008	POP 01-NOV-2010 TO 31-OCT-2011	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0020

CLAUSES INCORPORATED BY REFERENCE

52.203-3	Gratuities	APR 1984
52.203-6 Alt I	Restrictions On Subcontractor Sales To The Government (Sep 2006) -- Alternate I	OCT 1995
52.204-4	Printed or Copied Double-Sided on Recycled Paper	AUG 2000
52.204-9	Personal Identity Verification of Contractor Personnel	NOV 2006
52.212-4	Contract Terms and Conditions--Commercial Items	SEP 2005
52.212-4 Alt I	Contract Terms and Conditions--Commercial Items (Feb 2007)	FEB 2007
52.219-16	Liquidated Damages-Subcontracting Plan	JAN 1999
52.227-14	Rights in Data--General	JUN 1987
52.227-14 Alt III	Rights in Data--General (Jun 1987) - Alternate III	JUN 1987
52.227-19	Commercial Computer Software- Restricted Rights	JUN 1987
52.228-5	Insurance - Work On A Government Installation	JAN 1997
52.233-1	Disputes	JUL 2002
52.242-13	Bankruptcy	JUL 1995
52.243-3	Changes--Time-And-Material Or Labor-Hours	SEP 2000
52.244-2	Subcontracts	AUG 1998
52.244-2 Alt I	Subcontracts (Aug 1998) - Alternate I	JAN 2006
52.244-6	Subcontracts for Commercial Items	SEP 2006
52.245-2	Government Property (Fixed Price Contracts)	MAY 2004
52.245-9	Use And Charges	AUG 2005
52.246-2	Inspection Of Supplies--Fixed Price	AUG 1996
52.246-4	Inspection Of Services--Fixed Price	AUG 1996
52.246-6	Inspection--Time-And-Material And Labor-Hour	MAY 2001
52.247-34	F.O.B. Destination	NOV 1991

52.249-14	Excusable Delays	APR 1984
52.253-1	Computer Generated Forms	JAN 1991
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7002	Display Of DOD Hotline Poster	DEC 1991
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7004 Alt A	Central Contractor Registration (52.204-7) Alternate A	NOV 2003
252.204-7005	Oral Attestation of Security Responsibilities	NOV 2001
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Terrorist Country	DEC 2006
252.225-7012	Preference For Certain Domestic Commodities	JAN 2007
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	JUN 1995
252.227-7019	Validation of Asserted Restrictions--Computer Software	JUN 1995
252.232-7010	Levies on Contract Payments	DEC 2006
252.243-7001	Pricing Of Contract Modifications	DEC 1991
252.243-7002	Requests for Equitable Adjustment	MAR 1998
252.244-7000	Subcontracts for Commercial Items and Commercial Components (DoD Contracts)	NOV 2005
252.245-7001	Reports Of Government Property	MAY 1994

CLAUSES INCORPORATED BY FULL TEXT

52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS--COMMERCIAL ITEMS (NOV 2006)

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

(1) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(2) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Pub. L. 108-77, 108-78).

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

X__ (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (SEP 2006), with Alternate I (OCT 1995) (41 U.S.C. 253g and 10 U.S.C. 2402).

___ (2) 52.219-3, Notice of HUBZone Small Business Set-Aside (Jan 1999) (15 U.S.C. 657a).

___ (3) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (JUL 2005) (if the offeror elects to waive the preference, it shall so indicate in its offer) (15 U.S.C. 657a).

___(4) [Removed].

___ (5)(i) 52.219-6, Notice of Total Small Business Set-Aside (JUNE 2003) (15 U.S.C. 644).

___ (ii) Alternate I (OCT 1995) of 52.219-6.

___ (iii) Alternate II (MAR 2004) of 52.219-6.

___ (6)(i) 52.219-7, Notice of Partial Small Business Set-Aside (JUNE 2003) (15 U.S.C. 644).

___ (ii) Alternate I (OCT 1995) of 52.219-7.

___ (iii) Alternate II (MAR 2004) of 52.219-7.

_X_ (7) 52.219-8, Utilization of Small Business Concerns (MAY 2004) (15 U.S.C. 637 (d)(2) and (3)).

_X_ (8)(i) 52.219-9, Small Business Subcontracting Plan (SEP 2006) (15 U.S.C. 637(d)(4)).

___ (ii) Alternate I (OCT 2001) of 52.219-9

___(iii) Alternate II (OCT 2001) of 52.219-9.

_X_ (9) 52.219-14, Limitations on Subcontracting (DEC 1996) (15 U.S.C. 637(a)(14)).

___ (10)(i) 52.219-23, Notice of Price Evaluation Adjustment for Small Disadvantaged Business Concerns (SEP 2005) (10 U.S.C. 2323) (if the offeror elects to waive the adjustment, it shall so indicate in its offer).

___ (ii) Alternate I (JUNE 2003) of 52.219-23.

___ (11) 52.219-25, Small Disadvantaged Business Participation Program--Disadvantaged Status and Reporting (OCT 1999) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (12) 52.219-26, Small Disadvantaged Business Participation Program--Incentive Subcontracting (OCT 2000) (Pub. L. 103-355, section 7102, and 10 U.S.C. 2323).

___ (13) 52.219-27, Notice of Total Service-Disabled Veteran-Owned Small Business Set-Aside (May 2004).

_X_ (14) 52.222-3, Convict Labor (JUNE 2003) (E.O. 11755).

_X_ (15) 52.222-19, Child Labor--Cooperation with Authorities and Remedies (JAN 2006) (E.O. 13126).

_X_ (16) 52.222-21, Prohibition of Segregated Facilities (FEB 1999).

_X_ (17) 52.222-26, Equal Opportunity (APR 2002) (E.O. 11246).

_X_ (18) 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).

_X_ (19) 52.222-36, Affirmative Action for Workers with Disabilities (JUN 1998) (29 U.S.C. 793).

_X_ (20) 52.222-37, Employment Reports on Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans (SEP 2006) (38 U.S.C. 4212).

_X_ (21) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (DEC 2004) (E.O. 13201).

___ (22)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Products (AUG 2000) (42 U.S.C. 6962(c)(3)(A)(ii)).

___ (ii) Alternate I (AUG 2000) of 52.223-9 (42 U.S.C. 6962(i)(2)(c)).

_X_ (23) 52.225-1, Buy American Act--Supplies (JUNE 2003) (41 U.S.C. 10a-10d).

___ (24)(i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (NOV 2006) (41 U.S.C. 10a-10d, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, Pub. L 108-77, 108-78, 108-286, 109-53 and 109-169).

___ (ii) Alternate I (JAN 2004) of 52.225-3.

___ (iii) Alternate II (JAN 2004) of 52.225-3.

___ (25) 52.225-5, Trade Agreements (NOV 2006) (19 U.S.C. 2501, et seq., 19 U.S.C. 3301 note).

___ (26) 52.225-13, Restrictions on Certain Foreign Purchases (FEB 2006) (E.O.s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of Treasury).

___ (27) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (42 U.S.C. 5150).

___ (28) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (42 U.S.C. 5150).

___ (29) 52.232-29, Terms for Financing of Purchases of Commercial Items (FEB 2002) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

____ (30) 52.232-30, Installment Payments for Commercial Items (OCT 1995) (41 U.S.C. 255(f), 10 U.S.C. 2307(f)).

_X__ (31) 52.232-33, Payment by Electronic Funds Transfer--Central Contractor Registration (OCT 2003) (31 U.S.C. 3332).

____ (32) 52.232-34, Payment by Electronic Funds Transfer--Other than Central Contractor Registration (MAY 1999) (31 U.S.C. 3332).

____ (33) 52.232-36, Payment by Third Party (MAY 1999) (31 U.S.C. 3332).

____ (34) 52.239-1, Privacy or Security Safeguards (AUG 1996) (5 U.S.C. 552a).

____ (35)(i) 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).

____ (ii) Alternate I (APR 2003) of 52.247-64.

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

____ (1) 52.222-41, Service Contract Act of 1965, as Amended (JUL 2005) (41 U.S.C. 351, et seq.).

____ (2) 52.222-42, Statement of Equivalent Rates for Federal Hires (MAY 1989) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

____ (3) 52.222-43, Fair Labor Standards Act and Service Contract Act--Price Adjustment (Multiple Year and Option Contracts) (NOV 2006) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

____ (4) 52.222-44, Fair Labor Standards Act and Service Contract Act--Price Adjustment (February 2002) (29 U.S.C. 206 and 41 U.S.C. 351, et seq.).

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

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

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

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

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c), and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in paragraphs (i) through (vi) of this paragraph in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause--

(i) 52.219-8, Utilization of Small Business Concerns (May 2004) (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 $550,000 ($1,000,000 for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(ii) 52.222-26, Equal Opportunity (April 2002) (E.O. 11246).

(iii) 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).

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

(v) 52.222-39, Notification of Employee Rights Concerning Payment of Union Dues or Fees (DEC 2004) (E.O. 13201).

(vi) 52.222-41, Service Contract Act of 1965, as Amended (Jul 2005), flow down required for all subcontracts subject to the Service Contract Act of 1965 (41 U.S.C. 351, et seq.).

(vii) 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)

52.216-18 ORDERING. (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from 01 May 2007 through 31 Oct 2011.

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

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized in the Schedule.

(End of clause)

52.216-19 ORDER LIMITATIONS. (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $2,000.00 the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

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

(1) Any order for a single item in excess of $5,000,000.00;

(2) Any order for a combination of items in excess of $10,000,000.00; or

(3) A series of orders from the same ordering office within2 days that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.

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

(d) Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 5 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

52.216-20 DEFINITE QUANTITY. (OCT 1995)

(a) This is a definite-quantity, indefinite-delivery contract for the supplies or services specified, and effective for the period stated, in the Schedule.

(b) The Government shall order the quantity of supplies or services specified in the Schedule, and the Contractor

shall furnish them when ordered. Delivery or performance shall be at locations designated in orders issued in accordance with the Ordering clause and the Schedule.

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

(d) Any order issued during the effective period of this contract and not completed within that time shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 31 April 2012.

(End of clause)

52.216-22 INDEFINITE QUANTITY. (OCT 1995)

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

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

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

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 30 April 2012.

(End of clause)

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

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

(End of clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within 14 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.
(End of clause)

52.232-7 PAYMENTS UNDER TIME AND MATERIALS AND LABOR HOUR CONTRACTS (FEB 2007)

The Government will pay the Contractor as follows upon the submission of vouchers approved by the Contracting Officer or the authorized representative:

(a) Hourly rate. (1) Hourly rate means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are--

(i) Performed by the Contractor;

(ii) Performed by the subcontractors; or

(iii) Transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control.

(2) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the Schedule by the number of direct labor hours performed.

(3) The hourly rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by employees that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.

(4) The hourly rates shall include wages, indirect costs, general and administrative expense, and profit. Fractional parts of an hour shall be payable on a prorated basis.

(5) Vouchers may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer), to the Contracting Officer or authorized representative. The Contractor shall substantiate vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by--

(i) Individual daily job timekeeping records;

(ii) Records that verify the employees meet the qualifications for the labor categories specified in the contract; or

(iii) Other substantiation approved by the Contracting Officer.

(6) Promptly after receipt of each substantiated voucher, the Government shall, except as otherwise provided in this contract, and subject to the terms of paragraph (e) of this clause, pay the voucher as approved by the Contracting Officer or authorized representative.

(7) Unless otherwise prescribed in the Schedule, the Contracting Officer may unilaterally issue a contract modification requiring the Contractor to withhold amounts from its billings until a reserve is set aside in an amount

that the Contracting Officer considers necessary to protect the Government's interests. The Contracting Officer may require a withhold of 5 percent of the amounts due under paragraph (a) of this clause, but the total amount withheld for the contract shall not exceed $50,000. The amounts withheld shall be retained until the Contractor executes and delivers the release required by paragraph (g) of this clause.

(8) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis. If no overtime rates are provided in the Schedule and overtime work is approved in advance by the Contracting Officer, overtime rates shall be negotiated. Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract. If the Schedule provides rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.

(b) Materials. (1) For the purposes of this clause--

(i) Direct materials means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.

(ii) Materials means--

(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the Contractor under a common control;

(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;

(C) Other direct costs (e.g., incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.); and

(D) Applicable indirect costs.

(2) If the Contractor furnishes its own materials that meet the definition of a commercial item at 2.101, the price to be paid for such materials shall not exceed the Contractor's established catalog or market price, adjusted to reflect the--

(i) Quantities being acquired; and

(ii) Actual cost of any modifications necessary because of contract requirements.

(3) Except as provided for in paragraph (b)(2) of this clause, the Government will reimburse the Contractor for allowable cost of materials provided the Contractor--

(i) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or

(ii) Ordinarily makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.

(4) Payment for materials is subject to the Allowable Cost and Payment clause of this contract. The Contracting Officer will determine allowable costs of materials in accordance with Subpart 31.2 of the Federal Acquisition Regulation (FAR) in effect on the date of this contract.

(5) The Contractor may include allocable indirect costs and other direct costs to the extent they are--

(i) Comprised only of costs that are clearly excluded from the hourly rate;

(ii) Allocated in accordance with the Contractor's written or established accounting practices; and

(iii) Indirect costs are not applied to subcontracts that are paid at the hourly rates.

(6) To the extent able, the Contractor shall--

(i) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and

(ii) Take all cash and trade discounts, rebates, allowances, credits, salvage, commissions, and other benefits. When unable to take advantage of the benefits, the Contractor shall promptly notify the Contracting Officer and give the reasons. The Contractor shall give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that have accrued to the benefit of the Contractor, or would have accrued except for the fault or neglect of the Contractor. The Contractor shall not deduct from gross costs the benefits lost without fault or neglect on the part of the Contractor, or lost through fault of the Government.

(7) Except as provided for in 31.205-26(e) and (f), the Government will not pay profit or fee to the prime Contractor on materials.

(c) If the Contractor enters into any subcontract that requires consent under the clause at 52.244-2, Subcontracts, without obtaining such consent, the Government is not required to reimburse the Contractor for any costs incurred under the subcontract prior to the date the Contractor obtains the required consent. Any reimbursement of subcontract costs incurred prior to the date the consent was obtained shall be at the sole discretion of the Government.

(d) Total cost. It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule, and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during performing this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performing this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.

(e) Ceiling price. The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the Contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.

(f) Audit. At any time before final payment under this contract, the Contracting Officer may request audit of the vouchers and supporting documentation. Each payment previously made shall be subject to reduction to the extent of amounts, on preceding vouchers, that are found by the Contracting Officer or authorized representative not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. Upon receipt and approval of the voucher designated by the Contractor as the ``completion voucher'' and supporting documentation, and upon compliance by the Contractor with all terms of this contract (including, without limitation, terms relating to patents and the terms of paragraph (g) of this clause), the Government shall promptly pay any balance due the Contractor. The completion voucher, and supporting documentation, shall be submitted by the

Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(g) Assignment and Release of Claims. The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions:

(1) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible of exact statement by the Contractor.

(2) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(3) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(h) Interim payments on contracts for other than services.

(1) Interim payments made prior to the final payment under the contract are contract financing payments. Contract financing payments are not subject to the interest penalty provisions of the Prompt Payment Act.

(2) The designated payment office will make interim payments for contract financing on the [Contracting Officer insert day as prescribed by agency head; if not prescribed, insert ``30th''] day after the designated billing office receives a proper payment request. In the event that the Government requires an audit or other review of a specific payment request to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the specified due date.

(i) Interim payments on contracts for services. For interim payments made prior to the final payment under this contract, the Government will make payment in accordance with the Prompt Payment Act (31 U.S.C. 3903) and prompt payment regulations at 5 CFR part 1315.

(End of Clause)

52.232-19 AVAILABILITY OF FUNDS FOR THE NEXT FISCAL YEAR (APR 1984)

Funds are not presently available for performance under this contract beyond 31 Oct 2007. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond 31 Oct 2007, 31 Oct 2008, 31 Oct 2009, 31 Oct 2010 and 31 Oct 2011 respectively until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

52.233-4 APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004)

United States law will apply to resolve any claim of breach of this contract.

(End of clause)

52.244-5 COMPETITION IN SUBCONTRACTING (DEC 1996)

(a) The Contractor shall select subcontractors (including suppliers) on a competitive basis to the maximum practical extent consistent with the objectives and requirements of the contract.

(b) If the Contractor is an approved mentor under the Department of Defense Pilot Mentor-Protege Program (Pub. L. 101–510, section 831 as amended), the Contractor may award subcontracts under this contract on a noncompetitive basis to its proteges.

(End of clause)

52.246-19 WARRANTY OF SYSTEMS AND EQUIPMENT UNDER PERFORMANCE SPECIFICATIONS OR DESIGN CRITERIA (MAY 2001)

Definitions. Acceptance means the act of an authorized representative of the Government by which the Government assumes for itself, or as an agent of another, ownership of existing and identified supplies, or approves specific services rendered, as partial or complete performance of the contract.

Defect means any condition or characteristic in any supplies or services furnished by the Contractor under the contract that is not in compliance with the requirements of the contract.

Supplies means the end items furnished by the Contractor and related services required under this contract. Except when this contract includes the clause entitled Warranty of Data, supplies also mean ``data."

(b) Contractor's obligations. (1) The Contractor's warranties under this clause shall apply only to those defects discovered by either the Government or the Contractor within one year of testing and acceptance by the Government.

(2) If the Contractor becomes aware at any time before acceptance by the Government (whether before or after tender to the Government) that a defect exists in any supplies or services, the Contractor shall (i) promptly correct the defect, or (ii) promptly
notify the Contracting Officer, in writing, of the defect, using the same procedures prescribed in paragraph (b)(3) of this clause.

(3) If the Contracting Officer determines that a defect exists in any of the supplies or services accepted by the Government under this contract, the Contracting Officer shall promptly notify the Contractor of the defect, in writing, within 45 daysafter discovery of the defect. Upon timely notification of the existence of a defect, or if the Contractor independently discovers a defect in accepted supplies or services, the Contractor shall submit to the Contracting Officer, in writing, within 30 days a recommendation for corrective actions, together with supporting information in sufficient detail for the Contracting Officer to determine what corrective action, if any, shall be undertaken.

(4) The Contractor shall promptly comply with any timely written direction from the Contracting Officer to correct or partially correct a defect, at no increase in the contract price.

(5) The Contractor shall also prepare and furnish to the Contracting Officer data and reports applicable to any

correction required under this clause (including revision and updating of all other affected data called for under this contract) at no increase in the contract price.

(6) In the event of timely notice of a decision not to correct or only to partially correct, the Contractor shall submit a technical and cost proposal within 30 days to amend the contract to permit acceptance of the affected supplies or services in accordance with the revised requirement, and an equitable reduction in the contract price shall promptly be negotiated by the parties and be reflected in a supplemental agreement to this contract.

(7) Any supplies or parts thereof corrected or furnished in replacement and any services reperformed shall also be subject to the conditions of this clause to the same extent as supplies or services initially accepted. The warranty, with respect to these supplies, parts, or services, shall be equal in duration to that set forth in paragraph (b)(1) of this clause, and shall run from the date of delivery of the corrected or replaced supplies.

(8) The Contractor shall not be responsible under this clause for the correction of defects in Government-furnished property, except for defects in installation, unless the Contractor performs, or is obligated to perform, any modifications or other work on such property. In that event, the Contractor shall be responsible for correction of defects that result from the modifications or other work.

(9) If the Government returns supplies to the Contractor for correction or replacement under this clause, the Contractor shall be liable for transportation charges up to an amount equal to the cost of transportation by the usual commercial method of shipment from the place of delivery specified in this contract (irrespective of the f.o.b. point or the point of acceptance) to the Contractor's plant and return to the place of delivery specified in this contract. The Contractor shall also bear the responsibility for the supplies while in transit.

(10) All implied warranties of merchantability and "fitness for a particular purpose" are excluded from any obligation under this contract.

(c) Remedies available to the Government. (1) The rights and remedies of the Government provided in this clause--

(i) Shall not be affected in any way by any terms or conditions of this contract concerning the conclusiveness of inspection and acceptance; and

(ii) Are in addition to, and do not limit, any rights afforded to the Government by any other clause of this contract.

(2) Within 30 days after receipt of the Contractor's recommendations for corrective action and adequate supporting information, the Contracting Officer, using sole discretion, shall give the Contractor written notice not to correct any defect, or to correct or partially correct any defect within a reasonable time at the location specified in the applicable Delivery Order.

(3) In no event shall the Government be responsible for any extension or delays in the scheduled deliveries or periods of performance under this contract as a result of the Contractor's obligations to correct defects, nor shall there be any adjustment of the delivery schedule or period of performance as a result of the correction of defects unless provided by a supplemental agreement with adequate consideration.

(4) This clause shall not be construed as obligating the Government to increase the contract price.

(5)(i) The Contracting Officer shall give the Contractor a written notice specifying any failure or refusal of the Contractor to--

(A) Present a detailed recommendation for corrective action as required by paragraph (b)(3) of this clause;

(B) Correct defects as directed under paragraph (b)(4) of this clause; or

(C) Prepare and furnish data and reports as required by paragraph (b)(5) of this clause.

(ii) The notice shall specify a period of time following receipt of the notice by the Contractor in which the Contractor must remedy the failure or refusal specified in the notice.

(6) If the Contractor does not comply with the Contracting Officer's written notice in paragraph (c)(5)(i) of this clause, the Contracting Officer may by contract or otherwise--

(i) Obtain detailed recommendations for corrective action and either--

(A) Correct the supplies or services; or

(B) Replace the supplies or services, and if the Contractor fails to furnish timely disposition instructions, the Contracting Officer may dispose of the nonconforming supplies for the Contractor's account in a reasonable manner, in which case the Government is entitled to reimbursement from the Contractor, or from the proceeds, for the reasonable expenses of care and disposition, as well as for excess costs incurred or to be incurred;

(ii) Obtain applicable data and reports; and

(iii) Charge the Contractor for the costs incurred by the Government.

(End of clause)

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

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

http://farsite.hill.af.mil/

(End of clause)

252.212-7001 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMENT STATUTES OR EXECUTIVE ORDERS APPLICABLE TO DEFENSE ACQUISITIONS OF COMMERCIAL ITEMS (JUN 2006)

(a) The Contractor agrees to comply with the following Federal Acquisition Regulation (FAR) clause which, if checked, is included in this contract by reference to implement a provision of law applicable to acquisitions of commercial items or components.

____ 52.203-3 Gratuities (APR 1984) (10 U.S.C. 2207).

(b) The Contractor agrees to comply with any clause that is checked on the following list of Defense FAR Supplement clauses which, if checked, is included in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items or components.

____252.205-7000 Provision of Information to Cooperative Agreement Holders (DEC 1991) (10 U.S.C. 2416).

_X___252.219-7003 Small, Small Disadvantaged and Women-Owned Small Business Subcontracting Plan (DoD Contracts) (APR 1996) (15 U.S.C. 637).

____ 252.219-7004 Small, Small Disadvantaged and Women-Owned Small Business Subcontracting Plan (Test Program) (JUN 1997) (15 U.S.C. 637 note).

_X___ 252.225-7001 Buy American Act and Balance of Payments Program (JUN 2005) (41 U.S.C. 10a-10d, E.O. 10582).).

_X___ 252.225-7012 Preference for Certain Domestic Commodities (JUN 2004) (10 U.S.C. 2533a).

_X___ 252.225-7014 Preference for Domestic Specialty Metals (JUN 2005) (10 U.S.C. 2533a).

_X___ 252.225-7015 Restriction on Acquisition of Hand or Measuring Tools (JUN 2005) (10 U.S.C. 2533a).

____ 252.225-7016 Restriction on Acquisition of Ball and Roller Bearings (MAR 2006) (Section 8065 of Public Law 107-117 and the same restriction in subsequent DoD appropriations acts).

____ 252.225-7021 Trade Agreements (JUN 2006) (19 U.S.C. 2501-2518 and 19 U.S.C. 3301 note).

____ 252.225-7027 Restriction on Contingent Fees for Foreign Military Sales (APR 2003) (22 U.S.C. 2779).

____ 252.225-7028 Exclusionary Policies and Practices of Foreign Governments (APR 2003) (22 U.S.C. 2755).

____ 252.225-7036 Buy American Act--Free Trade Agreements--Balance of Payments Program (JUN 2006) (------ Alternate I) (JAN 2005) (41 U.S.C. 10a-10d and 19 U.S.C. 3301 note).

____ 252.225-7038 Restriction on Acquisition of Air Circuit Breakers (JUN 2005) (10 U.S.C. 2534(a)(3)).

_____ 252.226-7001 Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns (SEP 2004) (Section 8021 of Public Law 107-248 and similar sections in subsequent DoD appropriations acts).

_X___ 252.227-7015 Technical Data--Commercial Items (NOV 1995) (10 U.S.C. 2320).

_X___ 252.227-7037 Validation of Restrictive Markings on Technical Data (SEP 1999) (10 U.S.C. 2321).

_X__ 252.232-7003 Electronic Submission of Payment Requests (MAY 2006) (10 U.S.C. 2227).

_____ 252.237-7019 Training for Contractor Personnel Interacting with Detainees (SEP 2005) (Section 1092 of Pub. L. 108-375).

____ 252.243-7002 Requests for Equitable Adjustment (MAR 1998) (10 U.S.C. 2410).

_X___ 252.247-7023 Transportation of Supplies by Sea (MAY 2002) (_____Alternate I) (MAR 2000) (_____Alternate II) (MAR 2000) (____Alternate III (May 2002).

____252.247-7024 Notification of Transportation of Supplies by Sea (MAR 2000) (10 U.S.C. 2631).

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

252.225-7014 Preference for Domestic Specialty Metals, Alternate I (APR 2003) (10 U.S.C. 2533a).

252.237-7019 Training for Contractor Personnel Interacting with Detainees (SEP 2005) (Section 1092 of Pub. L. 108-375).

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)

CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The COR is a representative for the Government with limited authority who has been designated in writing by the Contracting Officer to provide technical direction, clarification, and guidance with respect to existing specifications and statement of work (SOW)/statement of objectives (SOO) as established in the contract. The COR also monitors the progress and quality of the Contractor's performance for payment purposes. The COR shall promptly report Contractor performance discrepancies and suggested corrective actions to the Contracting Officer for resolution.

The COR is NOT authorized to take any direct or indirect actions or make any commitments that will result in changes to price, quantity, quality, schedule, place of performance, delivery or any other terms or conditions of the written contract.

The Contractor is responsible for promptly providing written notification to the Contracting Officer if it believes the COR has requested or directed any change to the existing contract (or task/delivery order). No action shall be taken by the Contractor for any proposed change to the contract until the Contracting Officer has issued a written directive or written modification to the contract (or task/delivery order). The Government will not accept and is not liable for any alleged change to the contract unless the change is included in a written contract modification or directive signed by the Contracting Officer.

If the Contracting Officer has designated an Alternate COR (ACOR), the ACOR may act only in the absence of the COR (due to such reasons as leave, official travel, or other reasons for which the COR is expected to be gone and not readily accessible for the day).

COR authority IS NOT delegable.

INVOICING INSTRUCTIONS (WHS, A&PO Mar 2007)

In compliance with DFARS 252.232-7003, "Electronic Submission of Payment Request (March 2003)", Washington Headquarters Services, Acquisition & Procurement Office (WHS, A&PO) utilizes WAWF-RA to electronically process vendor request for payment. The web based system is located at https://wawf.eb.mil, which provides the technology for government contractors and authorized Department of Defense (DOD) personnel to generate, capture and process receipt and payment-related documentation in a paperless environment. The contractor is required to utilize this system when submitting invoices and receiving reports under this contract. Submission of hard copy DD250/Invoice/Public Vouchers (SF1034) will no longer be accepted for payment.

The contractor shall (i) ensure an Electronic Business Point of Contract is designated in Central Contractor Registration at http://www.ccr.gov/ and (ii) register to use WAWF-RA at https://wawf.eb.mil
within ten (10) days after award of the contract or modification incorporating WAWF-RA into the contract. The designated CCR EB point of contact is responsible for activating the company's CAGE code on WAWF by calling

1-866-618-5988. Once the company CCR EB is activated, the CCR EB will self-register on the WAWF and follow the instructions for a group administrator. Step by step instructions to register are available at http://wawf.eb.mil.

The contractor is directed to select either "Invoice as 2-in-1" for services only or "Invoice and Receiving Report (Combo)" for supplies or any combination of goods and services. Both types of invoices fulfill the requirement for submission of the Material Inspection and Receiving Report, DD Form 250.

Back up documentation may be attached to the invoice in WAWF under the "Misc Info" tab. Fill in all applicable information under each tab.

The following required information should automatically pre-populate in WAWF; if it does not populate, or does not populate correctly, enter the following information:

"Issue by DoDAAC" field enter **HQ0034**

"Admin DoDAAC" field enter **HQ0034**

"Payment DoDAAC" field enter HQ0338

"Service Acceptor/Extension" or "Ship to/ Extension" field enter HQ0020 and 4500.

"Inspect By DoDAAC/ EXT" fields "Leave Blank"

"LPO DoDAAC/ EXT" fields - Leave blank

Contractor shall verify that the DoDAACs automatically populated by the WAWF-RA system match the above information. If these DoDAACs do not match then the contractor shall correct the field(s) and notify the contracting officer of the discrepancy (ies).

Take special care when entering Line Item information . The Line Item tab is where you will detail your request for payment and material/services that were provided based upon the contract. Be sure to fill in the following items exactly as they appear in the contract:

- Item Number: If the contract schedule has more than one ACRN listed as sub items under the applicable Contract Line Item Number (CLIN), use the 6 character, separately identified Sub Line Item Number (SLIN) (e.g. – 0001AA) or Informational SLIN (e.g. – 000101), otherwise use the 4 character CLIN (e.g. – 0001).

- ACRN: Fill-in the applicable 2 alpha character ACRN that is associated with the CLIN or SLIN.

Note – DO NOT INVOICE FOR MORE THAN IS STILL AVAILABLE UNDER ANY CLIN/SLIN/ ACRN.

- Unit Price

- Unit of Measure

Shipment numbers must be formatted as follows:

Three (3) alpha characters followed by four (4) numeric characters.

For Services, enter 'SER' followed by the last 4 digits of the invoice number.

For Construction, enter 'CON' followed by the last 4 digits of the invoice number.

For Supplies, enter 'SUP' followed by the last 4 digits of the invoice number.

If the invoice number is less than 4 digits, enter leading zeros.

Before closing out of an invoice session in WAWF-RA but after submitting your document or documents, the contractor will be prompted to send additional email notifications. Contractor shall click on "Send More Email Notification" on the page that appears. Add the following email address john.hundley.ctr@whs.mil, sue.miller@pfpa.mil, mary.marshall@pfpa.mil, edna.rogers@pfpa.mil, denise.powell@pfpa.mil,and tim.darr@pfpa.mil. in the first email address block and add any other additional email addresses desired in the following blocks. This additional notification to the government is important to ensure that all appropriate persons are aware that the invoice documents have been submitted into the WAWF-RA system.

If you have any questions regarding WAWF, please contact the WAWF Help Desk at 1-866-618-5988.

LOCAL CLAUSES, SPECIAL CONTRACT REQUIREMENTS

The following full-text local clauses are incorporated into this contract

H-1 Subcontracting Goals
H-2 Public Holidays
H-3 Key Personnel
H-4 Pentagon Delivery Requirements
H-5 Security Requirements

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Attachment 1	HQ0034-07-R-1016 CDRL # 1	1	
Attachment 10	HQ0034-07-R-1016 CDRL #10	1	
Attachment 11	HQ0034-07-R-1016 CDRL #11	1	
Attachment 12	HQ0034-07-R-1016 CDRL #12	1	
Attachment 13	HQ0034-07-R-1016 CDRL #13	1	
Attachment 14	HQ0034-07-R-1016 CDRL #14	1	
Attachment 15	HQ0034-07-R-1016 CDRL #15	1	
Attachment 16	HQ0034-07-R-1016 CDRL #16	1	
Attachment 17	HQ0034-07-R-1016 CDRL #17	1	
Attachment 18	HQ0034-07-R-1016 CDRL #18	1	
Attachment 19	HQ0034-07-R-1016 CDRL #19	1	

Attachment 2	HQ0034-07-R-1016 CDRL #2	1
Attachment 20	HQ0034-07-R-1016 CDRL #20	1
Attachment 21	HQ0034-07-R-1016 CDRL #21	1
Attachment 22	HQ0034-07-R-1016 CDRL #22	1
Attachment 23	HQ0034-07-R-1016 CDRL #23	1
Attachment 24	HQ0034-07-R-1016 CDRL #24	1
Attachment 25	HQ0034-07-R-1016 CDRL #25	1
Attachment 26	HQ0034-07-R-1016 CDRL #26	1
Attachment 27	HQ0034-07-R-1016 CDRL #27	1
Attachment 28	DD Form 254, Contract Security Classification Specification	2
Attachment 29	DD Form 254, Block 13 Continuations	3
Attachment 3	HQ0034-07-R-1016 CDRL #3	1
Attachment 30	DD Form 254, attach 1	3
Attachment 31	DD Form 254, attach 2	2
Attachment 4	HQ0034-07-R-1016 CDRL #4	1
Attachment 5	HQ0034-07-R-1016 CDRL #5	1
Attachment 6	HQ0034-07-R-1016 CDRL #6	1
Attachment 7	HQ0034-07-R-1016 CDRL #7	1
Attachment 8	HQ0034-07-R-1016 CDRL #8	1
Attachment 9	HQ0034-07-R-1016 CDRL #9	1

H-1 SUBCONTRACTING GOALS

H-1 SUBCONTRACTING GOALS

The following subcontracting goals have been established for this requirement:

Small Business	30%
HUBZone SB	4%
SDB	14%
WOSB	6%
SDVOSB	2%

H-2 PUBLIC HOLIDAYS

H-2 PUBLIC HOLIDAYS

The following are the public holidays observed by the federal workforce during the performance of this contract:

New Years Day	Martin Luther King's Birthday	Presidents Birthday
Memorial Day	Independence Day	Labor Day
Columbus Day	Veteran's Day	Thanksgiving Day
Christmas Day	Inauguration Day*	

*Inauguration Day is only a holiday if deemed a holiday for Federal Government employees.

The contractor is expected to deliver the performance requirements specified in the Statement of Objectives (SOO) regardless of the holidays affecting the federal workforce.

H-3 KEY PERSONNEL

H-3 KEY PERSONNEL

- The Contractor shall notify the Contracting Officer prior to making any changes in personnel assigned to key positions under this contract and all resultant Delivery/Task Orders. The key positions are identified as follows:

  Program Manager
  Installation Services Manager
  Maintenance/Repair Chief
  Logistics Manager
  Quality Control Manager
  Information Assurance Officer

- During the first 180 calendar days of performance, the Contractor shall make no substitutions of key personnel unless illness, death, or termination of employment necessitates the substitution. The Contractor shall notify the Contracting Officer as soon as possible after the occurrence of any of these events and provide the information required below. After the initial 180 calendar day period, the Contractor may propose substitutions. The Contractor shall provide a detailed explanation of the circumstances necessitating the proposed substitutions, complete resumes for the proposed substitutes, and any additional information requested by the Contracting Officer. The Contractor shall, prior to making any substitution permanent, demonstrate to the satisfaction of the Contracting Officer that the qualifications of the proposed substitute personnel are equal to or better than the qualifications of the personnel originally identified for the position. The Contracting Officer will notify the Contractor within 15 calendar days after receipt of all required information of the decision on proposed substitutions.

H-4 PENTAGON DELIVERY RQMT

H-4 PENTAGON DELIVERY REQUIREMENTS

All persons and vehicles requiring access to deliver, transport, pick-up goods, services and materials to the Pentagon Reservation and associated buildings will be processed through the Pentagon Remote Delivery Facility (RDF). Persons must adhere to the current delivery and security requirements and procedures below:

- The following information must be provided in advance to the COR, through the prime contractor:

1. Driver name
2. Company
3. Government POC
4. Vehicle description
5. Tag number

- Once at the RDF the following will occur:
  1. Drivers and passengers must have a valid Pentagon Pass and or have a favorable national criminal investigation check conducted,
  2. Driver must have 2 forms of ID
  3. Driver must have a valid drivers licensed
  4. The vehicle will be inspected by K-9

Hours of Operation
0400-1600 Mon-Friday
0600-1400 Sat

Failure to follow the above procedures will result in the delivery being rejected at the RDF and will not be considered a Government caused delay for performance considerations.

H-5 SECURITY REQUIREMENTS

H-5 SECURITY REQUIREMENTS

Upon award and prior to commencement of work, the Contractor shall provide the Contracting Officer with written certification that the Contractor has been granted a Facility Security Clearance (FCL) by the Defense Security Service (DSS), at the SECRET level or higher (No Storage Requirement), and that the FCL is active and in good standing. Classification guidance is contained in the DD Form 254, Contract Security Classification Specification issued as part of this Task Order. As required, the Contractor shall be provided further guidance in writing on a revised DD 254.

Within 45 days of award, the Contractor shall provide to the Contracting Officer, written certification that all Contractor employees assigned against this Task Order have been granted at least an Interim eligibility for access to classified information at the SECRET level.

Contractor employees performing work against this Contract shall be required to provide personal identification information, sufficient for the Government to conduct a National Crime Information Center (NCIC) files inquiry by submitting a completed DD Form 2249, DOD Building Pass Application to the COR for processing. Upon favorable adjudication of this inquiry, the employee shall be issued a temporary DOD Building Pass, and granted interim access to PENREN Information Technologies (IT) systems. Upon receipt of notification from the Contractor's Facility Security Officer that the individual has been granted at least interim eligibility for access to classified information, a permanent DOD Building Pass will be issued. Unfavorable adjudication of the NCIC shall result in the individual shall be denied a DOD Building Pass and unless issues are sufficiently mitigated, shall be removed from the project.

STATEMENT OF OBJECTIVES

STATEMENT OF OBJECTIVES

FOR

PENTAGON FORCE PROTECTION AGENCY (PFPA)

INTEGRATED SECURITY SERVICES CONTRACT (ISSC)

Prepared by

PFPA, SECURITY SERVICES DIRECTORATE

1.0 SCOPE

1.1 Summary Information 7

1.2 Objectives 7
1.2.1 Interoperability 8
1.2.2 Scalability 8

1.3 Current Situation 9
1.3.1 Pentagon Reservation & Government Owned/Leased Facilities within NCR 9
1.3.1.1 Location 9
1.3.1.2 Operation 10

1.4 Desired Situation 10
1.4.1 Pentagon Reservation & Government Owned/Leased Facilities within NCR 10
1.4.1.1 Location 11
1.4.1.2 Operation 11

1.5 Summary of Services and Materials Requested 11
1.5.1 Management and Personnel 11
1.5.2 System Engineering and Planning 12
1.5.3 Subsystem Descriptions 12
1.5.3.1 Common Support Systems 12
1.5.3.2 Command, Control, and Communications System 12
1.5.3.3 Access Control System 12
1.5.3.4 Intrusion Detection System 13
1.5.3.5 Assessment System 13
1.5.3.6 Video Badging 13
1.5.3.7 Active/Passive Barrier Systems 13
1.5.3.8 Security Booths, Kiosks and Bullet Resistant Components 14
1.5.3.9 Screening Devices 14
1.5.4 Installation and Testing 14
1.5.5 Supplemental Requirements 14
1.5.5.1 Integrated Logistics Support 14
1.5.5.2 Quality Assurance/Quality Control Program 15
1.5.5.3 Technical Services 15

2.0 REFERENCES 15

2.1 Government Documents 15
2.1.1 Code of Federal Regulations (CFR) 15
2.1.2 Department of Defense (DOD) & Unified Facility Guide Specifications (UFGS) 15
2.1.3 National Institute of Standards and Technology (NIST) 17

2.2 Commercial Documents 17
2.2.1 American National Standards Institute (ANSI) 17
2.2.2 Institute of Electrical and Electronics Engineers (IEEE) 18
2.2.3 International Telegraph and Telephone Consultative Committee (CCITT) 18
2.2.4 International Organization for Standardization(ISO) 18
2.2.5 National Fire Protection Association (NFPA) 19

2.2.6 Underwriters Laboratory (UL) 19

2.3 Acronyms 19

2.4 Definitions 22

3.0 REQUIREMENTS 25

3.1 Management and Personnel 25
3.1.1 Contractor Management 25
3.1.1.1 Program Management 25
3.1.1.2 Program Management Plan 25
3.1.1.3 Program Schedule 26
3.1.1.4 Review Meetings 26
3.1.1.5 Reports 26
3.1.2 Contractor Personnel Qualifications 27
3.1.2.1 Contractor Representatives 27
3.1.2.2 Minimum Personnel Qualifications 27
3.1.2.3 Specific Personnel Qualifications 27
3.1.2.4 Conduct of Personnel 29
3.1.2.5 Facility Clearance 29
3.1.2.6 Personnel Security Clearances 29

3.2 System Engineering and Planning 30
3.2.1 Site Survey Report 30
3.2.2 Technical Design Package 30

3.3 Subsystem Detailed Requirements 31
3.3.1 Common Support Systems 31
3.3.1.1 Computers 31
3.3.1.2 Network Equipment 32
3.3.1.3 Cabling and Associated Hardware 32
3.3.1.4 Uninterruptible Power Supplies (UPS) 32
3.3.2 Command, Control, and Communications System (CCCS) 33
3.3.2.1 ACS/IDS/Assessment Front End 33
3.3.2.2 Computer Aided Dispatch/Records Management System (CAD/RMS) 35
3.3.2.3 Radio System 36
3.3.2.4 Audio Source Recording (ASR) 36
3.3.3 Access Control System (ACS) 37
3.3.3.1 Access Control Host and Peripherals 37
3.3.3.2 Delayed Door Egress System (DDES) 39
3.3.3.3 Guard Patrol Supervisory System (GPSS) 40
3.3.3.4 Vehicle Entry Control System 40
3.3.3.5 Visual Image Recognition System (VIRS) 41
3.3.4 Intrusion Detection Systems (IDS) 41
3.3.4.1 Primary Intrusion Detection System 42
3.3.4.2 Audio Duress System (ADS) 43
3.3.4.3 Electronic Article Surveillance System (EASS) 44
3.3.5 Assessment System 44
3.3.5.1 Video Assessment System (VAS) 44
3.3.5.2 Audio Assessment System (AAS) 45
3.3.6 Video Badging System (VBS) 46
3.3.6.1 System Description 46
3.3.6.2 Performance Requirements 46
3.3.7 Passive and Active Barrier Systems (PABS) 46
3.3.7.1 System Description 46
3.3.7.2. Performance Requirements 47
3.3.8. Security Booths, Kiosks, and Bullet resistant Components 47
3.3.8.1. System Description 47
3.3.8.2. Performance Requirements 47
3.3.9. Screening Devices 47
3.3.9.1. System Description 47
3.3.9.2. Performance Requirements 48

3.4 Security System Installation and Testing 48
3.4.1 Pre-Delivery Testing 48
3.4.2 Installation 48

3.4.2.1 Installation Tools and Permits....48
3.4.2.2 Installation Practices....48
3.4.2.3 Interfacing with Existing Equipment....49
3.4.2.4 As Built Drawings....49
3.4.3 Post Installation Testing....49

3.5 Integrated Logistics Support....49
3.5.1 Automated Integrated Logistics Support (ILS) Program....49
3.5.1.1 Maintenance Management System (MMS)....50
3.5.1.2 Warranty Management System (WMS)....50
3.5.1.3 Training Management System (TMS)....51
3.5.1.4 Configuration Management System (CMS)....51
3.5.1.5 Documentation Management System (DMS)....51
3.5.1.6 Management System Reports....51
3.5.2 Maintenance Plan....51
3.5.2.1 Hardware Maintenance....51
3.5.2.2 Replacement Parts....51
3.5.2.3 Software Maintenance....52
3.5.2.4 Preventive Maintenance....52
3.5.2.5 On-Call Maintenance....52
3.5.2.6 Technical Support....53
3.5.3 Warranty....53
3.5.4 Training....53
3.5.5 Configuration Management....54
3.5.6 System Manual....54
3.5.6.1 Technical Module....55
3.5.6.2 Hardware Module....55
3.5.6.3 Operating System Software Module....56
3.5.6.4 Application Software Module....56
3.5.6.5 Operations Module....56
3.5.7 Risk Management Plan....57
3.5.8 Quality Assurance/Quality Control (QA/QC) Program....57
3.5.9 Technical Services....57
3.5.9.1 Security Industry Evaluation....57
3.5.9.2 Replacement and Upgrade....57
3.5.9.3 ISSC Testbed....58

3.6 Information Assurance....58
3.6.1 Certification and Accreditation (C&A)....58

3.6.2 System Security 58

3.7 Contract Support Information 59
3.7.1 General 59
3.7.1.1 Scope Of Work 59
3.7.1.2 Background Information 60
3.7.1.3 Government Observations 60
3.7.1.4 Interface with Government Operation 60
3.7.1.5 Safety 60
3.7.1.6 Security 62
3.7.1.7 Conservation of Utilities 62
3.7.1.8 Codes 62
3.7.2 Property Installed at the Pentagon and Services 62
3.7.2.1 Property 62
3.7.2.2 Services 63
3.7.3 Contractor Furnished Items 63
3.7.3.1 Property 63
3.7.3.2 Property Storage 64
3.7.3.3 Disposal of Damaged or Removed Equipment 64
3.7.3.4 Housekeeping Practices 64
3.7.4 Applicable Documents 64
3.7.5 Proposal Response 64
3.8 Organizational Conflict of Interest 65

1.0 Scope

1.1 Summary Information

The Integrated Security Services Contract (ISSC) is a total system approach to automating and improving the physical security system used to protect Department of Defense (DoD) sites including, the Pentagon, and sites within the National Capitol Region (NCR). ISSC emphasizes the use of computer-based solutions to meet security requirements and integrates the operation of multiple subsystems to improve efficiency and control. Functions and processes within ISSC are divided into 9 major subsystem categories, which are:

a) common support systems
b) command, control, & communications systems
c) access control systems
d) intrusion detection systems
e) assessment systems
f) video badging systems
g) Active/Passive barrier systems
h) Security Booths, Kiosks and Bullet Resistant Components (BRC)
i) Screening Devices

These major subsystem categories are further divided into minor subsystems, which are defined in subsequent requirements paragraphs. An ISSC is designed and built from the available subsystems to meet individual site requirements. Other types of security, access control and or detection systems may apply in order to encompass unique requirements.

1.2 Objectives

The objective of the ISSC is the design, procurement, installation, training, and maintenance of automated, integrated physical security systems for multiple DoD sites. The overriding design requirement for each of the computer-based subsystems within ISSC shall use open systems design concepts, which are compatible with existing systems. Open systems are those that conform to open specifications[1] for interfaces, services, and supporting formats. This conformance enables properly engineered subsystems to be easily integrated into a wide variety of systems with minimal changes to interoperate with other subsystems. Integration of the various computer-based subsystems shall be accomplished through compliance with standard interfaces defined by standards bodies such as International Organization for Standardization (ISO), American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), and applicable DOD Regulations. Adherence to this design philosophy is intended to foster the overall objective of effectively and efficiently designing, procuring, installing, operating, and maintaining automated, integrated physical security systems through the benefits of interoperability and scalability.

[1] An open specification (or standard) is a public specification that is maintained by an open, public consensus process to accommodate new technology over time and that is consistent with standards.

1.2.1 Interoperability

Interoperability allows a diverse mix of subsystems to operate together as an integrated whole, sharing data and tools in a useful and transparent fashion. Interoperability of components and subsystems is a key design requirement for ISSC and requires the use of subsystems designed to the maximum extent practicable with open standards and defacto open standards.[2] Wherever possible, the equipment offered by vendors should interoperate with existing equipment to save replacement costs. However, it is recognized that some replacement will be required especially in the upper levels of an existing system architecture. New equipment offered by the Contractor for implementation in later years of the ISSC shall be operationally compatible with equipment previously procured and installed under this contract to the maximum extent practicable.

[2]A defacto open standard is one that belongs to a particular company or organization but is widely available to others through licensing.

Wherever computers are required, they shall be widely available models based on open systems architecture, using multiple manufacturers as sources for components and spare parts.

ISSC subsystem computers shall use common widely used buses, including but not limited to ISA, EISA, PCI, S-BUS, and VME. The Contractor shall provide converters, if required, to join unlike buses together.

Standard network protocols shall be used, such as Transmission Control Protocol / Internet Protocol (TCP/IP) layered over open standard physical layer protocols such as Ethernet, token ring, or Fiber Distributed Data Interface (FDDI) for Local Area Networks (LANs) and X.25, frame relay or Asynchronous Transfer Mode (ATM) for wide area networks. A LAN shall provide a pathway for data exchange among various ISSC computer-based subsystems.

ISSC computer databases shall be Structured Query Language (SQL) compliant to provide commonality to database interfaces.

1.2.2 Scalability

Scalability requires that it be possible for a diverse mix of ISSC subsystems and components to be combined and configured to meet widely varying site requirements. Through open system design ISSC shall be scaleable from the smallest system requirements such as a single small building to very large system requirements such as a large building or a campus made up of several buildings. ISSC shall accommodate a range of system sizes, both physical and functional.

1.3 Current Situation

1.3.1 Pentagon Reservation and Government Owned/Leased Facilities in the National Capital Region

The Pentagon Force Protection Agency (PFPA) provides physical security for both perimeter and interior spaces of the Pentagon Reservation and over 140 Government owned and leased facilities. Department of Defense (DoD) activities located in these buildings can also request additional security services on a cost reimbursable basis. DOD regulations mandate minimum-security requirements for all DoD facilities. PFPA and each individual security manager have some flexibility in meeting/exceeding minimum-security requirements based on site-specific needs & mission requirements.

1.3.1.1 Location

All physical security work is performed in buildings, or campus style environments within PFPA areas of responsibility located within the National Capital Region. This primarily encompasses Maryland, Pennsylvania, the District of Columbia and Virginia, but can include other areas within the United States or Overseas as defined by PFPA. The buildings are categorized into four groups: Pentagon Reservation, Government Owned Buildings, Government Leased Buildings and Residences in a combination of both urban/rural environments.

1.3.1.1.1 Pentagon Reservation

The DoD owns the Pentagon Reservation, which includes the Pentagon, Navy Annex and the Heating and Refrigeration Plant. The reservation is located in Arlington County, VA and therefore State and local laws, codes and ordinances are jurisdictional to the Pentagon Reservation. The Pentagon is being renovated with the completion date currently projected in 2011. This renovation will be conducted in six segments. The basement is one segment. The rest of the Pentagon is divided into five equal segments, which are planned to be designed, and constructed one segment at a time.

1.3.1.1.2 Government Facilities

The Government owns and leases approximately 140 buildings for DoD in the NCR. The DoD is responsible for the security at many of these buildings.

1.3.1.1.3 Residences

The residences of the Secretary of Defense and Deputy Secretary of Defense and others as designated by PFPA are or will be equipped with security equipment, which is installed, operated, and maintained by PFPA.

1.3.1.2 Operation

Security equipment is installed to secure the perimeter of buildings and interior office spaces. Internal spaces must be secured in accordance with (IAW) all applicable DOD regulations to include but not limited to Director, Central Intelligence Directive (DCID) 6/9, DCID 6/3 Protecting Sensitive Compartmented Information within Information Systems, DOD 5200.28 Security Requirements for Automated Information Systems, DOD 5200.400 Information Technology Security Certification and Accreditation Process, DOD 5220.22M National Industrial Security Program Operating Manual (NISPOM), DOD 5200.1R Information Security Program, and Administrative Instruction (AI-26) Office Secretary of Defense Supplement to DOD 5200.1R.

1.3.1.2.1 Intrusion Detection System (IDS)

The IDS is used to alert the security force of an unauthorized entry. Duress alarms are used to protect key personnel. Equipment enclosures are protected with tamper circuits. IDS sensors of various types are used to protect exterior doors, windows, interior office doors, and office spaces. Motion sensors are used to protect various perimeter areas.

1.3.1.2.2 Access Control System

A digital video badging system creates a DoD Building pass, which is used for access control. The video badging system and the access control systems are linked via network such that badge numbers and necessary personnel data is passed to the access control system automatically upon badge creation. Homeland Security Presidential Directive 12 (HSPD 12) mandates a common identification standard for federal employees and contractors. Based upon this directive, the National Institute for standards and

technology (NIST) developed the Federal Information Processing Standards Publication 201 (FIPS 201). Current specifications are defined by SEIWG-012, but subject to change as per FIPS 201 implementation.

1.3.1.2.3 Assessment System

The assessment system allows law enforcement personnel to monitor and assess public areas through the use of video cameras and audio intercommunication. The Closed Circuit Television (CCTV) system is used to monitor interior and exterior areas. The signals are transmitted over fiber cable, coaxial cable, telephone lines or wireless. An audio duress system is used to communicate between the monitoring office and remote intercom devices.

1.4 Desired Situation

1.4.1 Pentagon Reservation and Government Owned/Leased facilities within NCR

PFPA will continue to provide security for the perimeter and interior spaces of the Pentagon and over 140 other buildings. The ISSC contractor shall perform system engineering, installation, maintenance and monitoring of the various security systems as directed by PFPA.

1.4.1.1 Location

All physical security work is performed in buildings, or campus style environments within PFPA areas of responsibility located within the National Capital Region. This encompasses Maryland, Pennsylvania, the District of Columbia and Virginia. The buildings are categorized into four groups: Pentagon Reservation, Government Owned Buildings, Government Leased Buildings and Residences in a combination of urban/rural environments

1.4.1.2 Operation

Security equipment is installed to secure the perimeter of buildings and interior office spaces. Internal spaces must be secured in accordance with all applicable DOD regulations to include but not limited to Director, Central Intelligence Directive (DCID) 6/9, DCID 6/3 Protecting Sensitive Compartmented Information within Information Systems, DOD 5200.28 Security Requirements for Automated Information Systems, DOD 5200.400 Information Technology Security Certification and Accreditation Process, DOD 5220.22M National Industrial Security Program Operating Manual (NISPOM), DOD 5200.1R Information Security Program, and Administrative Instruction (AI-26) Office Secretary of Defense Supplement to DOD 5200.1R

Increasing amounts of automated security equipment will be installed to secure the perimeter of buildings and interior office spaces to include; offices, supply rooms, and utility rooms (electrical, mechanical, communications). The use of digital video badging systems to create building passes and ID badges with standardized badge numbers encoded on magnetic stripe or smart chip is expected to increase and promote sharing of badges among DoD facilities. HSPD-12 and FIPS-201 specifications outline these new requirements and are referenced in performance criteria of systems below. Electronic article surveillance will be increasingly common to protect the DoD from loss of pilferable equipment and materials. The use

of automated situation assessment systems will increase in all facilities allowing control center personnel to monitor public areas and respond quickly to situations. The DoD facilities, as a whole, require a complete integrated physical security system. Systems designed will be open and interoperable with other existing systems located within DoD.

1.5 Summary of Services and Materials Requested

The Contractor shall provide the complete services necessary for the delivery of requested security systems at the Pentagon and other DoD sites as specified in individual delivery orders.

1.5.1 Management and Personnel

The Contractor shall function under a management structure, which supports the analysis, system engineering, design, purchase, installation, maintenance support and training of large-scale security systems at multiple sites occurring simultaneously at geographically diverse locations.

1.5.2 System Engineering and Planning

Contractors shall provide professional system engineering services and be trained, certified, licensed and experienced in the installation, application and maintenance of complex security systems, to include cost estimating, planning, design, integration, programming, training and maintenance, which can be scaled to support small areas such as a utility closet to larger complexes such as the Pentagon which has numerous entry points, thousands of tenants, visitors, and hundreds of internally controlled spaces.

1.5.3 Subsystem Descriptions

The Contractor shall provide a complete system including the hardware and software necessary for the operation of a turn-key security system. The general performance requirements for the nine major sub-system components are defined in the following paragraphs.

1.5.3.1 Common Support Systems

All of the subsystems that form a part of ISSC require common support systems or components. These items may include: computers, network equipment; cabling (twisted pair, coaxial, wireless and fiber), associated cabling hardware (transceivers, connectors, terminators, patch panels, and racks), and uninterruptible power supplies. These items are the basic components of ISSC, which shall be usable and interchangeable throughout ISSC.

1.5.3.2 Command, Control, and Communications System

The Command, Control, and Communications System (CCCS) serves as the focal point of ISSC where several subsystems are integrated. It provides the hardware and software that can control all other ISSC subsystems and provide a common user interface to the ISSC operator. The CCCS may also support a Computer Aided Dispatch/Records Management System (CAD/RMS), a Radio System, Audio Source Recording (ASR) and Mustering System.

1.5.3.3 Access Control System

The Access Control System (ACS) provides automated control of designated doors, turnstiles, gates and vehicle barriers through various types of identification devices. In an integrated system, this subsystem is centrally controlled by the CCCS front-end host, which may have several associated client stations to allow monitoring, and management functions to be performed from several different locations. At the periphery it is made up of access control devices and associated hardware including, but not limited to card readers, keypads, biometric personal identity verification devices, and locking devices. Between these end devices and the CCCS host processor, the Independent Local Processor (ILP) serves to distribute the capability of the ACS by hosting portions of the main access control database and independently controlling a segment of the overall system. An ILP can be connected directly to the CCCS front end or may be connected to another ILP, which is in turn connected to the CCCS front end. Communication occurs between the host and an ILP on an as needed basis to report events to the host and update the ILP's database. This hierarchical architecture allows for scalability from very small systems up to very large systems. The ACS may also include a Delayed Door Egress System (DDES), a Guard Patrol Supervisory System (GPSS), a Vehicle Entry Control System, and a Video Recognition System (VIRS).

1.5.3.4 Intrusion Detection System

The Intrusion Detection System (IDS) provides monitoring of alarm sensors connected to the inputs of an ILP. In an integrated system, this subsystem is centrally controlled by the CCCS front-end computer. At the periphery it is made up of alarm initiating devices and associated hardware including, but not limited to door contacts, motion sensors, video motion sensors, glass shock sensors, cabinet tamper switches, duress switches, and exterior perimeter protection devices. Between these end devices and the CCCS host processor, the ILP serves to distribute the capability of the IDS. An ILP can be connected directly to the CCCS front end or may be connected to another ILP, which is in turn connected to the CCCS front end. This hierarchical tree architecture allows for scalability from very small systems up to very large systems. The IDS may also include an Audio Duress System (ADS) and a Electronic Article Surveillance System (EASS).

1.5.3.5 Assessment System

The Assessment System, which consists of the Video Assessment System (VAS) and the Audio Assessment System (AAS), allows law enforcement personnel to monitor and assess public areas through the use of video cameras and audio intercommunication devices. It is an integrated subsystem of ISSC, which is interfaced to and controlled by the CCCS front-end system. The closed circuit television equipment includes, but is not limited to cameras, housings, mounts, lenses, signal amplification, and equalization devices, transmission media, recording equipment, switching/control equipment, and lighting enhancements. Audio intercoms are coupled to CCTV cameras for alarm caller assessment purposes. Master intercoms are also integrated with ISSC Command and Control to facilitate communications between control room personnel and remote sites. A determination will be made during the Site Survey process whether the sites existing phone system/lines may be used for the AAS.

1.5.3.6 Video Badging

The Video Badging System (VBS) consists of a system of personal computers equipped with video cameras and badge printers operating networked to enable multiple enrollment and administration workstations to provide cardholder enrollments, badge issuance, database configuration, and report functions.[3] A commonality of communications protocols and database applications between the VBS and the ISSC CCCS allows the exchange of data for automatic enrollment of new cardholders into the ISSC access control system database and retrieval of video image and badge data information for card holders from the VBS database.[4] The VBS must be compatible with FIPS –201 standards.

1.5.3.7 Active/Passive barrier systems

The Passive and Active Vehicle Barrier Systems consist of all industry and DoD Force Protection standard barrier systems, to include but not limited to; barriers, traffic control, landscaping, environmental design, physical perimeter security and vehicle standoff strategies which support security and law enforcement operations. Contractor shall comply with minimum requirements set forth in UFC 4-022-02, Selection and Application of Vehicle Barriers, as well as requirements set forth in IDO's.

1.5.3.8 Security Booths, Kiosks and Bullet Resistant Components (BRC)

The Security Booths, Kiosks and Bullet Resistant Components (BRC) shall consists of all material, labor and equipment to fabricate, deliver and install (BR) hardened security booths, desks, kiosks, and vehicle/pedestrian "access point" structures, for both interior/exterior applications, IAW DoD Regulations, Force Protection Standards, Unified Facility Criteria (UFC), NCPC, and site specific design/property owner constraints. These Kiosks will house a variety of security controls, systems and equipment as defined by individual delivery orders.

1.5.3.9 Screening Devices

Screening devices shall consist of all electronic systems designed to detect contraband, weapons, hazardous materials, CBRN or other prohibited items, to include but not limited to x-ray machines, metal detectors, hand held detectors and mobile screening systems.

1.5.4 Installation and Testing

The Contractor shall be responsible for the complete configuration, system engineering, programming, integration, shipment, installation, and testing of systems as per Individual Delivery Orders (IDO). The Contractor shall develop a system, which shall support site-specific Government requirements. The Contractor shall provide the services of a qualified team of installation professionals with the necessary experience to install the equipment properly while having minimal effect on the day-to-day operations of the facility.

[3]The VBS may be a single standalone badge station for small sites with low badge populations.

[4]The access control database and badging system databases may simply be separate, linked tables within the same database server.

1.5.5 Supplemental Requirements

1.5.5.1 Integrated Logistics Support

The Contractor shall develop a comprehensive integrated logistics support (ILS) program, which shall control and monitor the status of all installed equipment using an automated system. The Contractor shall provide training and maintenance services to support the deployed equipment and permit the facility to utilize the ISSC to its maximum effectiveness. The Contractor shall use an automated program, which shall track, and control all documentation associated with the ISSC program.

1.5.5.2 Quality Assurance/Quality Control Program

The Contractor shall develop a quality control and assurance program, which shall aid in the satisfactory performance of all tasks under this contract and compliance with all applicable DOD Regulations, Instructions, Codes, and Standards. To include but not limited to Probability of Detection, False Alarm Rates, and Acceptable Quality Levels.

1.5.5.3 Technical Services

The Contractor shall maintain a testbed, conduct briefings, industry demonstrations, and on-site support of all ISSC equipment.

2.0 References

2.1 Government Documents

2.1.1 Code of Federal Regulations (CFR)

47 CFR 15	Radio Frequency Devices
21 CFR 1020	Performance Standards for Ionizing Radiation Emitting Product
32 CFR-32	Conduct on the Pentagon Reservation

2.1.2 Department of Defense (DOD)

AI-26	Administrative Instruction-26, Office of Secretary of Defense (OSD) Information Security Supplement
AI-30	Administrative Instruction-30, Security for Pentagon Reservation
DCID 6/3	Protecting Sensitive Compartmented Information within Information Systems

DCID-6/9	Physical Security Standards of Sensitive Compartmented Information Facilities (SCIF).
DCSSC (May 2002)	Pentagon Renovation (PENREN) Design and Construction, Security Standards & Criteria
DOD 2000.12	DOD Anti-Terrorism, Force Protection (AT/FP) Program
DOD 2000.12H	DOD AT/FP Handbook
DOD 2000.16	DOD Anti-Terrorism, Standards
DoD Dir. 5220.22M	National Industry Security Program Operating Manual, January 1995.
DoD Dir. 5200.1R	Information Security Program
DoD Dir. 5200.8R	Security of DOD Installations and Resources
DOD 5200.28	Security Requirements for Automated Information Systems
DOD 5200.400	Information Technology Security Certification and Accreditation Process
DOD 8500.1	Information Assurance (IA)
DOD 8500.2	Information Assurance (IA) Implementation
DODD O-8530.1	Computer Network Defense (CND)
DOD 8570.1	Information Assurance Training, Certification, and Workforce Management
DOD 5400.7-R	DOD Freedom of Information Act Program
FIPS-201	Federal Information Processing Standards Publication (FIPS pub) 201
HSPD-12	Homeland Security Presidential Directive #12
SEIWG-012	Prime Item Product Function Specification for Magnetic Stripe Credentials (2/28/94).
UFC 4-010-01	DOD Minimum Anti-Terrorism Standards for Buildings

UFC 4-022-01	Security Engineering Entry Control Facilities/Access Control Points
UFC 4-022-02	Selection & Application of Vehicle Barriers
UFC 4-022-03	Security Engineering Fences, Gates, and Guard Facilities
UFC 4-020-01	Security Engineering Planning Manual
UFC 4-020-02	Security Engineering Design Manual

Unified Facility Guide Specifications (UFGS)

Note: Used as attachments to Individual Delivery Orders, when completed/edited by Govt. To include, but not limited to the following;

UFGS 02821A	Fencing
UFGS 02821N	Chain Link Fence & Gates
UFGS 02840A	Active Vehicle Barriers
UFGS 02841N	Traffic Barriers
UFGS 08390	Blast Resistant Doors
UFGS 08850	Fragment Retention Film for Glass
UFGS 11035	Bullet Resistant Components
UFGS 13703N	Commercial Intrusion Detection Systems
UFGS 16528A	Exterior Lighting Including Security & CCTV Applications
UFGS 16751A	Closed Circuit Television Systems
UFGS 2820-01.0010	Electronic Safety & Security, Electronic Security Systems

2.1.3 National Institute of Standards and Technology (NIST)

NIST FIPS Pub 46-1	(Jan 1988) Data Encryption Standard

2.2 Commercial Documents

2.2.1 American National Standards Institute (ANSI)

ANSI A 1.4	(1983) Sound Level Meters
ANSI C2(1993)	National Electrical Safety Code
ANSI C2	(1990; TIA 90-2 Errata) National Electrical Safety Code
ANSI X3.64	(1979; R 1990) Additional controls for Use with American National Standard Code for Information Interchange
ANSI X3.135	(1992) Information Systems - Database Language SQL (Includes ANSI X3.168-1989)
ANSI X3.154	(1988) Office Machines and Supplies - Alphanumeric Machines-Keyboard Arrangement
ANSI X3.166	(1990) Fiber Distributed Data Interface (FDDI) Physical Layer Medium Dependent
ANSI X3.92	(1981; R 1988) Data Encryption Standard

2.2.2 Institute of Electrical and Electronics Engineers (IEEE)

IEEE C62.41	(1991) Surge Voltages in Low-Voltage AC Power Circuits
IEEE Std 100	(1988) IEEE Standard Dictionary of Electrical and Electronics Terms
IEEE Std 142	(1991) IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems
IEEE Std 446	(1987) Emergency and Standby Systems for Industrial and Commercial Applications

2.2.3 International Telegraph and Telephone Consultative Committee (CCITT)

CCITT-01	(1988) Data Communication Over the Telephone Network, Series V Recommendations (CCITT Blue Book - Vol. VIII - fascicle VIII.1)

2.2.4 International Organization for Standardization(ISO)

ISO 9002 -	Standards and Quality
ISO 7810	(1985) Identifications Cards - Physical Characteristics
ISO 7811/1	(1985) Identification Cards - Recording Technique, Part 1: Embossing
ISO 7811/2	(1985) Identification Cards - Recording Technique, Part 2:Magnetic Stripe
ISO 7811/3	(1985) Identification Cards - Recording Technique, Part 3: Location of Embossed Characters on I0-1 Cards
ISO 7811/4	(1985) Identification Cards - Recording Technique, Part 4: Location of Read-Only Magnetic Tracks 1 and 2
ISO 7811/5	(1985) Identification Cards - Recording Technique, Part 5: Location of Read-Write Magnetic Track - Track 3
ISO/IEC 8802.3	(1993) [ANSI/IEEE Std. 802.3, 1993 Edition], Information Technology -- Local and Metropolitan area networks -- Part 3: Carrier Sense Multiple Access with collision detection (CSMA/CD) access method physical layer specifications
ISO 10007	Quality Management - Guidelines for Configuration Management

2.2.5 National Fire Protection Association (NFPA)

NFPA 70	(1993) National Electrical Code

2.2.6 Underwriters Laboratory (UL)

UL294	Standard for Access Control System Units

UL1076	Standard for Proprietary Burglar Alarm Units and Systems
UL 1981	Standard for Central-Station Automation Systems
UL2050	National Industrial Security Systems

2.3 Acronyms

AAS	Audio Assessment System
ACS	Access Control System
ADA	American with Disabilities Act
ADS	Audio Duress System
AILS	Automated Integrated Logistics Systems
ANSI	American National Standards Institute
AQL	Acceptable Quality Level
ASR	Audio Source Recording
ASTM	American Society for testing and materials
ATM	Asynchronous Transfer Mode
AVI	Automatic Vehicle Identification
BMS	Balanced Magnetic Switch
bps	Bits per Second
BR	Bullet Resistant
BRC	Bullet Resistant Components
CAD	Computer Aided Dispatch
CAD/RMS	Computer Assisted Dispatch/Records Management System
CBRN	Chemical Biological Radiological & Nuclear
CCCS	Command Control & Communications System
CCITT	Consultative Committee on International Telegraphy and Telephony
CCTV	Closed Circuit Television
CDRL	Contract Data Requirements List
CFR	Code of Federal Regulations
CM	Configuration Management
CMS	Configuration Management System
COTR	Contracting Officer Technical Representative
CPU	Central Processing Unit
DBMS	Database Management System
DCID	Director Central Intelligence Directive
DDE	Dynamic Data Exchange
DDES	Delayed Door Egress System

DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DoD	Department of Defense
DoS	Department of State
DPI	Dots Per Inch
PFPA	Pentagon Force Protection Agency
ECP	Engineering Change Proposal
EBACS	Electronic Badging and Access Control System
EIA	Electronic Industries Association
EASS	Electronic Article Surveillance System
EMT	Electro-Metallic Tubing
EVI	Electronic Video Imaging
FDDI	Fiber Distributed Data Interface
FIPS-201	Federal Information Processing Standards Publication-201
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GFP	Government Furnished Property
GPSS	Guard Patrol Supervisory System
GSA	General Services Administration
GUI	Graphical User Interface
HSPD-12	Homeland Security Presidential Directive-12
Hz	Hertz (Cycles per Second)
IAW	In Accordance With
IDO	Individual Delivery Order
IDS	Intrusion Detection System
I/O	input/output
IEEE	Institute of Electrical & Electronics Engineers
ILP	Independent Local Processor
ILS	Integrated Logistics Support
ISSC	Integrated Security Services Contract
ISO	International Standards Organization
JPEG	Joint Photographics Expert Group
KB	Kilobytes
Kb/sec	Kilobits per second
kVA	KiloVoltampere
LAN	Local Area Network
LPR	License Plate Reader
MB/sec	Megabytes per Second
Mb	Megabit
MB	Megabyte

MHZ	Megahertz
mm	Millimeters
MMS	Maintenance Management System
MODEM	Modulator - demodulator
ms	millisecond
NCPC	National Capital Planning Commission
NCR	National Capitol Region
NCRMS	National Capitol Region Management System
NEC	National Electrical Code
NFPA	National Fire Protection Association
NIC	Network Interface Card or Not in contract.
NIST	National Institute for Standards and Technology
OLTP	Online Transactions Processing
OSHA	Occupational Safety & Health Administration
OSI	Open Systems Interconnection
PC	Personal Computer
PCI	Peripheral Component Interconnect
PIN	Personal Identification Number
PFPA	Pentagon Force Protection Agency
PLC	Program Logic Controller
PM	Program Manager
QA	Quality Assurance
QC	Quality Control
RAM	Random Access Memory
RMS	Records Management System
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SOW	Statement of Work
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol / Internet Protocol
TDP	Technical Design Package
TMS	Training Management System
UFC	Unified Facility Criteria
UFGS	Unified Facility Guide Specifications
UL	Underwriters Laboratories
UPS	Uninterruptible Power Supply
URL	Underwriters Laboratory
UTP	Unshielded Twisted Pair
WHS	Washington Headquarters Service
VAS	Video Assessment System

VBS	Video Badging System
VGA	Video Graphics Array
VIRS	Visual Imaging Recognition System
WMS	Warranty Management System

2.4 Definitions

ACCEPTABLE QUALITY LEVEL (AQL) - The maximum percent defective, maximum number of defects per hundred units, or number of defects in the lot that can be considered satisfactory on the average, or degree of deviation from perfect performance for such specific contract requirements before the Government shall consider contract performance unacceptable. If the defective performance does not exceed the AQL, the Government shall not reject the service. AQL for IDS/ACS is defined by applicable DOD Regulations for IDS and Access Control Systems to include but not limited to DOD 5200.1R and DCID 6/9. False Alarm Rates shall not exceed one alarm per sensor, per 30-day period per zone. An error rate of 0.01 percent shall be the standard for high security projects within the ISSC program. The ISSC Maintenance and Quality Control & Quality Assurance programs shall be designed to meet or exceed AQL.

ACCESS CONTROL ALARM - An access control alarm shall be enunciated when the ACS detects improper use of ACS procedures or equipment.

CALENDAR DAY. The time from midnight to midnight.

CLOSED DAY - Base closure, on a daily basis, resulting from command decisions.

CONTRACTING OFFICER (Contract Officer) - A person duly appointed with the authority to enter and administer contracts on behalf of the Government.

CONTRACTING OFFICER'S REPRESENTATIVE (Contract Officer Representative) - An individual designated in writing by the Contracting Officer to act as an authorized representative of the Contracting Officer to perform specific contract administrative functions within the scope and limitations as defined by the Contracting Officer. This individual may also be called contracting officer's technical representative (Contracting Officer TR) or technical representative (TR).

CONTRACTOR - The Contractor (KTR), its subsidiaries and affiliates, joint ventures involving the Contractor, or any entity that the Contractor may have merged or any individual or entity that helped or advised the Contractor in the preparation of a proposal under this solicitation.

DEFECT - Any nonconformance of a unit of service with specified requirements.

DURESS ALARM - The ACS shall provide a duress alarm. A duress alarm shall be enunciated when entering a special code into a keypad or by activating a panic switch. This alarm category shall take precedence over other alarm categories.

DOD SITE - Site at which DoD is responsible for security.

FALSE ALARM - A false alarm is the activation of an alarm sensor by some influence that cannot be identified as related to an intrusion attempt or nuisance alarm. False alarms shall not exceed one false alarm per sensor, per 30-day period. The ICCS Maintenance, Quality Control and Quality Assurance Programs shall be designed to track and validate compliance.

GOVERNMENT FURNISHED PROPERTY (GFP) - Defined by the clause FAR 52.245-02 contained in this solicitation.

GUARD TOUR ALARM - The ACS shall provide a guard tour alarm. This shall be a special alarm that is enunciated at the console if a guard is either early or late at a specified check-in location.

INTEGRATION - An engineering process involving the combination and/or configuration of two or more systems or components into a single interoperable system.

INTEROPERABILITY - When two or more systems have been successfully integrated such that they can share data effectively and perform useful functions.

INTRUSION ALARM - The annunciation of an alarm by the ACS when entry into an access-controlled area is attempted without using ACS procedures.

LEGAL PUBLIC HOLIDAYS. Holidays in each calendar year identified as follows:

New Year's Day, January 1;
Martin Luther King's Birthday, the third Monday in January;
Presidents Day, the third Monday in February;
Memorial Day, the last Monday in May;
Independence Day, July 4;
Labor Day, the first Monday in September;
Columbus Day, the second Monday in October;
Veteran's Day, November 11;
Thanksgiving Day, the fourth Thursday in November
Christmas Day, December 25.

The contractor is expected to deliver the performance requirements specified in the Statement of Objectives (SOO) regardless of the holidays affecting the federal workforce.

NUISANCE ALARM - A nuisance alarm is the activation of an alarm sensor by some influence for which the sensor was designed but which is not related to an intrusion attempt. Nuisance alarms shall not exceed 1 alarm per sensor, per 30 days period.

PENTAGON OPERATING HOURS. 6:00 AM to 4:00 PM, Mondays through Fridays, excluding legal public holidays.

POWER LOSS ALARM - The ESS shall detect when system components experience loss of power exceeding 2 seconds, and shall enunciate an alarm. The alarm shall identify the zone experiencing the power loss. Circuitry shall be designed to fail to an alarm condition with the loss of power.

PROBABILTY OF DETECTION - Each zone shall have a continuous probability of detection greater than 90 percent and shall be demonstrated with a confidence level of 95 percent. This probability of detection is defined as 45 successful detections out of 46 tests or 98 successful detections out of 103 tests. The actual number of tests performed, per sensor, to demonstrate system performance shall be nominated by the Contractor in the performance verification test procedures submitted to the Government for approval.

QUALITY ASSURANCE - Those actions taken by the Government to assure that the quality of purchased goods and services received are acceptable according to established standards and requirements of the contract.

QUALITY CONTROL - Those actions taken by the Contractor to control the production of goods or services so that they meet or exceed the requirements of Contract and specific probability of detection and acceptable quality levels for security systems designed, installed, monitored, and maintained.

SYSTEM HEAVY LOAD DEFINITION - System heavy load conditions are defined as the occurrence of alarms at the rate of 10 alarms per second distributed evenly among all local processors in the system. The alarm printer shall continue to print out all occurrences, including time of occurrence, to the nearest second

TYPE I ERROR RATE - A Type I error means that the system denies access to an authorized, enrolled individual.

TYPE II ERROR RATE - A Type II error means that the system grants access to an unauthorized individual.

3.0 Requirements

The Contractor shall provide the necessary services and materials to design, procure, install, secure, perform training, and maintain automated, integrated physical security systems for multiple sites in the DoD within acceptable quality levels.

3.1 Management and Personnel

3.1.1 Contractor Management

This management relates to the overall contract as well as specific management functions related to individual delivery orders within the contract.

3.1.1.1 Program Management

The Contractor shall implement a Program Management structure to efficiently and cost effectively administers the ISSC program. The Contractor shall designate a central point of contact for substantive communication with the Government.

3.1.1.2 Program Management Plan

The Contractor shall implement a detailed plan for the overall management of the ISSC contract. The plan shall be a comprehensive overview of all aspects of the program.

3.1.1.3 Program Schedule

The Contractor shall use a program scheduling software package that is compatible with Primavera to develop and maintain schedules. The software package shall be used to develop schedules for each delivery order as well as the overall ISSC program. These schedules shall be updated on a regular basis to accurately reflect the schedule at any given time. The Government shall have electronic on-line access to the program schedules.

3.1.1.4 Review Meetings

The Contractor shall be responsible for hosting, at their facilities, or attending at other designated sites, ISSC Program Management Meetings. These meetings shall be attended by the prime Contractor, major subcontractors when required, and the Government representatives (which may include other contractors). The meetings will be held to conduct review and discussion of the major aspects of the contracts operation. This includes past period performance and next period performance.

a) The first meeting shall be held within 15 calendar days after contract award. Contractor personnel shall include the program manager, administrative persons*, contracting, the project engineer and the security system analyst.
b) Contract Program Review Meeting shall be conducted once every 3 months (quarterly) and shall include the Program Manager, administrative personnel, contracting and Project Management personnel.
j) Informal "working" meetings can occur as necessary and agreed upon by the Contractor and the Government.
k) Formal "working" meetings shall be scheduled as required to review IDO status.
l) The Contractor shall prepare and submit minutes for all meetings attended by the Government.

*Administrative persons include the contractor personnel responsible for the performance of the company on the contract.

3.1.1.5 Reports

3.1.1.5.1 Program Report

The Contractor shall submit monthly progress reports detailing the status of the ISSC project/contract. This will include overall information and status for the ISSC project and on each active delivery order.

3.1.1.5.2 Delivery Order Report

The Contractor shall submit monthly progress reports for each active delivery order to the Government. These reports shall provide overall status and specific information for the individual delivery orders. The status report shall contain as a minimum the following information:

a) performance issues
b) schedule / status
c) CDRLs

d) integrated logistics reports (inventory, warranty and maintenance)

3.1.2 Contractor Personnel Qualifications

The Contractor shall provide a workforce possessing the skills, knowledge, and training to satisfactorily perform the services required by this contract. The Contractor shall staff the management organization with qualified personnel for the positions described in the following paragraphs. Contractor personnel supporting IA functions shall be appropriately certified in accordance with DOD 8570.01-M prior to being engaged. Contractor personnel who fail to maintain certification shall be removed from the contract. The contractor shall be responsible for any retraining expenses required by the individual to meet certification requirements.

3.1.2.1 Contractor Representatives

Contractor shall provide an on-site person who shall be physically present during normal duty hours to act as site supervisors, and conduct total management coordination and furnish liaison with the Government during system installation. The supervisor shall be the point of contact with the Government. The supervisor shall have the authority to make technical decisions on-site on behalf of the Contractor.

3.1.2.2 Minimum Personnel Qualifications

All Contractor or subcontractor's employees, engaged in the contract activities specified herein, must be licensed by the state, county, and/or local municipal authorities of the given work site. This license pertains to those trades, crafts or professions, which require licensing by such jurisdiction. The license must be of a grade or level consistent with the requirement of the work being performed and/or as established by the appropriate jurisdiction(s). The Contractor shall provide an ongoing employee training program for their employees which shall include, but not be limited to technical training, safety training, and quality assurance/quality control training. This training shall be provided to the necessary personnel performing work under this SOW.

3.1.2.3 Specific Personnel Qualifications

In view of the complexity of the scope of the program and the wide variety of program assignments anticipated under the contract, the following are desired levels of education, training and experience of the technical and management staff to be supplied. A combination of education and experience will be weighted under a "whole person concept", on a case be case basis. Personnel who have been previously denied or relieved of any security duties or other security-related duties for reasons of security violations,negligence or nonperformance of duties will not be deemed acceptable unless specifically approved by the Government and an investigation into the circumstances surrounding the denial.

3.1.2.3.1 Key Personnel

The positions in the following paragraphs are considered key personnel for the execution of this contract. Resumes shall be provided for the personnel in these categories. In the event that any of them must be replaced, or additional personnel required, the replacement or additional resume must be submitted to the KO for approval. Personnel not meeting these requirements may be accepted for these positions upon review and concurrence by the Government Project personnel

and the Contracting Office. Other tasks and/or requirements can be defined in the individual delivery orders.

3.1.2.3.1.1 Program Manager

The Program Manager (PM) shall have, as a minimum, 10 years experience in the application of complex security systems, and a bachelor's degree in, Management, Engineering, Mathematics, Physics, Computer Science, or other related technical field with an advanced degree in operations management or business administration preferred. The PM must be able to manage a large-scale program with multiple technical tasks (delivery orders) requiring the application of considerable knowledge in security equipment, software, engineering, facility operations, management support, and related fields. The PM shall be responsible for briefing a wide range of individuals to include high-ranking members of the United States (US) Government. Incumbent must obtain & maintain a TS/SCI clearance while employed in this duty position.

3.1.2.3.1.2 Installation Services Manager

The Installation Services Managers must have, as a minimum, 5 years experience in the application of complex security systems, general supervision and management of personnel & technical functions. Installation Services Managers are responsible for supervising technicians and coordinating all aspects of the installation of electronic physical security systems at multiple sites in a specific geographic location. The Installation Services Manager assists senior managers in the general management of program installation activities. Incumbent must obtain & maintain a secret clearance while employed in this duty position

3.1.2.3.1.3 Maintenance / Repair Chief

The Maintenance Chief must have, as a minimum, 3 years experience in the application of complex security systems, and 5 years experience in the general supervision and management of personnel or technical functions. Maintenance Chiefs are responsible for coordinating all aspects of the maintenance and support of electronic physical security, passive and active barrier and screening systems. Shall comply with all related requirements and functions as stated in section 3.5. Incumbent must obtain & maintain a secret clearance while employed in this duty position

3.1.2.3.1.4 Quality Control Manager

The Quality Control Manager shall have, as a minimum, a bachelor's degree in a related field or 6 years of experience in the field or in a related field. Quality Control Manager must have extensive knowledge of security installation applications and procedures. Quality Control Manager must have a broad knowledge of all industry standards, local and national building codes, and regulations. Shall comply with all related requirements and functions as stated in section 3.5 Incumbent must obtain & maintain a secret clearance while employed in this duty position.

3.1.2.3.1.5 Logistics Manager

Logistics Managers shall have, as a minimum, an associate's degree or 5 years of experience in logistics or a related field. Shall be responsible for inventory control of all ISSC material including spares, warranties and new systems. Shall comply with all related requirements and

functions as stated in section 3.5. Incumbent must obtain & maintain a secret clearance while employed in this duty position.

3.1.2.3.1.6 Information Assurance Officer (IAO)
The Information Assurance Officer (IAO) shall have, as a minimum, an associate's degree or 5 years of experience in information assurance, and an IAT level III or IAM level I certification as defined in appendix 3 of DOD 8570.01-M. The IAO shall be responsible for developing, implementing, and maintaining a secure enclave environment. Shall comply with all related requirements and functions as stated in section 3.6. Incumbent must obtain and maintain a Top Secret clearance with SCI access while employed in this duty position.

3.1.2.4 Conduct of Personnel
The Contractor's personnel must comply with the rules and regulations of individual sites where work is performed. Failure to do so will result in the Government requiring the Contractor to remove the employee from the job site. The reasons for removal are misconduct; security violations; or being under the influence of alcohol, drugs, or other incapacitating agents. Upon determination by the Government, Contractor employees shall be subject to dismissal from the premises. Such action is necessary in the interests of the Government. The removal from the job site or dismissal from the premises shall not relieve the Contractor of the requirement to provide sufficient personnel to do the services as required by this work statement. Incumbent must obtain & maintain a secret clearance while employed in this duty position.

3.1.2.5 Facility Clearance
The Contractor shall possess or obtain a clearance at the classification level of "TOP SECRET" prior to contract start date. Application for facility clearance shall be made to the Government who will process the application.

3.1.2.6 Personnel Security Clearances
All contract personnel must posses, at minimum a SECRET security clearance and meet the additional security requirements established in the Director of Central Intelligence Directive 6/9 (DCID 6/9) The Contractor shall identify appropriate individual's performing work under this contract that will require access to classified information and shall submit them for "SECRET or TOP SECRET" security clearances within 10 work days after receipt of facility clearance or 10 work days after contract award if the Contractor already possesses a facility clearance. Application for personnel security clearances shall be made in accordance with DoD Directive 5220.22M., Section 2. Applications for new personnel requiring security clearances shall be submitted within 10 workdays of hire by the Contractor. The Government reserves the right to have the contractor provide documentation to verify compliance with these security requirements. All contractor personnel assigned under this contract must possess a clearance consistent with PFPA Personnel Security Clearance Policy and position sensitivity requirements. PFPA-SSD Security will provide security classification guidance for the performance of this contract.

3.2 System Engineering and Planning

The Contractor shall incorporate Government defined security requirements at various facilities within the NCR, as specified in individual delivery orders. Once individual site requirements have been validated and approved by both tenant (owner/user), and the PFPA, the Contractor shall develop a security system concept that meets the defined requirements. To include but not limited to; technical design plan, component integration plans, system integration, cost analysis and installation schedule.

3.2.1 Site Survey Report

As necessary the site survey information shall be compiled into a single document with the raw data from the site including sketches, photographs, survey sheets, and annotated site drawings. This report shall include details about current site conditions that will affect performance of the system to be installed. The Contractor shall document any existing equipment that can be used as part of the security system. The Contractor shall catalogue the equipment as potential Government Furnished Equipment and make a recommendation as to its utility and report any deficiencies. This report shall be delivered to the Government for review and validation.

3.2.2 Technical Design Package

As necessary the Contractor shall prepare a site specific Technical Design Package (TDP) which provides a detailed bill of materials listing all of the hardware and software required to meet the site's specific requirements for a protective system. The TDP shall be comprehensive in identifying the technical steps required to integrate, secure, and install material, and all steps required to achieve a fully functional system in accordance with Government requirements. Where necessary, the TDP shall address the integration of existing systems at a site. The TDP shall provide for the sequence of installation of system components and subsystems and shall clearly identify any schedule constraints or dependencies based on required changes to the site, which are the responsibility of the site. Drawings and written descriptions shall be included which depict and represent the layout of the system in sufficient detail to guide installation and maintenance.

3.3 Subsystem Detailed Requirements

The Contractor shall provide the systems, subsystems, and components described in the following paragraphs. The following information provides the system descriptions and performance requirements for the core ISSC subsystems. ISSC systems at individual sites will combine some or all of these subsystems to build a comprehensive automated physical security system depending on the specific requirements of the site. Some sites may require all of the subsystems while others may require only a few. Some sites will require systems meeting stringent requirements for protection of highly sensitive areas while others only require lower cost systems to protect collateral areas. In each case, the open systems interfaces supported by each subsystem are of paramount importance so that the various combinations can be accomplished with minimal need to perform additional integration and with minimal burden on the end user of the physical security system.

3.3.1 Common Support Systems

Each of the subsystems that form a part of ISSC requires common support systems or components. These items shall include but not limited to computers, network equipment, cabling (twisted pair, coaxial, wireless, and fiber), associated cabling hardware (transceivers, connectors, terminators, patch panels, and racks), and uninterruptible power supplies. These items are the basic hardware components of ISSC, which shall be usable and interchangeable throughout ISSC. This will significantly reduce spare parts requirements, storage requirements, and maintenance costs.

3.3.1.1 Computers

Many of the subsystems that are described in subsequent sections include computers as core parts of their architecture. For every one of these types of system, there are several manufacturers, which sell systems using widely available personal computers (PCs) and/or widely available file servers as client stations and hosts. PCs and fileservers, widely available commercially, provide sufficient computing power to perform the required tasks. The market is also rapidly producing newer and more powerful computers each year as applications grow in functionality and demand more resources. Computer equipment shall be provided by the Contractor with the following features and functions:

a) The Contractor shall provide regularly improving computers over the life of the contract to keep pace with the growth in physical security applications and also to stay current with what is widely available commercially.

b) The computers provided shall span a range of common computer platforms suitable to support all of the individual subsystems described in the following paragraphs.

c) This range shall include small, medium, and large PC workstations and a small and large file server.

d) The large systems shall include the fastest widely available processor, large RAM banks, large hard drive(s), large monitors, and be suited to host the most intensive applications. Minimum requirements identified in each subsystem performance requirements.

e) The small systems will be for those physical security applications with lesser requirements and lower budgets and shall include processors, which are still widely available, but incorporate progressively less RAM, smaller hard drives, and smaller monitors than the large system. Minimum requirements identified in each subsystem performance requirements.

f) The options provided shall include a wide variety of computer peripherals such as printers, modems; tape backup units, memory expansion, etc.

3.3.1.2 Network Equipment

The ISSC designer will require many different types of computer network equipment to design and construct integrated electronic physical security systems involving TCP/IP over Ethernet, FDDI, ATM, and potentially other physical layer protocols. These devices range from high-end routers and switching devices to network interface cards for the PCs. Network equipment shall be provided by the Contractor with the following features and functions:

a) Multiple types of network devices shall be provided.
b) The network devices provided shall include as a minimum Routers, Bridges, Concentrators, Hubs, and Repeaters.
c) Network Interface Modules shall be provided for these network devices, which support various media (fiber, coax, twisted pair) and various LAN protocols (Ethernet, FDDI, ATM, etc.).
d) Transceivers and Network Interface Cards shall be provided for PCs and Fileservers for various media (fiber, coax, twisted pair) and various LAN protocols (Ethernet, FDDI, ATM, etc.).

3.3.1.3 Cabling and Associated Hardware

ISSC installations will require cabling in various types and quantities. Some installations will have major cable plant requirements to support large geographical areas and systems scalability. Cabling and associated material shall be provided by the Contractor with the following features:

a) Multiple cable types and associated materials manufactured in accordance with industry standards shall be provided.
b) The cable types provided shall include twisted pair, coaxial, and fiber (single mode and multimode).
c) The cable types provided shall include distribution cables and trunk cables
d) The cabling types offered shall provide a range of products capable of operating in varying weather conditions and environments.
e) The associated materials provided shall include but not limited to repeaters, transmitters, modems, conduit, patch panels and patch cables; connectors, switches, splices, and terminators; equipment racks and rackmount hardware.

3.3.1.4 Uninterruptible Power Supplies (UPS)

Many subsystems of ISSC will require power filtration and/or battery backup. The UPS equipment offered by the Contractor shall support the following functions and features:

a) Each shall be a completely integrated, static UPS providing regulated, low-transient, low-distortion power for system components.
b) Recommended UPSs shall be provided as required per IDOs.
c) The vendor shall offer a range of UPS units to meet varying requirements from small 0.5 to 5 KVA, medium 6 to 10 KVA, and large 11 to 20 KVA in capacity.
d) The units shall be configurable such that battery storage can be increased from very low amounts up to several minutes or hours of storage time depending upon local requirements as specified

3.3.2 Command, Control, and Communications System (CCCS)

The Command, Control, and Communications System (CCCS) serves as the focal point of ISSC. It provides the hardware and software front end, which controls overall operation of other subsystem functions, which make up ISSC. The CCCS shall also support a Computer Aided Dispatch/Records Management System (CAD/RMS), a Radio System, a universal timing source for use by the subsystems and Audio Source Recording (ASR) when required for specific sites.

3.3.2.1 ACS/IDS/Assessment Front End

3.3.2.1.1 System Description

The Command, Control, and Communications controller for the ISSC is hosted on a modular, scaleable, digital computer-based system and is the primary point of operator interface and interaction. It is the central integrating computer-based system for the command and control subsystem of the other subsystems of the ISSC. The CCCS controller distributes its functions and control of the overall system, when required, through the use of Independent Local Processors (ILPs). Additionally, it may be connected via the network to the video badging system (VBS) enabling the dynamic exchange of cardholder database information between the two systems. It may be connected to the electronic article surveillance system for immediate detection and reporting of attempted removal of tagged equipment through protected portals. It may be connected to the computer-aided dispatch and records management system that assists in the automation of the security response function in the event of an alarm.

3.3.2.1.2 Performance Requirements

The Command, Control, and Communications controller shall support the following features and functions:

a) Command, Control, and Communications within ISSC shall reside within the structure of a personal computer (PC)-based network scalable to accommodate government requirements. The ISSC shall have redundant multi-tasking, multi-user Central Processing Units (CPUs) with at least one pair of the CPUs in a hot-tap configuration with automatic switchover. Each CPU within the pair shall be capable of performing the full system control. For a small system, the ISSC may consist of a single CPU but if required, could easily be expanded to a multi-user, redundant system.

b) Application of open system computing standards shall enable ease of data exchange between designated subsystems and the command and control of each of these subsystems from ISSC operator and administrator interface terminals.

c) ISSC command, control and communication shall be supported by a multitasking, real time operating system such that multiple applications are simultaneously displayed in different areas on the screen and updated in real time as a background process.

d) Software applications employed within ISSC shall employ a graphical user interface (GUI) that enables the operator to configure and control the individual subsystems with the mouse, keyboard, or touch-screen.

e) Control of any subsystem within ISSC shall be possible from two or more networked stations.

f) These stations shall be capable of being geographically separated such that control of the system can be performed at multiple locations.

g) The system shall be configurable such that control functions and event reporting can be directed to one or more desired stations within the control network.

h) An on-screen live video window and facility map graphics shall be integral to all electronic systems (IDS, ACS and CCTV) with icons or other indicators to visually identify alarms and aid in dispatch.

i) System software shall permit database partitioning to restrict operators access to only the portions of the cardholder/device databases authorized under any given password. System shall be configured in a Global/Regional concept and allow central cardholder database partitioning

j) ISSC command, control and communication architecture shall be based on a distributed intelligence scheme through the use of database distribution techniques.

k) A universal timing signal shall be provided to permit synchronization of the activities of all the ISSC subsystems.

l) All user definable parameters shall be reviewed with the user and validated by the user upon installation of the system by the Contractor.

m) The Contractor's system shall have the capability for backup/storage of all data on ISSC systems and all sub-system components, whether the system is fully configured, consists of only one subsystem, or consists of several subsystems. These backup capabilities shall be extensive enough to allow complete recovery of data from a system which has failed/crashed. The backup/recovery hardware, software, and methods will incorporate the latest technology so that speed, efficiency, and capacity will be maximized, and full compliance with DOD regulatory requirements.

n) Comply with all applicable DOD Regulatory, UL Standards (294, 1076, 1981, 2050) and UFC criteria for Electronic Security systems.

The associated Independent Local Processors (ILPs) shall support the following functions and features:

a) Independent Local Processors (ILP) and ISSC servers and workstations shall be scaleable with database and archival capacity determined by the specific requirements of the individual delivery order.

b) In the event of communications loss between the ISSC CPU(s) and the local areas of control, the system shall provide automatic up/down load of data from the ISSC CPU(s) to the Independent Local Processor (ILP) controlling the local operations upon restoration of operations. Upon restoration of communications, the ILP shall automatically update the CPU(s) with all transactions that ILP performed during the communications loss.

c) ILPs shall accept all industry standard identification device communications formats and shall not use communications formats to the central computer that are proprietary or nonstandard.

d) ILP shall be capable of storing ACS information on a minimum of 20,000 individuals and capable of meeting Govt. requirements as specified in individual delivery orders.
e) Locally, continuously monitor and control the status of a minimum of 8 card readers and their interconnection lines.
f) Provide at the card reader or ILP, the activation and de-activation of electric strikes and monitoring and bypassing of the door switch.
g) Permit individual or groups of card readers to be activated or de-activated via commands from the central processor.
h) Be assembled modularly to facilitate expansion and to provide software diagnostic aids for troubleshooting and maintenance.
i) Provide internal 6 hour battery backup as a minimum.
j) During loss of communication between the ILP and the next higher-level processor, the ILP shall provide full local control.
k) Upon restoration of communications, automatically update the CPU with all transactions that occurred during the communication loss.
l) Provide full access control by recognizing and processing individual personnel coded information on the access control cards (facility and individual codes).
m) Continuously monitor the status (secure or alarm) of up to 16 supervised sub-zones and their interconnection lines (line supervision).
n) Provide a minimum of 4 control output signals when commanded.

3.3.2.2 Computer Aided Dispatch/Records Management System (CAD/RMS)

3.3.2.2.1 System Description

The CAD/RMS subsystem supports event handling and dispatching tasks simultaneously. It combines the functions of call taker and dispatcher in a unified console. The objectives of this subsystem are to:

a) Streamline the processing of alarm events and improve the ability to handle peak loads.
b) More effectively process the selection of units for assignment to calls and ensure that the optimum units are selected.
c) Reduce the time required for initial alerting and dispatch communications to assigned units and provide them with complete and accurate dispatch information.
d) Provide automated support to the operations function in a format suitable for computer analysis.
e) Provide automated support to the report creation and report management functions of the DoD.

3.3.2.2.2 Performance Requirements

a) The CAD/RMS system shall be an integrated system of computers, display stations, printers, remote microcomputers, communications network, databases, and software.

b) The system shall be supported by a multitasking, real time operating system such that multiple applications are simultaneously displayed in different areas on the screen and updated in real time as background processes.
c) The CAD/RMS shall have the capability to interface to County, State, and Federal computer systems, and other interfaces to provide an integrated operating system.
d) The system shall be sufficiently "user friendly" such that police personnel and civilian personnel can operate it with training.
e) Application of the principles of open systems shall enable integration of the CAD/RMS with ISSC Command and Control and other computer-based systems.
f) The system shall be capable of expanding the number of dispatching positions with the addition of hardware.
g) The system shall support the single entry concept where an incident can be traced from the initial alarm event through CAD to the Record Management System (RMS).
h) Primary interaction between the user and the computer shall be via pre-formatted, fill-in-the-blank screen layouts.

3.3.2.3 Radio System

3.3.2.3.1 System Description
The radio subsystem provides a means of communication between control center personnel and law enforcement personnel at the site or remote sites.

3.3.2.3.2 Performance Requirements
a) The radio system shall be a two-way, high power system supporting both data and voice communication.
b) These two channels shall be the primary voice and data communication system between the dispatcher and personnel in the field.
c) The system shall include at least a base station, vehicle terminals, and handheld units. The system shall have operating capability for two (2) dispatcher positions.
d) These positions shall be combined call taker /dispatcher functions.
e) The system shall be capable of expanding to five full-function satellite-dispatching positions with the addition of necessary hardware.
f) Such expansion shall not result in the obsolescence of existing equipment or cause system operating delays.

3.3.2.4 Audio Source Recording (ASR)

3.3.2.4.1 System Description
This subsystem is intended to allow for the recording of various audio channels (intercom, telephone, and/or radio), which allows for flexible playback and review of past events.

3.3.2.4.2 Performance Requirements
a) Audio recording equipment shall be provided to maintain records of activity from various audio sources. Audio based systems shall connect to audio recorders

equipped for automatic audio detection recording activation to conserve the recording medium.

b) Recordings shall be date and time stamped and shall be able to be rapidly searched based on the time stamp information.

c) Recorded audio sources shall include but not be limited to telephone, 2-way radio, intercom, and the Audio Duress System.

d) The system shall accept the universal timing signal generated by the ISSC.

e) The system shall have the ability to record audio signals for a minimum of 8 hours without having to change the recording medium.

3.3.3 Access Control System (ACS)

The Access Control System (ACS) provides automated control of designated doors, turnstiles, gates and vehicle barrier systems through various types of identification devices. As part of an integrated system, this subsystem is centrally controlled by the CCCS front -end host, which may have several associated client stations to allow monitoring, and management functions to be performed from several different locations. Depending on the site requirements, the ACS may also perform as a stand-alone system and act as its own CCCS system. At the periphery it is made up of access control devices and associated hardware including, but not limited to card readers, keypads, biometric personal identity verification devices, and locking devices. Between these end devices and the CCCS host processor, the ILP serves to distribute the capability of the ACS by hosting portions of the main access control database and independently controlling a segment of the overall system. An ILP can be connected directly to the CCCS front end or may be connected to another ILP, which is in turn connected to the CCCS front end. Communication occurs between the host and an ILP on an as needed basis to report events to the host and update the ILP's database. This hierarchical architecture allows for scalability from very small systems up to very large systems. The ACS may also include a Delayed Door Egress System (DDES), a Guard Patrol Supervisory System (GPSS), a Vehicle Entry Control System, and a Visual Recognition System (VIRS).

3.3.3.1 Access Control Host and Peripherals

3.3.3.1.1 System Description

A fully functional Access Control System requires a central host controller (that can function as the CCCS host for a standalone ACS), intermediate devices such as Independent Local Processors (ILPs), and wide variety of end devices at the periphery.

3.3.3.1.2 Performance Requirements

The system shall support the following Access Control System functions and features at the system level.

a) Have the system capacity for a minimum of 25,000 personnel with expansion possible to a minimum of 250,000.

b) Be modular in construction and implementation.

c) Automatically download all necessary ACS data to ILP level both globally & regionally

f) Process, enunciate, and activate a single access control system status change within 1.2 seconds. To include generating an alarm condition, when tenants inadvertently fail to secure alarmed zones within programmed "secure hours" or at the end of the occupied duty day.

g) Permit the minimum throughput processing time of 12 individuals per portal, per minute. "Portal" to include any, doors, turnstiles, pedestrian gates, vehicle access control points, or other electronic devices installed to control access to a specific area.

e) Include software for anti-passback detection, strike release duration, and door open alarm condition.

f) Incorporate historical reporting of varying forms of access transactions. To include specific "event" driven reports, which pinpoint alarmed activity at specific door, portal, person, priority, or sensor location, and general logging reports, which record all transactions combined. Reports to be furnished to authorized Government personnel "on demand", without bogging down system, and within 2 hours of written request.

g) Have the capability to track a minimum of 10 access control levels per individual.

h) Monitor and control at least 1024 card readers.

i) Provide the capability for security managers to control the access rights to the facilities that they control. The ability to control access shall be by individual in the database assigned to specific card readers.

j) Provide for automatic voiding of selected individual cards from the system after user-defined periods.

k) Provide for a minimum of 256 operator passwords.

l) Enable real-time transfer of all enrolled data to the ILP level.

m) Maintain a current file on each enrollee. System shall provide for user-defined and generated data fields and user-defined sorting capabilities.

n) Produce user-defined and generated data lists and other reports upon demand for security management purposes.

o) Use password controls to prevent unauthorized access to data and partitions within the database.

p) Prevent database files information from being lost or damaged by power or equipment failures.

q) Report unauthorized entry attempts, by individual name and card number, to selected ACS terminals.

r) Automatically void selected cards that have been used for attempts of unauthorized entry.

s) Be capable of interfacing with biometric devices for controlling access.

t) Card readers shall be tamper and vandal resistant devices with a visual display to indicate status and optionally provide a keypad for the input of a Personal Identification Number (PIN).

u) Card keys should be swipe through, proximity, or insert (as determined by the individual site survey), high coercivity, magnetic stripe compliant with the SEIWG-012 and FIPS-201 specifications. The system shall be able to read,

process, and determine individual access rights based on the complete 25 digit SEIWG-012 encoded number or future FIPS-201 specifications.

v) Capable of communicating with and exchanging data with a Video Badging System (VBS) database via a network.

w) Support multiple means for enrollment and modification of personnel data, such as keypads, customer service terminals, and client stations over the LAN.

x) Enable the establishment of multiple access groups; groups of individuals assigned identical access privileges based on access portal, time, and day of the week.

y) Provide a Graphical User Interface (GUI).

z) Provide a wide variety of access control devices and associated hardware including, but not limited to, card readers, keypads, turnstiles, mantraps, biometric personal identity verification devices, locking devices, egress devices, passive & active barrier systems, using industry standard power and communications formats.

aa) Accept the universal timing input from the Command, Control and Communication subsystem.

bb) Provide for ACS interface with CCTV, IDS, and intercom systems as required by IDO's.

cc) Must meet all applicable DOD Regulations & UFC criteria for Electronic Security Systems to include probability of detection, false alarm rates, and acceptable quality levels.

dd) Must meet all applicable UL standards(294, 1076, 1981 & 2050)

3.3.3.2 Delayed Door Egress System (DDES)

3.3.3.2.1 System Description

This subsystem allows for effective control and emergency use of doors that are not configured as primary access portals. These are doors that are not regularly used entrances or exits, and are secured under normal conditions. In the event of an emergency these doors must permit exit while informing control center personnel that the exit is in use. The delay function is a tool, which discourages unauthorized or nuisance use of the doorway while retaining its full use as an emergency exit. The system shall be applied in full compliance with local codes applicable to the individual site.

3.3.3.2.2 Performance Requirements

a) The delayed door egress system shall use a variety of commercially available, code compliant hardware (electromagnetic locks, electric strikes, mechanical push bar, etc) controlled by an adjustable timing mechanism on specified emergency exit doors. Delayed egress systems must comply with local fire/life safety codes, as well as the Pentagon Reservation Building Code.

b) Egress attempts shall be enunciated at the central host controller.

c) Through an interface to the DDES central controller, the ISSC CCCS shall have the ability to report the present status of each door in the system.

d) Interaction of the DDES with ISSC Command and Control shall enable operator assessment of pre-release conditions generated by egress attempts through ISSC video assessment resources.
e) Authorized egresses shall be permitted by the operator on a per door basis.
f) An emergency release of all doors shall be possible via a single console mounted key switch, or by a password protected output command function through the ISSC CCCS.
g) Doors shall be individually connected to, and released by the Fire Alarm system in the event of the automatic detection of a fire alarm condition.

3.3.3.3 Guard Patrol Supervisory System (GPSS)

3.3.3.3.1 System Description

This subsystem is intended to support the systematic coverage of patrol areas and the efficient use and monitoring of law enforcement personnel. "Guard patrols" are preprogrammed into the system that require patrolling law enforcement personnel to physically check-in at various key checkpoints during the course of their patrolling shift. This insures that key areas are regularly inspected and cleared while monitoring the general whereabouts of patrolling law enforcement personnel in the case of emergency or other diversions from their assigned patrol.

3.3.3.3.2 Performance Requirements

a) An on-line guard patrol system shall be an integral part of the ISSC ACS.
b) Designated ACS devices shall act as checkpoints on patrols.
c) The system shall be capable of tracking a minimum of 16 concurrent patrols.
d) ISSC Command and Control terminals shall report patrol initiation, progress, completions, and exceptions.
e) Patrols shall be entirely configurable by authorized ISSC operators both before and during patrols.
g) All patrol histories shall be logged to file and shall be available as a standard history report.

3.3.3.4 Vehicle Entry Control System

3.3.3.4.1 System Description

The Vehicle Entry Control subsystems shall include modern forms of vehicle identification such as License Plate Readers and Automatic Vehicle Identification to identify vehicles entering controlled parking lots and traffic areas via a variety of passive/active vehicle barriers; to include but not limited to; automated electronic/hydraulic vehicle barriers/bollards, gates and arms; fixed barriers/bollards; guard control booths; vehicle explosive scanning devices; and other requirements as required by individual delivery orders. Information obtained through these systems is then shared with the ACS, which determines access rights for the specific vehicles for specific areas and opens gates and barriers when appropriate to allow these vehicles through these systems.

3.3.3.4.2 Performance Requirements (license plate reader and automated vehicle identification)

a) A license plate reader system shall enable the capture of a video image of an automobile license plate and conversion of the image to a digital data stream for input to ISSC ACS.
b) The system shall provide processing in less than one second and reliable operation under extreme weather conditions.
c) A software application shall be provided to enable the creation of a vehicle database operating on the ISSC Command and Control network that shall allow the verification of authorization for individual vehicles.
d) An automatic vehicle identification system shall be provided that is based on equipping vehicles with a coded tag that will be detected and verified by readers located at vehicle barriers.
e) Integration of the output from the AVI system processor shall be readily portable to ISSC Command and Control to enable management and control of the user database of tag/vehicle information.
f) A software application shall be provided to enable the creation of a vehicle database operating on the ISSC Command and Control network that shall allow the verification of authorization for individual vehicles.

3.3.3.5 Visual Image Recognition System (VIRS)

3.3.3.5.1 System Description

This subsystem allows law enforcement personnel to easily make use of data and images stored in the master badging and access control databases from remote locations. This is a computer based system which connects to the master database via a standard network and is allowed read only access to data for the purpose of verifying identity, access rights, and other pertinent information. This system serves as a backup or supplement to the primary access control system.

3.3.3.5.2 Performance Requirements

a) The VIRS client application shall be modular such that it can be loaded on any standard PC in the network and access the central database over the standard TCP/IP network service or by serial modem interface.
b) Security personnel shall be able to call-up video badging information for verification of the identity of badge holders through ISSC terminals.
c) Integration with the badging system central database shall allow authorized operators to retrieve the video image and personal data of the cardholder.
d) VIRS shall be provided as a an integral feature of the ACS application software.

3.3.4 Intrusion Detection Systems (IDS)

The Intrusion Detection System (IDS) provides monitoring of alarm sensors connected to the inputs of Independent Local Processors (ILP). This system is centrally controlled by the IDS or CCCS front-end computer. At the periphery it is made up of alarm initiating devices and associated hardware. Between these end devices and the CCCS host processor, the ILP serves to distribute the capability of the IDS. An ILP can be connected directly to the CCCS front end or may be connected to another ILP, which is in turn connected to the CCCS front end. This

hierarchical tree architecture allows for scalability from very small systems up to very large systems. The IDS may also include an Audio Duress System (ADS) and an Electronic Article Surveillance System (EASS).

3.3.4.1 Primary Intrusion Detection System

3.3.4.1.1 System Description

A fully functional Intrusion Detection System requires a host controller, intermediate devices such as Independent Local Processors (ILPs), and a wide variety of end devices at the periphery. The required end devices include alarm initiating devices and associated hardware such as, but not limited to, door contacts, motion sensors, video motion sensors, glass shock sensors, cabinet tamper switches, duress switches, and exterior perimeter protection devices (such as underground motion sensors, fence-line sensors, microwave sensors, blast mitigation and electronic surveillance protection window coating).

3.3.4.1.2 Performance Requirements

The system shall support the following Intrusion Detection System functions and features at the system level.

a) Provide at least 4 levels of alarm prioritization based on a class such as duress, intrusion, tamper, and maintenance and the ability to further prioritize alarms within the class to at least an additional 4 levels.
b) Provide field-programmable graphics/mimics and mission software to aid in dispatch.
c) Provide a Graphical User Interface (GUI), which supports color-graphic map displays for detailing floor plans and single alarm point annunciation, to aid in dispatch.
d) Provide database file partitioning to support a global/regional concept.
e) Provide alarm/video matrix interface for CCTV call-up upon alarm condition
f) Monitor and control a minimum of 5,000 alarm zone (accounts).[5]
g) Provide for a minimum of 16 time zones.
h) Process and enunciate 5 IDS alarm events within 2 second average of the detected IDS alarm conditions. To include generating an alarm condition, when tenants inadvertently fail to secure alarmed zones within programmed "secure hours" or at the end of the occupied duty day.
i) Place alarm zones in the secure mode from access, and vice versa, by three different methods, using secure/access devices, system operator commands, and CPU generated changes using time zones.
j) Provide graphic displays, which identify the status of all alarms and ILPs. To include a rapid method for alarm monitors to conduct status checks of all active zones, at the beginning/ending of each shift to verify continued operation, in-maintenance status, station failure, or station recovery.
k) Provide line supervision to meet DCID 6/9 criteria for SCIFs.

[5] Maximum system envisioned may have as many as 100,000 alarm zones and an appropriate number of ILPs.

l) Communicate with and control a minimum of 512 ILPs.
m) Provide keypad secure/access switches with at least 12 digit keypads and field adjustable activation delays from 15 to 90 seconds.
n) Incorporate historical reporting of varying forms of intrusion detection alarms. To include specific "event" driven reports which pinpoint alarmed activity at a specific door, portal, person, priority, or sensor location, and general logging reports, which record all alarms combined. Reports to be furnished to authorized Government personnel "on demand", without bogging down system, and within 1 hour of written request in both electronic or hard copy form.
o) Alarm setup shall include full text descriptions of each alarm point, scheduling, routing, and linking to individual, or groups of outputs.
p) Provide multiple types of alarm initiating devices including, but not limited to, door contacts, motion sensors, video motion sensors, glass shock sensors, cabinet tamper switches, duress switches, and exterior perimeter protection devices.
q) Must meet all applicable DOD Regulations & UFC criteria for Electronic Security Systems to include probability of detection, false alarm rates, and acceptable quality levels.
r) Must meet all applicable UL standards (294, 1076, 1981, 2050)

3.3.4.1.3 System Requirements

Per DoD Directive 5220.22M, Chapter 5 Section 9, the contractor performing installation, service, and/or maintenance of an intrusion detection system must be listed by Underwriters Laboratories (UL). The IDS equipment installed must also be listed by UL.

3.3.4.2 Audio Duress System (ADS)

3.3.4.2.1 System Description

The Audio Duress subsystem provides two way audio communication between control center personnel and individuals located in areas which are identified as potential sites for personal assault such as parking lots or stairwells. The communication can be initiated either by push-button and/or by noise levels exceeding a preset threshold such as a shout for help. This subsystem is integrated with the CCCS to provide annunciation of an alarm at the central location.

3.3.4.2.2 Performance Requirements

a) An audio duress alarm system with listen-in and talkback capabilities shall provide protection against personal assaults in parking lots, stairwells, or other secluded areas as determined via individual site surveys.
b) The system shall employ sound detection circuitry with an adjustable threshold feature that shall sense sound pressure levels and create alarm conditions when levels exceed the set threshold.
c) Push-buttons shall permit manual activation of the communication circuit at each speaker/microphone location.

3.3.4.3 Electronic Article Surveillance System (EASS)

3.3.4.3.1 System Description

As the IDS works to detect unauthorized entry into a controlled building, the electronic article surveillance subsystem monitors unauthorized entry of prohibited items (weapons, explosives, etc.) or the removal of controlled property from a controlled building., or other requirements as specified in individual delivery orders. This subsystem is used to screen incoming items or to register, catalog, and tag controlled equipment. The system then monitors at exit points for tagged equipment being carried through the exit and triggers alarm events, when appropriate, to personnel controlling entry or exit to facilities.

3.3.4.3.2 Performance Requirements

a) The Electronic Article Surveillance System shall be a computer-based networked system to screen incoming items, or identify and catalog equipment and to prevent unauthorized removal of equipment from the protected premises.
b) The system shall include computer hardware, software, identification tags, scanners or explosive/metal screening devices.
c) The system shall facilitate the creation of a database for protected equipment.
d) Scanners shall be used as read devices to detect removal and determine ownership of tagged equipment as displayed on the system terminal.
e) Open systems standards shall be applied in the design of the computer-based system to interoperate with other computer-based systems within ISSC, if required.

3.3.5 Assessment System

The Assessment System allows security and law enforcement personnel to monitor and assess public areas through the use of video cameras and audio intercommunication devices. It is an integrated subsystem of ISSC, which is interfaced to and controlled by the CCCS front-end system. The closed circuit television equipment includes, but is not limited to cameras, housings, mounts, lenses, signal amplification and equalization devices, transmission media, recording devices, video storage equipment, and switching/control equipment. Audio intercoms are coupled to Closed Circuit Television (CCTV) cameras for alarm caller assessment purposes. Master intercoms are also integrated with ISSC Command and Control to facilitate communications between control room personnel and remote sites.

3.3.5.1 Video Assessment System (VAS)

3.3.5.1.1 System Description

The video assessment subsystem is a CCTV system allows security and law enforcement personnel to monitor and assess activities via live video views of public areas throughout a controlled facility. Larger systems typically involve switcher or multiplexer equipment to feed many cameras to smaller banks of video monitors and computer terminals either in a control center or other key locations.

3.3.5.1.2 Performance Requirements

a) The video assessment subsystem shall be an integrated subsystem of ISSC providing real time video information to the system operators and associated equipment.
b) A system of closed circuit television surveillance equipment shall include, but not be limited to cameras, housings, mounts, lenses, signal amplification, and equalization devices, transmission media, recording equipment, and switching/control equipment.
c) Switching of video signals and control of camera positioning devices shall be entirely configurable through the ISSC command and control terminals and through dedicated control keyboards.
d) Integration of the VAS into the ISSC shall permit alarm associated automatic video call-up for any alarm device within the system to be displayed on a video monitor or directly on the ISSC terminal as configured by the user/operator.
e) Video recording capability shall be through camera multiplexers, videocassette recorders, digital frame storage devices, and optical storage devices.
h) Transmission of the video signals shall be by fiber optic, coaxial, network and hard wire cable as determined during the Site Survey or IDO.
i) Meet all applicable DOD Regulations and UFC Criteria on the design, installation, and maintenance of video assessment (CCTV) systems.

3.3.5.2 Audio Assessment System (AAS)

3.3.5.2.1 System Description

The audio assessment subsystem is an intercom system, which allows security and law enforcement personnel to monitor and assess activities via live, two-way audio channels between control centers and key areas in and around a controlled facility. Larger systems typically involve operator consoles to terminate and manage many intercom systems.

3.3.5.2.2 Performance Requirements

a) Audio intercoms shall be coupled to CCTV cameras for alarm caller assessment purposes.
b) Master intercoms shall be integrated with ISSC Command and Control.
c) It shall be possible to link remote intercom stations with the IDS to permit assessment of alarm activity.
d) The system shall operate as a standard intercom with calls being initiated manually either from the substation, or from the master intercom.
e) Activation of the call button from a sub-station shall cause the associated camera view to be displayed on an ISSC CCCS station.
f) Operation from the substation shall be hands free talk back.
g) Transmission of the intercom signals shall be by existing telephone equipment and cable wherever feasible.

3.3.6 Video Badging System (VBS)

3.3.6.1 System Description

The Video Badging System consists of a personal computer equipped with video camera and badge printer. It may be networked with other badge stations to enable multiple enrollment and administration workstations. Whether standalone or networked, the badge system provides cardholder enrollment, badge issuance, production of parking permits, database configuration, and report functions. The use of video photography to capture images for ID badges adds greater flexibility to this security operation. The digital image may be used many times to print new badges, include in reports, and display at law enforcement terminals for rapid identification.

3.3.6.2 Performance Requirements

a) A commonality of communications protocols and database applications between the VBS and the ISSC CCCS shall allow the exchange of data for automatic enrollment of new cardholders into the ISSC access control system database for both pedestrian and vehicle access and retrieval of video image and badge data information for card holders from the VBS database.

b) Electronic Video Imaging (EVI) shall be used to create personal identification badges with the images stored in a standard format (e.g. JPEG, GIF, TGA).

c) Parking permits shall be produced in the same manner although video images may not be required.

d) Badges shall be capable of including signature, cardholder image, graphics logos, text, bar code, magnetic stripe, or an embedded integrated circuit.

e) Badges encoded shall be SEIWG-012 (current specification) and future HSPD-12 and FIPS-201 compliant.

f) User customized layouts for the badges shall be possible.

g) The VBS shall be provided as a complete system including operating system, applications and database management software, terminals, video capture equipment, badges, and badge production equipment.

h) The VBS application software shall support Dynamic Data Exchange (DDE) interprocess communications to allow for interface of the VBS to other applications.

i) This database shall be capable of supporting a minimum of 25,000 active records expandable to a minimum of 250,000 and shall be capable of storing inactive records for a period of five years.

3.3.7 Passive and Active Vehicle Barrier Systems

3.3.7.1 System Description

The Passive and Active Vehicle Barrier Systems shall consist of all industry and DoD Force Protection standards for barrier systems to include but not limited to pop up plate barriers, bollards, sliding gates, fencing, planters, earth berms, traffic control, security landscaping, physical protection through environmental design, physical perimeter security and other vehicle standoff strategies which support various security and law enforcement operations, and threat conditions.

3.3.7.2 Performance Requirements

a) Strive to meet standards set forth in the National Capital Urban Design and Security Plan adopted by the National Capital Planning Commission on May 5, 2005.
b) Comply with the American Disabilities Act (ADA) and the Architectural Barriers Act (ABA).
c) All systems shall comply with DoD and/or Department of State (DOS) certifications. DOS Publication, SD-SDT-02.01.
d) All active barrier systems shall have programmable logic control (PLC).
e) All Barrier systems shall be equipped to meet applicable Federal and State safety standards to prevent damage to property or persons.
f) All barrier systems shall comply with minimum requirements set forth is UFC 4-022-02, "Selection and Application of Vehicle Barriers" and Guide Specification #02840 as completed/edited by Government per individual IDO and site-specific requirements.

3.3.8 Security Booths, Kiosks and Bullet Resistant Components (BRC)

3.3.8.1 System Description

The Security Booths, Kiosks and Bullet Resistant Components (BRC) shall consists of all material, labor and equipment to fabricate, deliver and install (BR) hardened security booths, desks, kiosks, vehicle/pedestrian access points, and over watch positions in both interior/exterior applications. IAW DoD Regulations, Force Protection Standards, Unified Facility Criteria (UFC), NCPC, as well as site-specific design or property owner constraints. These Kiosks will house a variety of security controls, systems and equipment as defined by individual delivery orders.

3.3.8.2 Performance Requirements

a) As defined by individual delivery orders and completed UFGS.

3.3.9 Screening Devices

3.3.9.1 System Description

Screening devices shall consist of all electronic systems designed to detect contraband, weapons, hazardous materials, CBRN or other prohibited items to include but not limited to x-ray machines, metal detectors, hand held detectors and mobile screening systems.

3.3.9.2 Performance Requirements

a) defined by individual delivery/purchase orders.

3.4 Security System Installation and Testing

The Contractor shall be responsible for the installation and testing of the installed ISSC at the Government facilities. The Government will witness testing as defined in individual delivery orders. The Contractor shall develop and maintain an ISSC test bed at the Contractor's facilities. The test bed shall be used to perform pre-delivery testing, system evaluations and technology evaluations. The Contractor shall also use the test bed to maintain a mock ISSC dedicated for customer demonstration purposes.

3.4.1 Pre-Delivery Testing

The Contractor shall perform pre-delivery testing, and adjustment of the completed ISSC and all subsystems in the Contractor's test bed facility. Testing shall include consideration of any existing ISSC hardware, firmware, and software that may be installed at the site. The Contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing. The Contractor shall develop test plans for each test. Test procedures shall explain in detail, step-by-step actions and expected results demonstrating compliance with the performance requirements. The plan must be approved by the Government prior to testing. Written notification of planned testing shall be given to the Government at least 14 days prior to the test. Pre-delivery testing shall be performed on a representative sample from the actual hardware to be installed. Test reports shall be used to document results of the tests. Reports shall be delivered to the Government within 7 days after completion of each test.

3.4.2 Installation

The Contractor shall be capable of providing complete installation of all system hardware, software, firmware, interconnecting wiring and communications interfaces necessary for the complete operation of the system. Though facility modifications/site preparations required to support equipment installation such as footings, trenching for cable installation, pavement cutting and patching, construction of walls, installation of power and telephone services, and other site construction/modifications shall be the responsibility of the government, some minor levels of site preparation work may be required.

3.4.2.1 Installation Tools and Permits

The Contractor shall supply all tools and equipment necessary to perform installation tasks and is responsible for obtaining all permits associated with the ISSC installation.

3.4.2.2 Installation Practices

The Contractor shall install all system components and appurtenances, including Government furnished equipment in accordance with the manufacturer's instructions (unless a deviation is approved in writing by the Contracting Officer), ANSI C2, NEC and shall furnish all necessary conduit, cable, connectors, terminators, interconnections, services, and adjustments required for a complete and operable system. Unless otherwise directed in an individual delivery order or technical direction letter, all interior wiring, including low voltage wiring outside the security center control console and equipment racks, cabinets, boxes and similar enclosures, shall be installed in Electric Metallic Tubing (EMT) and hidden to the maximum extent possible.

Interconnection wiring between components mounted in the same rack or cabinet does not need to be installed in conduits. Data Transmission Media shall not be pulled into conduits or placed in raceways, compartments, outlet boxes, junction boxes, or similar fittings with other building wiring. Flexible cords or cord connections shall not be used to supply power to any components of the CCTV system, except where specifically agreed upon as a result of the Site Survey. Grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.

3.4.2.3 Interfacing with Existing Equipment

The Contractor shall be responsible for interfacing with any existing security or other associated equipment that may be determined to be usable during the Site Survey.

3.4.2.4 As Built Drawings

The Contractor shall maintain a revised set of drawings, elementary diagrams and wiring diagrams of the ISSC to be used for "as-built" drawings. This set shall be accurately kept up to date by the Contractor with all changes and additions to the ISSC and shall be delivered to the Government with the final acceptance test report. The Contractor shall deliver these drawings to the Government for review and approval. If the as-built work is not complete, the Contractor will be so advised and shall complete the work as required. For all work completed in relation to the renovation program, red line drawings will be submitted to PenRen for incorporation into the final As-Built documents.

3.4.3 Post Installation Testing

The Contractor shall provide complete testing and system certification services before final acceptance. The Contractor shall be responsible for ensuring that the hardware and software is in full compliance with the delivery order statement of work, including applicable reference documents. The Contractor shall perform post installation testing, and adjustment of the completed ISSC and all subsystems. The Contractor shall provide all personnel, equipment, instrumentation, and supplies necessary to perform all testing. The Contractor shall use test plans developed for the pre-installation testing. Written notification of planned testing shall be given to the Government at least 14 days prior to the test. Post installation testing shall be performed on all hardware installed. Test reports shall be used to document results of the tests. Reports shall be delivered to the Government within 7 days after completion of each test.

3.5 Integrated Logistics Support

The Contractor shall perform the following Integrated Logistic Support functions for installed ISSC configurations. All systems and plans described in this section must be reviewed/approved by Government within 30 days after contract award, and fully implemented within 30 days after Government acceptance.

3.5.1 Automated Integrated Logistics Support (ILS) Program

The Contractor shall implement an automated computer based logistics program.

3.5.1.1 Maintenance Management System (MMS)

The MMS shall use a Structured Query Language (SQL) compliant relational database software application to maintain accurate maintenance records on all systems and components delivered and/or installed. The MMS shall provide the Government and Contractor with information pertaining to the extended maintenance agreements and maintenance schedules and activity on all systems and components, equipment preventative maintenance requirements, perform repair histories, track repair costs, anticipated life cycle replacements, and generate reports. The Contractor shall furnish their own IBM-compatible computer and laser printer. The MMS program shall be user-friendly and menu-driven.

For all individual pieces of equipment the Contractor shall develop equipment item information that includes equipment name, equipment tag number, manufacturer, model and serial numbers, nameplate data, supplier information, recommended spare parts, replacement cost, startup date, and notes.

Develop preventative maintenance procedures, develop the estimated time to perform preventative maintenance work; craft or job skill required; budget identification for the work; tools, materials, and spare parts needed; and instructions for proper and safe repair procedures. Develop appropriate intervals for preventative maintenance of each piece of equipment according to manufacturer's standards. The program shall be able to list all work to be done, showing the due date, and continue to note that preventative maintenance work is required until it has been completed.

The MMS shall be capable of tracking performance and cost of corrective maintenance. Delivery orders shall be used in conjunction with this element. The MMS shall be accessible at all times to authorized government personnel. The Government shall be able to access the database and determine the status of all maintenance activities and costs. Training shall be made available to other government agencies as required. A substitution of providing training material such as video tape(s) and manuals may suffice, as required by each individual installation. Successful training of government employees shall be measured by the government's employees being capable of developing the reports without the Contractor's assistance.

3.5.1.2 Warranty Management System (WMS)

The WMS shall use a SQL compliant relational database software application to maintain accurate warranty records on all systems and components delivered and/or installed. The WMS shall provide the Government and Contractor with information pertaining to warranty coverage and warranty activity on all systems and components. The MMS and WMS shall be linked such that maintenance history and warranty status for a given system can be easily correlated.

3.5.1.3 Training Management System (TMS)

The TMS shall use a SQL compliant relational database software application to maintain accurate training records on all Government and Contractor personnel trained on all systems and components. The TMS shall provide the Government and Contractor with information pertaining to the training schedules and all training records. The TMS shall be linked to the MMS to provide data correlation between maintenance records and training records.

3.5.1.4 Configuration Management System (CMS)

The CMS shall use a SQL compliant relational database software application to implement the Contractors approved Configuration Management Plan. The CMS shall maintain all the configuration data for all systems delivered and/or installed. The CMS shall also maintain all the system software, hardware, and firmware documentation data. The CMS shall be linked to the MMS to correlate data between the maintenance records and all the system configurations.

3.5.1.5 Documentation Management System (DMS)

The Contractor shall maintain a comprehensive and automated documentation program. The program shall provide a means to develop, distribute, update, and track all of the documentation associated with this contract to include, at a minimum, all manuals, designs, and drawing packages.

3.5.1.6 Management System Reports

The Management systems shall be capable of developing various reports for the different systems, MMS, WMS, TMS, DMS and CMS. The Government will have electronic on-line access to generate specific reports. The Contractor shall deliver reports as specified in individual delivery orders.

3.5.2 Maintenance Plan

The Contractor shall develop an ISSC Maintenance Plan for all equipment. All systems and plans described in this section must be reviewed/approved by Government within 30 days after contract award, and fully implemented within 30 days after Government acceptance. The plan shall, at a minimum, address issues of each subparagraph below.

3.5.2.1 Hardware Maintenance

The Contractor shall provide all services required and equipment necessary to maintain the ISSC equipment as may be present at an operational site and requested by the Government. Existing physical security systems at individual sites may be included and priced at the request of the Government under individual delivery orders. The Contractor shall maintain a spare parts inventory and active logistics program to support the fielded equipment for the term of the contract.

3.5.2.2 Replacement Parts

The Contractor shall review the applicable site maintenance plans. Based on this review, the contractor shall recommend to the Government suitable quantities of spare parts and bench stock for various key
materials and components required to perform rapid response maintenance on mission critical systems or rapid enhancement to mission critical systems. Once the Government approves the list, the Government may procure these items and the Contractor shall store these items on or near the site specified in the delivery order.

3.5.2.3 Software Maintenance

The Contractor shall provide software updates to incorporate new functions and/or correct problems.

3.5.2.4 Preventive Maintenance

The contractor shall perform preventive maintenance before a breakdown occurs. Preventive maintenance services are those services applied during and between operations to keep the hardware and software operating properly. Preventive maintenance inspections shall be performed no less frequently than recommended by the Original Equipment Manufacturer. Preventive maintenance shall include the running of diagnostic programs according to all applicable service manuals, lubricating, cleaning, and making corrective adjustments as necessary. Preventive maintenance plans/schedules will be reviewed and approved by Government.

The Contractor shall integrate the approved preventative maintenance program into the Maintenance Management System (MMS) defined in Paragraph 3.5.1.1. The Government reserves the right to revise the frequency of preventive maintenance based on need and budgetary constraints. The Contractor shall integrate changes to the preventative maintenance schedules as defined and approved by Government.

3.5.2.5 On-Call Maintenance

The Contractor shall perform on-call or unscheduled maintenance, as required and defined by the COR, to place a piece of equipment, system, or sub-system back in service after a failure or breakdown has occurred. On-call maintenance shall be performed after notification that equipment and or operating software is inoperative. The Contractor shall provide the Government with a designated point of contact and make arrangements to enable its maintenance representative to receive such a notification or provide an answering service or other continuous telephone coverage to permit the Government to make such contact. On-call maintenance service shall continue until the inoperable equipment is restored to an operable condition.

3.5.2.5.1 Response to Service Calls

The Contractor shall provide varying response capabilities to service calls as specified in applicable DOD Regulations & Government requirements. A service call shall consist of prompt, on-site response between two (2) hours and forty-eight (48) hours depending on site requirements. A service call is a verbal or written request (by telephone, e-mail, pager or otherwise) from the COR or authorized representative. The call is to report a malfunction or maintenance problem. Service calls may require response by the Contractor at hours other than those identified as site operating hours. The Contractor shall commit the appropriate resources necessary to accomplish the repair.

3.5.2.5.2 Completion of Service Calls

A service call shall be completed within forty-eight (48) hours from the time the service call is issued to the Contractor. If a service call cannot be resolved within the specified time period, the COR may grant a waiver of the time requirement. The Contractor shall submit a written request that gives: (1) an explanation of the delay; (2) the estimated time for completion of the service

call; (3) evidence showing an effort to comply with the time requirement. If immediate repairs cannot be made, the Contractor upon coordination with tenant occupant/security manager shall take all necessary actions or measures necessary to protect the life safety of the public and/or Government property.

3.5.2.6 Technical Support
The Contractor shall establish and support a trouble desk during normal duty hours (0600 hours to 1800 hours EST). The Contractor shall maintain an e-mail account and an off duty hours answering system or service for technical support inquiries. Technical support shall be provided as a standard service for all users of ISSC systems, equipment, and software. The Contractor shall maintain a log of all inquiries and their content. The log will be incorporated into a Support Report and delivered to the COR. The report will contain, as a minimum, the following:

a) Date of inquiry
b) Name of inquirer
c) Organization name
d) Purpose of inquire
e) Solution
f) Purpose Summary of all inquires

3.5.3 Warranty
The Contractor shall provide all post installation services and equipment necessary to maintain the installed system equipment and software in an operational state. The warranty period shall be for one (1) year or for the length of the Original Equipment Manufacturer's warranty whichever is greater. The warranty period shall begin after formal written acceptance of the system. All system software shall be placed in an independent escrow source with yearly updates provided by the Contractor. Tracking all installed equipment by make, model, serial number, location, date installed, date accepted, and anticipated life cycle replacement shall be an integral part of the warranty management & maintenance plans.

3.5.4 Training The Contractor shall be capable of providing a full program of training for operation and system administration of the installed system to designated ISSC staff. Acceptance of the installation at a particular Government site shall be contingent upon the completion of the training program. The Contractor shall conduct training for designated personnel in the maintenance and operation of ISSC as specified. The training shall be oriented to the specific system being installed. Training instructors shall be proficient in teaching the topics for the various courses and have direct experience with the installed equipment.

3.5.4.1 User Training (Tenants & PFPA Personnel)
User training shall be taught at the project site (prior to system activation or acceptance). User training shall include the following minimum topics.

a) How to properly Activate/Deactivate alarmed zones (access, secure)
b) How to conduct monthly alarm tests
c) System failure notification process

d) How to utilize all site specific system components installed (Duress, door release buttons, intercoms, card readers, electronic locks, magnetic locks, CCTV, barrier controls)
e) Procedures for adding, modifying, deleting user accounts

3.5.5 Configuration Management

The Contractor shall maintain Configuration Management (CM) for ISSC as defined by ISO 10007, Quality Management - Guidelines for Configuration Management. The Contractor shall develop, update and maintain a computer based, automated Configuration Management System (CMS) to provide Configuration Identification and Configuration Status Accounting of all equipment and software developed, installed, or associated with this contract.

The Contractor shall develop a CM Plan for ISSC to document the Contractor's CM approach to meet the requirements of this contract including control of changes for technology insertion upgrades.

The Contractor shall be the ISSC contract CM Manager. All software, hardware, and documentation changes, with respect to CM, shall be the responsibility of the Contractor. All software, hardware, and documentation changes that impact the system's compliance with the requirements of the ISSC Statement Of Work will be reviewed and approved by the Government.

The Contractor shall maintain current records and system block diagrams, system layouts, configuration identification, and complete ISSC system inventory of equipment by make, model, serial number, date installed, locations installed, and warranty coverage periods, for all equipment installed or in rotating spares (bench stock) for all ISSC primary & secondary subsystems. Documents shall be updated and provided to Government quarterly or "on-demand" as needed.

3.5.6 System Manual

An ISSC system manual shall be developed and delivered for each individual system installed. The system manual will contain the following modules specific to each individual ISSC.

3.5.6.1 Technical Module

The Contractor shall provide a full technical system description identifying all functions the system will perform and a list, statement, table, or other document which identifies each of the stated requirements of the system and gives a description of how the system design will meet those requirements. Descriptions and calculations shall show how the equipment will operate with connected systems to meet the performance of this specification. The manual shall identify the operational requirements for the system/subsystem and explain the theory of operation, design philosophy, and specific functions. A description of hardware functions, interfaces, and requirements shall be included for all system operating modes. The Contractor shall provide complete system and component documentation. Documentation shall include device specifications, descriptions of the used and unused portions of the system capacity, and operations and maintenance manuals.

The technical module shall include, as a minimum, the following:

a) System/subsystem block diagram.
b) System/subsystem installation, block diagrams, and wiring diagrams.
c) System/subsystem physical layouts and schematics.
d) Details of interfaces to other systems/subsystems.
e) Details of connections to power sources, including grounding.
f) Details of surge protection device installations.
g) Details of cable splicing and connector installations and terminations.
h) Details of underground, aerial, and messenger cable installation on poles, cable entrance to buildings.
i) Detail device wiring installation.

All specified manufacturer's certifications shall be included with the manual.

3.5.6.2 Hardware Module

The hardware manual shall describe all equipment furnished and shall include, as a minimum:

a) General description and specifications.
b) Installation and check-out procedures.
c) Equipment electrical schematics and layout drawings.
d) Data and video transmission system schematics.
e) Alignment and calibration procedures.
f) Manufacturer's repair parts list indicating sources of supply.
g) Interface definition.
h) System/subsystem schematics and wiring.
i) System/subsystem setup.

The manual shall include manufacturers' data for all materials and equipment provided under this specification.

3.5.6.3 Operating System Software Module

The system software shall support the application programs. The software module shall describe the functions of all software and shall include all other information necessary to enable proper loading, testing, and operation. The software module shall include, as a minimum, the following:

a) Definition of terms and functions.
b) Use of system and applications software.
c) Procedures for system initialization, start-up and shutdown.
d) Report generation.
e) Data base format and data entry requirements.
f) Directory of all disk files.
g) Description of all communications protocols, including data formats, command characters, and a sample of each type of data transfer.

3.5.6.4 Application Software Module

The application software shall support the overall functioning of the system and sub-system components. The application software module shall describe the functions of all application software modules and shall include all other information necessary to enable proper loading, testing, and operation. The module shall contain, as a minimum, the following:

a) Definition of terms and functions.
b) Use of applications software and the integration with the system software and the security system hardware.
c) Procedures for application software initialization, startup and shutdown.
d) Data base format and data entry requirements.
e) Directory of all disk files.
f) Description of all communications protocols, including data formats, command characters, and a sample of each type of data transfer between software and hardware components.

3.5.6.5 Operations Module

The Operations module shall include, as a minimum, information fully describing the following:

a) Computers and peripherals.
b) System startup and shutdown procedures.
c) Use of system, command, and applications software.
d) Recovery and restart procedures.
e) Graphic alarm presentation.
f) Use of report generator and generation of reports.
g) Data entry.
h) Operator commands.
i) Alarm messages and printing formats.
j) System access requirements.

3.5.7 Risk Management Plan

The Contractor shall provide a plan or strategy to maintain a system as operational in the event of system and/or component failure, which result in the level of security being compromised as a result of the failure. All systems and plans described in this section must be reviewed/approved by Government within 30 days after contract award, and fully implemented within 30 days after Government acceptance. The Contractor shall provide operational recommendations and guidelines in the event of the following, as a minimum, problems:

a) main, head end command, control, and communication failure
b) failure of the access control function of the entire system as well as failure at an individual secured space
c) failure of the intrusion detection function of the entire system as well as failure at an individual secured space
d) power failures

3.5.8 Quality Assurance/Quality Control (QA/QC) Program

The Contractor shall develop a QA/QC Plan for the ISSC Program based on all applicable DOD Regulations (for the type of systems installed). The Government shall review/approve QA/QC plans prior to implementation. All systems and plans described in this section must be reviewed/approved by Government within 30 days after contract award, and fully implemented within 30 days after Government acceptance. The QA/QC program shall identify potential and actual problem areas, and take necessary corrective measures (throughout the life of the contract) and to maintain acceptable quality levels that meets or exceeds DOD Regulatory requirements. The basic intent of the program is to make the Contractor responsible for complying with all quality & performance requirements. All methods, procedures, and forms shall support this idea.

3.5.9 Technical Services

The Contractor shall provide the services of personnel experienced in the evaluation/testing, design, fielding and use of ISSC equipment. The Contractor shall act, as required, as technical advisors to the Government in security equipment-related issues.

3.5.9.1 Security Industry Evaluation

The Contractor shall continuously evaluate and monitor the security industry for new/upgraded equipment and systems. This includes obtaining systems and equipment for evaluation in the ISSC Testbed. The Contractor shall deliver a quarterly report about the industry and the items evaluated in the testbed.

3.5.9.2 Replacement and Upgrade

The Contractor may receive requests for proposals for replacement and upgrades to existing equipment. Any orders issued for work of this nature shall be placed by the issuance of a delivery order by the Contracting Officer. The delivery order will describe the service to be provided, the equipment, start date, completion date, and total cost.

3.5.9.3 ISSC Testbed

The Contractor shall maintain a testbed facility, which shall be used to perform pre-delivery testing, system evaluations and technology evaluations. The Contractor shall also use the testbed to maintain a mock ISSC, which can be used for customer demonstration purposes. The testbed shall be established in time to accommodate the first scheduled pre-delivery test.

3.6 Information Assurance

The Contractor shall perform the following Information Assurance functions. All systems and plans described in this section must be reviewed/approved by Government within 30 days after contract award, and fully implemented within 30 days after Government acceptance.

3.6.1 Certification and Accreditation (C&A)

Document and provide to Government system architecture and operating environment. Develop and maintain System Security Plan. Participate in information system risk assessment and Security Test & Evaluations (ST&E) during the C&A process. Develop, document, and integrate technical security solutions.

3.6.2 System Security

The Contractor shall provide a plan or strategy to maintain a secure baseline in accordance with statutory requirements and DOD 8500.2. The Contractor shall as a minimum:

a) Support, monitor, test, and troubleshoot hardware and software information assurance problems
b) Recognize a potential security violation, take appropriate action to report the incident as required by regulations, and mitigate any adverse impact
c) Apply appropriate system access controls
d) Implement, apply, and monitor established IA safeguards in accordance implementation plans and standard operating procedures
e) Implement applicable patches including information assurance vulnerability alerts (IAVA), information assurance vulnerability bulletins, and technical advisories
f) Understand and implement technical vulnerability corrections
g) Enter assets in the DOD vulnerability management system
h) Implement DOD and component password policy
i) Implement specific IS security countermeasure
j) Analyze patterns of noncompliance and take appropriate technical actions to minimize security risks and insider threat
k) Manage accounts, network rights, and access to systems and equipment
l) Assess the performance of IA security controls within the security system
m) Evaluate potential IA security risks and take appropriate corrective and recovery action.
n) Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the system security plans and requirements
o) Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements
p) Develop and implement access consol lists on routers, firewalls, and other network devices
q) Install perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic
r) Implement response actions in reaction to security incidents
s) Provide direction to system developers regarding correction of security problems identified during testing
t) Develop and apply effective vulnerability countermeasures for the enclave
u) Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards
v) Schedule and perform regular and special backups on all enclave systems
w) Analyze IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and take or recommend appropriate action
x) Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the security information system
y) Supervise or manage protective or corrective measure when an IA incident or vulnerability is discovered

z) Ensure that IA requirements are integrated into the Continuity of Operations Plan (COOP) for the security system
aa) Ensure that system security configuration guidelines are followed
bb) Monitor system performance and review for compliance with IA security and privacy requirements within the security system environment
cc) Collect and maintain data needed to meet system IA reporting and C&A requirements
dd) Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of the security network systems operation.
ee) Help prepare IA certification and accreditation documentation
ff) Take actions as needed to ensure that accepted products meet Common Criteria requirements
gg) Evaluate proposals to determine if proposed security solutions effectively address enclave requirements, as detailed in solicitation documents

3.7 Contract Support Information

The paragraphs in the following contract support information section are general in nature. As necessary, individual delivery orders will address the appropriate requirements of this nature and provide more details related to the administration and execution of the task at the specific site.

3.7.1 General

3.7.1.1 Scope Of Work

The Contractor shall provide personnel, equipment, miscellaneous hardware and appurtenances, management, and any other items and services necessary to install a fully operational ISSC following the guidelines described in the Statement of Work (SOW). The Contractor shall act to the standards and specifications in this contract.

3.7.1.1.1 Hours Of Operation

The Contractor shall be required to perform on-site work during the normal operating hours for the individual sites. These operating hours exclude Legal Public Holidays, listed in paragraph 2.4 of this work statement, and emergency service calls. Exceptions to the hours, such as required equipment shutdown, will be reviewed and approved by the COR.

3.7.1.1.2 Security System Operation

Normally, a security system is in operation 24 hours per day, seven days per week, 365 days per year. The Contractor shall conduct all inspections and preventative maintenance activities at times that do not interfere with the operation of the system during normal Operating Hours for the individual site. If possible, only small portions of the system may be taken out of service for maintenance repairs, minor repairs, or major repairs. Emergency repairs may occur at any time as required to expedite placement of any portion of the system back in service. Scheduled maintenance that requires equipment shutdown shall be performed as much as possible over weekends or legal holidays or closed days so that the system is fully operational during normal Operating Hours.

3.7.1.2 Background Information

All activities associated with the security system installation and maintenance shall be coordinated with individual designated point of contact.

3.7.1.3 Government Observations

The Contractor shall not deny Government access to Government owned facilities, equipment, or computers, which are operated by the Contractor. Government personnel will not interfere with Contractor performance.

3.7.1.4 Interface with Government Operation

Performance of work by Contractor personnel under the terms of this contract shall not interfere with regularly scheduled Government operational activities. Exceptions will be reviewed by the COR.

3.7.1.5 Safety

The Contractor shall provide for the safety and well-being of personnel employed in the administration of this contract. The Contractor shall implement a safety program for employees performing work under this contract.

3.7.1.5.1 Pentagon Renovation Program Safety Requirements

All employees who will be supporting the Pentagon Renovation Program shall meet the following requirements:

3.7.1.5.1.1 Shall attend the safety-training program prior to reporting to work.

3.7.1.5.1.2 Shall have Personal Protective Equipment (PPE) when on site to include: safety glasses,
reflective vest, safety helmet, and work boots.

3.7.1.5.2 Safety Plan

The contractor shall implement a safety plan as part of the safety program, if not already in place. This shall be in accordance with standard commercial practices.

3.7.1.5.3 Accident Reporting

The Contractor shall maintain an accurate record of accidents resulting in traumatic injury or death and accidents resulting in damage to Government property, supplies, and equipment. The Contractor shall report accidents to the Government in writing within the time frame specified by OSHA.

3.7.1.5.4 Occupational Safety and Health Act (OSHA)

The Contractor shall comply with the OSHA. Contractor personnel shall wear safety items required by OSHA during the performance of tasks requiring protective equipment or clothing.

3.7.1.5.5 Smoking

The Contractor shall comply with policies governing smoking at the specific Government facilities involved.

3.7.1.6 Security

Contractor personnel or any representative of the Contractor, entering DoD facilities shall abide by all security regulations. They shall be subject to security checks according to Title 32, Code of Federal Regulations, Part 40b, and Title 18 USC, Section 930.

3.7.1.6.1 Installation Access

The Contractor shall be responsible for assuring all Contractor personnel authorized to do work under this contract obtain installation access. The Contractor shall abide by each site's access policies. When the employee no longer does work under the delivery order, the Contractor shall return Government furnished identification.

3.7.1.6.2 Vehicle Registration

Contractor personnel owned or company owned motor vehicles entering DoD facilities shall have a valid state license and shall be registered with the DoD site, if required. The Contractor shall register the vehicles before commencement of contract work. State license and registration shall be maintained current while the vehicle is in use at each DoD facility. Contractor personnel, operating motor vehicles on a DoD facility, shall have a valid state operator's license for the category of vehicle being operated. The drivers shall comply with Title 32, Code of Federal Regulations, Part 40b regarding motor vehicle use at each installation. The Contractor shall provide transportation for Contractor personnel to and from local security installation sites.

3.7.1.6.3 Search and Seizure

Contractor personnel and property shall be subject to search and seizure upon entering a DoD facility, while at a DoD facility, and upon leaving a DoD facility in accordance with Title 32, Code of Federal Regulations, Part 40b and Title 18 USC, Section 930.

3.7.1.7 Conservation of Utilities

Contractor personnel shall practice utilities conservation and shall operate under conditions that preclude waste of Government furnished utilities.

3.7.1.8 Codes

All applicable national and local codes shall apply to the particular type(s) of equipment being maintained and all service and repair work shall meet national safety codes and regulations.

3.7.2 Property Installed at the Pentagon/Facility and Services

For each site where the ISSC will be installed, the Government will provide a list of the property and services that the Government will provide to the Contractor.

3.7.2.1 Property

The Contractor shall not use property provided by the Government for any purpose other than in the performance of this contract.

3.7.2.1.1 Facilities

The COR in conjunction with the Contracting Officer will review and decide upon requests for the Government to supply an area for the Contractor to place a Contractor's site trailer for day to day operations at a specific DoD facility during the performance of a delivery order. Utility outlets will be provided for the Contractor's use with the site trailer. Specific information concerning this arrangement will be specified in the delivery order.

3.7.2.1.2 Equipment
The Contractor is to supply all equipment necessary to support this SOW, except that equipment explicitly identified as Government Furnished Equipment.

3.7.2.1.4 Forms
The Government will provide Government forms necessary for the Contractor to perform to the SOW.

3.7.2.1.5 Publications
The Government will provide publications defined as Government Furnished Information in the SOW.

3.7.2.1.6 Parking
The Government will furnish parking space for Contractor employees' privately owned vehicles (POV) and Contractor owned vehicles at a designated parking area at each DoD facility during the performance of a delivery order, as space permits.

3.7.2.2 Services

3.7.2.2.1 Utilities
The Government will provide and maintain potable water, firewater, and electrical service to the Contractor's trailer.

3.7.2.2.2 Refuse Collection
The Government will provide general refuse collection from Contractor occupied areas on Government property. This does not include disposal of equipment parts or components requiring disposal or hazardous material; this shall be the responsibility of the Contractor.

3.7.3 Contractor Furnished Items

The Contractor shall furnish all property and services necessary to perform the requirements of this contract/delivery orders, other than those identified in delivery orders as GFP. Contractor furnished property and services should interoperate, when possible, with existing Government systems.

3.7.3.1 Property

3.7.3.1.1 Tools and Special Testing Equipment
The Contractor shall furnish all tools and equipment required to install, maintain and repair the systems and equipment defined in this contract. The Contractor shall furnish all special testing

equipment. The Contractor shall have items sufficient for the normal maintenance and expedient emergency repair of the equipment covered under this contract.

3.7.3.1.2 Replacement Parts
The Contractor shall have readily available an adequate supply and/or supplier of emergency repair or replacement parts.

3.7.3.1.3 Automated Integrated Logistics System (AILS) Equipment
The Contractor shall furnish their own computer that is devoted to the AILS. Government shall have access to the AILS electronic database files at all times. Access to the database can be at the Contractor's facility or using the Internet. The Contractor shall furnish to the Government a copy of any software required to allow Government access to the AILS database. The software shall be compatible with a standard computer operating system.

3.7.3.1.4 Office Supplies
The Contractor shall provide all expendable office supplies, computer paper, floppy discs and other materials required to perform services under this contract.

3.7.3.2 Property Storage
The Contractor is responsible for the storage of all equipment and materials associated with this SOW. Any on-site or off-site storage space shall be furnished and maintained by the Contractor at his sole expense. All property stored by the Contractor shall be stored in accordance with the manufacturer's recommendations.

3.7.3.3 Disposal of Damaged or Removed Equipment
The Contractor shall be responsible for disposal of any parts or components associated with this SOW during the performance of a delivery order.

3.7.3.4 Housekeeping Practices
The Contractor shall maintain work areas and occupied spaces, on Government facilities, in a neat, clean, and orderly condition. The Contractor shall promptly remove from the site all old parts or trash generated from a maintenance or repair activity. The Contractor shall adhere to all local, state, and federal environmental regulations regarding the handling and disposal of all cleaning fluids, solvents, and hazardous wastes.

3.7.4 Applicable Documents
For each site where the ISSC will be installed the Government will provide a list of Applicable Documents that the Government will provide or make available to the Contractor.

The Government shall furnish all documents and forms coded as Government-Furnished Information (GFI) and the Contractor shall furnish all documents and forms coded as Contractor-Furnished (C).

The documents will be coded as advisory (A) or mandatory (M). The Contractor shall follow those coded as mandatory, but only to the extent specified in this contract when a specific part of the document is referenced herein. When specific parts of documents coded "M" are referenced,

the referenced, the remainder of that document may be considered "A". Supplements, amendments, or revisions to mandatory documents may be issued during the term of the contract, and shall be in full force and effective immediately upon receipt by the Contractor. The Contractor shall follow the requirements in these mandatory supplements, amendments, or revisions during the life of the contract pending negotiation. The Contractor shall post and update mandatory publications as change notices are provided by the Government.

Upon completion of the order or contract as stated in individual delivery orders, the Contractor shall return to the Government all publications provided to the Contractor by the Government. For documents furnished by the Contractor, the Contractor shall be responsible for maintaining current documents and for obtaining all supplements, amendments, and revisions as they become issued.

3.7.5 Proposal Response

When the contractor receives a Request for Proposal or Quotation the usual response times will be as follows:

Priority (Surge) – the contractor will provide a complete proposal or quote within one (1) business day after receipt of the RFP/RFQ.

Routine - the contractor will provide a complete proposal or quote within three- (3) business day after receipt of the RFP/RFQ.

Allowances can be made for unusual situations.

3.8 Organizational Conflict of Interest

The term "organizational conflict of interest" means that the Contractor (which term hereinafter shall be deemed to include its chief executives, directors, any consultants, or subcontractors utilized under this contract other than a vendor selling incidental material) has interests which (i) may diminish its capacity to give impartial, technically sound, objective assistance and advice in performing this contract, (ii) may otherwise result in a biased work product under this contract, or (iii) may result in an unfair competitive advantage to itself or others.

The contractor's attention is directed to FAR Subpart 9.5, Organizational Conflicts of Interest. In the execution of certain contract tasks, it is anticipated that assigned contractor personnel will require access to confidential or proprietary business, technical and financial information belonging to the Government or other companies. The information may include but is not limited to pre-decisional budget and acquisition sensitive information, preparation of specifications or work statements, and evaluation services. After receipt thereof, the contractor and affected individuals shall treat such information as confidential and agree not to appropriate such information to its own use or to disclose such information to third parties unless specifically authorized by the contracting officer in writing. The foregoing obligations, however, shall not apply to:

- Information which, at the time of receipt by the contractor, is in the public domain;

- Information which is published after receipt thereof by the contractor or otherwise becomes part of the public domain through no fault of the contractor;

- Information which the contractor can demonstrate was in his possession at the time of receipt thereof and was not acquired directly or indirectly from the Government or other companies;

- Information, which the contractor can demonstrate, was received by it from a third party that did not require the contractor to hold it in confidence.

The contractor shall obtain the written agreement, in a form satisfactory to the contracting officer, of each employee permitted access, whereby the employee agrees that he will not discuss, divulge or disclose any such information or data to any person or entity except those persons within the contractor's organization directly concerned with the performance of the contract.

The contractor agrees, if requested by the Government, to sign an agreement identical, in all material respects, to the provisions of this clause, with each company supplying information to the contractor under this contract, and to supply a copy of such agreement to the contracting officer. From time to time upon request of the contracting officer, the contractor shall supply the Government with reports itemizing information received as confidential, proprietary, pre-decisional budget information, or acquisition sensitive information, and setting forth the company or companies from which the contractor received such information.

The contractor agrees that upon request by the contracting officer it will execute a contracting officer approved agreement with any party whose facilities or proprietary data it is given access to or is furnished, restricting use and disclosure of the data or the information obtained from the facilities. Upon request by the contracting officer, contractor personnel shall also sign such an agreement.

If after award, the contractor discovers an organizational conflict of interest, with respect to this contract, it shall make an immediate and full disclosure in writing to the Contracting Officer. The disclosure shall include identification of the conflict, the manner in which it arose, and a description of the action the Contractor has taken or proposes to take to avoid, eliminate or neutralize the conflict. The Government may, however, terminate the contract.

In the event that the Contractor was aware of an organizational conflict of interest prior to award of this contract and did not disclose the conflict to the Contracting Officer or becomes aware of an organizational conflict of interest after award of this contract and does not disclose the conflict of interest within ten (10) working days of becoming aware of such conflict, the Government may terminate the contract and the contractor shall not be entitled to reimbursement of any cost

incurred in performing this contract or payment of any fee thereunder. Further, such costs shall not be allocable or chargeable, directly or indirectly, to any other contract with the Government.

The rights and remedies of the Government provided in this clause shall not be exclusive and are in addition to any other rights and remedies of the Government provided by law or under this contract.

The Contractor agrees that during performance of the contract and for a period of three (3) years after the completion of performance of this contract, the Contractor, including all divisions thereof, and any affiliate of the Contractor, any joint venture involving the Contractor, any entity into or with which it may subsequently merge or affiliate, or any other successor or assign of the contractor, shall not:

(a) Supply information or material received from this contract, to any firm participating in or having a known prospective interest in the subject matter areas for which the sensitive information described in paragraph (i) above was initially submitted, nor enter into any contractual relationship which would affect or appear to affect the equity and integrity of its recommendations.

(b) Furnish to the United States Government, either as a prime contractor or as a subcontractor, any component of any system for which the sensitive information described in paragraph (1) above was initially submitted, that it is not currently obligated to deliver for defense purposes.