AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) ▶	RATING	PAGE 1 OF 1 PAGES

2. CONTRACT *(Proc. Inst. Indent.)* NO. GS00Q12NRD4010	3. EFFECTIVE DATE See Blk 20c	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.

5. ISSUED BY CODE NR000

General Services Administration
Federal Acquisition Service,
10304 Eaton Place, Suite 2B-20
Fairfax, VA 22030

6. ADMINISTERED BY *(If other than Item 5)* CODE NR000

General Services Administration
Federal Acquisition Service,
10304 Eaton Place, Suite 2B-20
Fairfax, VA 22030

7. NAME AND ADDRESS OF CONTRACTOR *(No., street, county, State and ZIP Code)*

TeleCommunication Systems, Inc. (TCS)
275 West Street
Annapolis, MD 21401

CODE 0HAL7 FACILITY CODE

8. DELIVERY

□ FOB ORIGIN □ OTHER *(See below)*

9. DISCOUNT FOR PROMPT PAYMENT

10. SUBMIT INVOICES *(4 copies unless otherwise specified)* TO THE ADDRESS SHOWN IN ▶ ITEM 12

11. SHIP TO/MARK FOR CODE NR000

General Services Administration/FAS
10304 Eaton Place, Suite 2C-05
Fairfax, VA 22030-2337

12. PAYMENT WILL BE MADE BY CODE

General Program Division
PO Box 419279 Room-1011
Kansas City, MO 64131

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:

□ 10 U.S.C. 2304(c)( ) □ 41 U.S.C. 253(c)( )

14. ACCOUNTING AND APPROPRIATION DATA

2012.2012.299X.TDBA.00.A00VB120.TDR17.H08.
TS1006

15A. ITEM NO.	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
		1		1,000.00	1,000.00

15G. TOTAL AMOUNT OF CONTRACT ▶ $ 1,000.00

16. TABLE OF CONTENTS

CONTRACTING OFFICER WILL COMPLETE ITEM 17 (SEALED-BID OR NEGOTIATED PROCUREMENT) OR 18 (SEALED-BID PROCUREMENT) AS APPLICABLE

17. ☒ CONTRACTOR'S NEGOTIATED AGREEMENT *(Contractor is required to sign this document and return* 1 *copies to issuing office.)* Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. *(Attachments are listed herein.)*

18. □ SEALED-BID AWARD *(Contractor is not required to sign this document.)* Your bid on Solicitation Number including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the terms listed above and on any continuation sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your bid, and (b) this award/contract. No further contractual document is necessary. (Block 18 should be checked only when awarding a sealed-bid contract.)

19A. NAME AND TITLE OF SIGNER *(Type or Print)*

Richard A. Young
Executive Vice President and Chief Operating Officer

20A. NAME OF CONTRACTING OFFICER

Jenni K. Lewis

19B. NAME OF CONTRACTOR

BY Richard A. Young
(Signature of person authorized to sign)

19C. DATE SIGNED

08/28/2012

20B. UNITED STATES OF AMERICA

BY

Digitally signed by JENNI LEWIS
DN: c=US, o=U.S. Government, ou=General Services Administration, cn=JENNI LEWIS, 0.9.2342.19200300.100.1.1=47001000015913
Date: 2012.08.29 14:19:00 -04'00'

(Signature of Contracting Officer)

20C. DATE SIGNED

29Aug2012

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition is NOT usable

MSK

STANDARD FORM 26 (REV. 5/2011)
Prescribed by GSA - FAR (48 CFR) 53.214(a)

Notice Concerning Award

AWARD NO: GS00Q12NRD4010

CUSTOM SATCOM SOLUTIONS (CS2)

GSA ITS Acquisition Contract No. CONTRACT # GS00Q12NRD4010

Contract Type: Fixed Price, Multiple Award Indefinite Delivery, Indefinite Quantity Contract.

Contract Term: Base period of three (3) years and two (2) one-year Government options.

Minimum Dollar Guarantee and Maximum Contract Limitation

a. The minimum dollar guarantee for this contract is $1,000**.**

b. The maximum all-inclusive funding ceiling for this and any other contracts awarded as a result of solicitation No. QTA010CTA0003 is $2.6 Billion.

The minimum dollar guarantee and maximum contract limitation shall be applied to the base terms and all option years

Document Wide Changes

- The CS2 RFP number QTA010CTA0003 is replaced with CS2 contract number GS00Q12NRD4010.
- The word, "offeror," is replaced with contractor where appropriate.
- The word, "RFP," is replaced with the word, "contract," where appropriate.
- All amendment numbers in the headers are deleted.
- All dates in the footers are deleted.
- Each section contains continuous pagination. (Section B tables and Section J attachments remain separately paginated)

The following provision is incorporated in to the contract:

- The contractor's Final Revised Price Proposal, dated **May 16, 2012**, and all amendments thereto are hereby incorporated by reference into this contract.

Section A

The following content changes have been made to Section A:

Section A	Content of Change
A	The section title and Table of contents are changed from "Standard Form 33, Solicitation, Offer and Award" to Standard Form 26, Award Contract."
A	SF 30 is replaced with SF26

Section B

The following content changes have been made to the Section B tables:

Section B	Content of Change
Section B	Incorporation of the Contractor’s Section B price tables in Microsoft Excel
Section B tables	References to “Year 4” and “Year 5” and been changed to “Option 1” and “Option 2” in the Section B tables.

Section C

No content changes were made to Section C.

Section D

No content changes were made to Section D.

Section E

No content changes were made to Section E.

Section F

No content changes were made to Section F.

Section G

No content changes were made to Section G.

Section H

The following content changes have been made to the Section H:

Section H	Content of Change
Section H-12	Added date the PCO approved the submitted Small Business Subcontracting Plan

Section I

The following content changes have been made to Section I:

Section I	Content of Change
I	Inclusion of Clause 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (May 2012)

Section J

The following content changes have been made to Section J:

Section J	Content of Change
J	Table of contents changed to reflect the removal of Attachment J-4, “Small Business Subcontracting Goals Guidance;” Attachment J-7, “Corporate Experience Narrative;” and Attachment J-8, “Past Performance Questionnaire”
Attachment J-4	Deleted
Attachment J-7	Deleted
Attachment J-8	Deleted

Section K

Deleted.

Section L

Deleted.

Section M

Deleted.

SF26 AWARD DOCUMENT IS ATTACHED AS A SEPARATE PDF FILE

B.2.1 Pricing Tables (Year 1)

Table B.2.1-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	Service or Product	Price (Year 1)
100000-1	MWR Overall System Price	$32,469,893

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.1-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)				
CLIN*	Service or Product	Description of Service or Product	[redacted]	Price (Year 1)
100001-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	$458,918
100002-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year	[redacted]	$8,068,608
100003-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	$235,008
100004-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	$424,320
100005-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/Middle East per year	[redacted]	$7,523,846
100006-1	Service	Network operations center (NOC) operations cost	[redacted]	$217,200
100007-1	Service	Equipment Lease	[redacted]	$9,690,000
100008-1	Service	Installation - CENTCOM	[redacted]	$4,869,928
100009-1	Service	Installation - AFRICOM	[redacted]	$95,640
100010-1	Service	Installation - EUCOM, PACOM, BIOT	[redacted]	$266,041

100011-1	Service	Program Management cost per month	[redacted]	[redacted]	$125,976
100012-1	Service	Training	[redacted]	[redacted]	$53,864
100013-1	Service	Engineering Support cost per month	[redacted]	[redacted]	$277,656
100014-1	Service	Sustainment support cost per month	[redacted]	[redacted]	$162,888
		Optional Year 1 CLINs	[redacted]	[redacted]	
100015-1	Service	Onsite Technical Support – Africa per day	[redacted]	[redacted]	
100016-1	Service	Onsite Technical Support – Southwest Asia/Middle East per day	[redacted]	[redacted]	
100017-1	Service	Onsite Technical Support – Central Asia per day	[redacted]	[redacted]	
100018-1	Service	Onsite Technical Support – Pacific per day	[redacted]	[redacted]	
100019-1	Service	Onsite Technical Support – Europe per day	[redacted]	[redacted]	
100020-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	[redacted]	
100021-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per month	[redacted]	[redacted]	
100022-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	[redacted]	
100023-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	[redacted]	
100024-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per month	[redacted]	[redacted]	
100025-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per ORDU	[redacted]	[redacted]	
100026-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per ORDU	[redacted]	[redacted]	
100027-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per ORDU	[redacted]	[redacted]	
100028-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per ORDU	[redacted]	[redacted]	

100029-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per ODRU	[redacted]	
100030-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per LDRU	[redacted]	
100031-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per LDRU	[redacted]	
100032-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per LDRU	[redacted]	
100033-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per LRDU	[redacted]	
100034-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per LDRU	[redacted]	
100035-1	Product	Large Remote Deployable Units (LDRU's)	[redacted]	
100036-1	Product	Outpost Remote Deployable Units (ODRU's)	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

B.2.2 Pricing Tables (Year 2)

Table B.2.2-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	**Service or Product**	**Price (Year 2)**
100000-2	MWR Overall System Price	$17,383,001

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.2-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 2)**

			[redacted]	[redacted]	
100001-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	[redacted]	$470,391
100002-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year	[redacted]	[redacted]	$8,270,323
100003-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	[redacted]	$240,883
100004-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	[redacted]	$434,928
100005-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/Middle East per year	[redacted]	[redacted]	$7,711,943
100006-2	Service	Network operations center (NOC) operations cost	[redacted]	[redacted]	$148,416
100007-2	Service	Equipment Lease	[redacted]	[redacted]	$1
100008-2	Service	Installation - CENTCOM	[redacted]	[redacted]	$0
100009-2	Service	Installation - AFRICOM	[redacted]	[redacted]	$0
100010-2	Service	Installation - EUCOM, PACOM, BIOT	[redacted]	[redacted]	$0
100011-2	Service	Program Management cost per month	[redacted]	[redacted]	$23,004
100012-2	Service	Engineering Support cost per month	[redacted]	[redacted]	$47,124
100013-2	Service	Sustainment support cost per month	[redacted]	[redacted]	$35,988
		Optional Year 2 CLINs	[redacted]	[redacted]	
100014-2	Service	Onsite Technical Support – Africa per day	[redacted]	[redacted]	
100015-2	Service	Onsite Technical Support – Southwest Asia/Middle East per day	[redacted]	[redacted]	
100016-2	Service	Onsite Technical Support – Central Asia per day	[redacted]	[redacted]	
100017-2	Service	Onsite Technical Support – Pacific per day	[redacted]	[redacted]	
100018-2	Service	Onsite Technical Support – Europe per day	[redacted]	[redacted]	
100019-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	[redacted]	

100020-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per month	[redacted]	
100021-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	
100022-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	
100023-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per month	[redacted]	
100024-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per ORDU	[redacted]	
100025-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per ORDU	[redacted]	
100026-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per ORDU	[redacted]	
100027-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per ORDU	[redacted]	
100028-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per ODRU	[redacted]	
100029-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per LDRU	[redacted]	
100030-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per LDRU	[redacted]	
100031-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per LDRU	[redacted]	
100032-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per LRDU	[redacted]	
100033-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per LDRU	[redacted]	

100034-2	Product	Large Remote Deployable Units (LDRU's)	[redacted]	
100035-2	Product	Outpost Remote Deployable Units (ODRU's)	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

B.2.3 Pricing Tables (Year 3)

Table B.2.3-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	**Service or Product**	**Price (Year 3)**
100000-3	MWR Overall System Price	$13,381,231

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.3-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 3)**
100001-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	$361,613
100002-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year	[redacted]	$6,357,811
100003-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	$185,179
100004-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	$334,351
100005-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/Middle East per year	[redacted]	$5,928,556
100006-3	Service	Network operations center (NOC) operations cost	[redacted]	$114,084
100007-3	Service	Equipment Lease	[redacted]	$1

100008-3	Service	Installation - CENTCOM	[redacted]	[redacted]	$0
100009-3	Service	Installation - AFRICOM	[redacted]	[redacted]	$0
100010-3	Service	Installation - EUCOM, PACOM, BIOT	[redacted]	[redacted]	$0
100011-3	Service	Program Management cost per month	[redacted]	[redacted]	$23,580
100012-3	Service	Engineering Support cost per month	[redacted]	[redacted]	$39,168
100013-3	Service	Sustainment support cost per month	[redacted]	[redacted]	$36,888
		Optional Year 3 CLINs	[redacted]	[redacted]	
100014-3	Service	Onsite Technical Support – Africa per day	[redacted]	[redacted]	
100015-3	Service	Onsite Technical Support – Southwest Asia/Middle East per day	[redacted]	[redacted]	
100016-3	Service	Onsite Technical Support – Central Asia per day	[redacted]	[redacted]	
100017-3	Service	Onsite Technical Support – Pacific per day	[redacted]	[redacted]	
100018-3	Service	Onsite Technical Support – Europe per day	[redacted]	[redacted]	
100019-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	[redacted]	
100020-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per month	[redacted]	[redacted]	
100021-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	[redacted]	
100022-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	[redacted]	
100023-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per month	[redacted]	[redacted]	
100024-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per ORDU	[redacted]	[redacted]	
100025-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per ORDU	[redacted]	[redacted]	
100026-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per ORDU	[redacted]	[redacted]	

100027-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per ORDU	[redacted]	[redacted]	
100028-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per ODRU	[redacted]	[redacted]	
100029-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year per LDRU	[redacted]	[redacted]	
100030-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia per year per LDRU	[redacted]	[redacted]	
100031-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year per LDRU	[redacted]	[redacted]	
100032-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year per LRDU	[redacted]	[redacted]	
100033-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe/ Middle East per year per LDRU	[redacted]	[redacted]	
100034-3	Product	Large Remote Deployable Units (LDRU's)	[redacted]	[redacted]	
100035-3	Product	Outpost Remote Deployable Units (ODRU's)	[redacted]	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

B.2.4 Pricing Tables (Year 4)

Table B.2.4-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.4-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)

[redacted]

[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

B.2.5 Pricing Tables (Year 5)

Table B.2.5-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.5-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

[redacted]

[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

B.2.1 Pricing Tables (Year 1)

Table B.2.1-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 1)**
200000-1	GETN Overall System Price	$10,015,251

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.1-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 1)**
200000-1	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 0.5 MHz (13.5 MHz is required times 12 months)	[redacted]	$0
200001-1	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 1 MHz (13.5 MHz is required times 12 months)	[redacted]	$893,106
200002-1	Service	Network operations center (NOC) operations cost	[redacted]	$383,712
200003-1	Product	Gateway Site terminal cost	[redacted]	$1,709,043
200004-1	Product	Remote Site terminals cost HX system per unit	[redacted]	$2,385,020
200005-1	Product	Remote Site terminals cost Power View per unit	[redacted]	$1,113,400
200006-1	Service	Installation	[redacted]	$2,786,430
200007-1	Service	Training	[redacted]	$61,104
200008-1	Service	Project Management cost per month	[redacted]	$150,300
200009-1	Service	Engineering Support cost per month	[redacted]	$365,904
200010-1	Service	Sustainment support cost per month	[redacted]	$167,232

*CLINs 200000 through 299999 are reserved for GETN

B.2.2 Pricing Tables (Year 2)

Table B.2.2-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 2)**
200000-2	GETN Overall System Price	$1,414,890

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.2-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 2)**
200000-2	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 0.5 MHz	[redacted]	$0
200001-2	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 1 MHz	[redacted]	$915,462
200002-2	Service	Network operations center (NOC) operations cost	[redacted]	$393,312
200003-2	Product	Gateway Site terminal cost	[redacted]	$0
200004-2	Product	Remote Site terminals cost HX system per unit	[redacted]	$0
200005-2	Product	Remote Site terminals cost Power View per unit	[redacted]	$0
200006-2	Service	Installation	[redacted]	$0
200007-2	Service	Project Management cost per month	[redacted]	$23,004
200008-2	Service	Engineering Support cost per month	[redacted]	$47,124
200009-2	Service	Sustainment support cost per month	[redacted]	$35,988

*CLINs 200000 through 299999 are reserved for GETN

B.2.3 Pricing Tables (Year 3)

Table B.2.3-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 3)**
200000-3	GETN Overall System Price	$1,441,080

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.3-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 3)**
200000-3	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 0.5 MHz	[redacted]	$0
200001-3	Service	Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) 1 MHz	[redacted]	$938,304
200002-3	Service	Network operations center (NOC) operations cost	[redacted]	$403,140
200003-3	Product	Gateway Site terminal cost	[redacted]	$0
200004-3	Product	Remote Site terminals cost HX system per unit	[redacted]	$0
200005-3	Product	Remote Site terminals cost Power View per unit	[redacted]	$0
200006-3	Service	Installation	[redacted]	$0
200007-3	Service	Project Management cost per month	[redacted]	$23,580
200008-3	Service	Engineering Support cost per month	[redacted]	$39,168
200009-3	Service	Sustainment support cost per month	[redacted]	$36,888

*CLINs 200000 through 299999 are reserved for GETN

B.2.4 Pricing Tables (Year 4)

Table B.2.4-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.4-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

B.2.5 Pricing Tables (Year 5)

Table B.2.5-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.5-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

B.2.1 Pricing Tables (Year 1)

Table B.2.1-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 1)**
300000-1	BPT Overall System Price	$8,941,871

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.1-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 1)**
300000-1	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	$3,649,536
300001-1	Service	Multi-Cast Broadcast Channel (1 per region per year)	[redacted]	$1,152,000
300002-1	Service	Network operations center (NOC) operations cost per month	[redacted]	$72,396
300003-1	Product	IOC Central Site terminal cost	[redacted]	$1,303
300004-1	Product	Remote Site terminals cost per unit (IOC Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	$2,487,780
300005-1	Product	Remote Site antenna cost per unit (IOC + Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	$660,960
300006-1	Product	Remote Site vehicle mount cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$12,852
300007-1	Product	Remote Site vehicle power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$33,048
300008-1	Product	Remote Site universal AC power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$39,780
300009-1	Product	Remote Site emergency power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$99,756

3000010-1	Product	Remote Site AC/DC power supply (installed in transit case) cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$99,756
300011-1	Product	Remote Site transit case cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$206,244
300012-1	Service	Program Management cost per month	[redacted]	$79,632
300013-1	Service	Training	[redacted]	$31,276
300014-1	Service	Engineering Support cost per month	[redacted]	$96,288
300015-1	Service	Sustainment support cost per month	[redacted]	$219,264
		Optional CLINs (Year 1)	[redacted]	
300016-1	Service	Terminal (entire kit)	[redacted]	
300017-1	Product	FOC additional Central Site terminals cost per unit	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.2 Pricing Tables (Year 2)

Table B.2.2-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 2)**
300000-2	BPT Overall System Price	$4,985,796

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.2-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)				
CLIN*	**Service or Product**	**Description of Service or Product**	[redacted]	**Price (Year 2)**
300000-2	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	$3,649,536
300001-2	Service	Multi-Cast Broadcast Channel (1 per region per year)	[redacted]	$1,180,800

300002-2	Service	Network operations center (NOC) operations cost per month	[redacted]	[redacted]	$74,208
300003-2	Product	IOC Central Site terminal cost	[redacted]	[redacted]	$0
300004-2	Product	Remote Site terminals cost per unit (IOC Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	[redacted]	$0
300005-2	Product	Remote Site antenna cost per unit (IOC + Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	[redacted]	$0
300006-2	Product	Remote Site vehicle mount cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300007-2	Product	Remote Site vehicle power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300008-2	Product	Remote Site universal AC power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300009-2	Product	Remote Site emergency power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300010-2	Product	Remote Site AC/DC power supply (installed in transit case) cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300011-2	Product	Remote Site transit case cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	[redacted]	$0
300012-2	Service	Program Management cost per month	[redacted]	[redacted]	$23,004
300013-2	Service	Training	[redacted]	[redacted]	$0
300014-2	Service	Engineering Support cost per month	[redacted]	[redacted]	$38,208
300015-2	Service	Sustainment support cost per month	[redacted]	[redacted]	$20,040
		Optional CLINs (Year 1)	[redacted]	[redacted]	
300016-2	Service	Terminal (entire kit)	[redacted]	[redacted]	
300017-2	Product	FOC additional Central Site terminals cost per unit	[redacted]	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.3 Pricing Tables (Year 3)

Table B.2.3-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 3)**

300000-3	BPT Overall System Price	$5,201,681

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.3-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)				
CLIN*	Service or Product	Description of Service or Product	[redacted]	Price (Year 3)
300000-3	Service	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	$3,832,013
300001-3	Service	Multi-Cast Broadcast Channel (1 per region per year)	[redacted]	$1,210,320
300002-3	Service	Network operations center (NOC) operations cost per month	[redacted]	$76,056
300003-3	Product	IOC Central Site terminal cost	[redacted]	$0
300004-3	Product	Remote Site terminals cost per unit (IOC Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	$0
300005-3	Product	Remote Site antenna cost per unit (IOC + Gov Spares + TCS Spares) (3000 + 30 + 30)	[redacted]	$0
300006-3	Product	Remote Site vehicle mount cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300007-3	Product	Remote Site vehicle power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300008-3	Product	Remote Site universal AC power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300009-3	Product	Remote Site emergency power supply cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300010-3	Product	Remote Site AC/DC power supply (installed in transit case) cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300011-3	Product	Remote Site transit case cost per unit (IOC + Gov Spares + TCS Spares) (600 + 6 + 6)	[redacted]	$0
300012-3	Service	Program Management cost per month	[redacted]	$23,580
300013-3	Service	Training	[redacted]	$0

300014-3	Service	Engineering Support cost per month	[redacted]	[redacted]	$39,168
300015-3	Service	Sustainment support cost per month	[redacted]	[redacted]	$20,544
		Optional CLINs (Year 1)	[redacted]	[redacted]	
300016-3	Service	Terminal (entire kit)	[redacted]	[redacted]	
300017-3	Product	FOC additional Central Site terminals cost per unit	[redacted]	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.4 Pricing Tables (Year 4)

Table B.2.4-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.4-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

[redacted]

*CLINs 300000 through 399999 are reserved for BPT

B.2.5 Pricing Tables (Year 5)

Table B.2.5-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.5-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

[redacted]

*CLINs 300000 through 399999 are reserved for BPT

SECTION B
SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

The Contractor shall propose firm-fixed prices for each year of the period of performance which consists of a 3-year base period, plus two 1-year option periods. It is the Government's intention, through this section, to obtain prices for the services, related features, and equipment described in Section J Sample Task Orders (STOs). All prices shall conform to the format and structure defined herein.

B.2 SERVICES AND PRICES

Item prices shall be provided for the entire 5-year period. Each pricing element will be identified by a Contract Line Item Number (CLIN). CLIN ranges are allocated by STO number.

CLIN(s) for the 5-year period are six-digit numbers. For each CLIN, the Contractor may propose a single firm fixed price which would be valid for all 5 years of the contract. If proposed, the Contractor must clearly specify this in the pricing tables of its proposal. Alternately, separate pricing may be offered for each contract year using the CLIN structure defined below. CLIN periods for years 2 -5 will use the same CLIN structure as defined for year 1 and include a dash (-) with applicable years 2 through 5. For example, Table B.2-1 illustrates an acceptable CLIN numbering structure.

Table B.2-1. Notional CLIN Numbering Structure

Contract Year	CLIN
Year 1	100000-1
Year 2	100000-2
Year 3	100000-3
Year 4 (First one year option)	100000-4
Year 5 (Second one year option)	100000-5

For each STO, the contractor shall provide an overall system price for year 1 through 5. Additionally, the contractor shall separately price individual items detailed for each STO in Section J. The Offeror shall clearly identify how the separately priced individual items add up to the overall system price. The contractor may provide additional line item pricing as needed.

This pricing applies specifically to the STOs as outlined in the attachments of Section J. The individual prices provided in the Section B tables below are for the proposed solutions should they be required and ordered exactly as outlined in the Section J attachments.

All prices shall include the 2% GSA Management Fee. Prices shall be specified and billed in United States (U.S.) currency.

B.2.1 Pricing Tables (Year 1)

Table B.2.1-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	**Service or Product**	**Price (Year 1)**
100000-1	MWR Overall System Price	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.1-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 1)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per year	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month (excluding Onsite Technical Support)	[redacted]	
	Onsite Technical Support – Africa per day	[redacted]	
	Onsite Technical Support – Southwest Asia / Middle East per day	[redacted]	

	Onsite Technical Support – Central Asia per day	[redacted]	
	Onsite Technical Support – Pacific per day	[redacted]	
	Onsite Technical Support – Europe per day	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.1-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 1)**
200000-1	GETN Overall System Price	

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.1-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 1)**
	Commercial satellite communications infrastructure per unit cost. (For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) in 0.5 and 1 MHz increments as applicable)	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 200000 through 299999 are reserved for GETN.

Table B.2.1-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 1)**
300000-1	BPT Overall System Price	

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.1-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 1)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	IOC Central Site terminal cost	[redacted]	

	FOC additional Central Site terminals cost per unit	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.2 Pricing Tables (Year 2)

Table B.2.2-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	**Service or Product**	**Price (Year 2)**
100000-2	MWR Overall System Price	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.2-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 2)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per year	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month (excluding Onsite Technical Support)	[redacted]	

	Onsite Technical Support – Africa per day	[redacted]	
	Onsite Technical Support – Southwest Asia / Middle East per day	[redacted]	
	Onsite Technical Support – Central Asia per day	[redacted]	
	Onsite Technical Support – Pacific per day	[redacted]	
	Onsite Technical Support – Europe per day	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.2-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 2)**
200000-2	GETN Overall System Price	

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.2-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 2)**
	Commercial satellite communications infrastructure per unit cost. (For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) in 0.5 and 1 MHz increments as applicable)	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 200000 through 299999 are reserved for MWR.

Table B.2.2-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 2)**
300000-2	BPT Overall System Price	

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.2-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 2)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	IOC Central Site terminal cost	[redacted]	
	FOC additional Central Site terminals cost per unit	[redacted]	

	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.3 Pricing Tables (Year 3)

Table B.2.3-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)		
CLIN*	**Service or Product**	**Price (Year 3)**
100000-3	MWR Overall System Price	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.3-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 3)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per month	[redacted]	
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per year	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month (excluding Onsite Technical Support)	[redacted]	
	Onsite Technical Support – Africa per day	[redacted]	
	Onsite Technical Support – Southwest Asia / Middle East per day	[redacted]	

	Onsite Technical Support – Central Asia per day	[redacted]	
	Onsite Technical Support – Pacific per day	[redacted]	
	Onsite Technical Support – Europe per day	[redacted]	

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.3-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)		
CLIN*	**Service or Product**	**Price (Year 3)**
200000-3	GETN Overall System Price	

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.3-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 3)**
	Commercial satellite communications infrastructure per unit cost. (For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) in 0.5 and 1 MHz increments as applicable)	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	Gateway Site terminal cost	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 200000 through 299999 are reserved for MWR.

Table B.2.3-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)		
CLIN*	**Service or Product**	**Price (Year 3)**
300000-3	BPT Overall System Price	

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.3-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)			
CLIN*	**Service or Product**	[redacted]	**Price (Year 3)**
	Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost	[redacted]	
	Network operations center (NOC) operations cost	[redacted]	
	IOC Central Site terminal cost	[redacted]	
	FOC additional Central Site terminals cost per unit	[redacted]	
	Remote Site terminals cost per unit	[redacted]	
	Engineering Support cost per month	[redacted]	
	Sustainment support cost per month	[redacted]	

*CLINs 300000 through 399999 are reserved for BPT

B.2.4 Pricing Tables (Year 4, first one year option)

Table B.2.4-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.4-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.4-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.4-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for MWR.

Table B.2.4-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.4-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

*CLINs 300000 through 399999 are reserved for BPT

B.2.5 Pricing Tables (Year 5, second one year option)

Table B.2.5-1a Overall System Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.5-1b Detailed Price Table: Morale, Welfare, and Recreation (MWR)

Morale, Welfare, and Recreation (MWR)
[redacted]

[redacted]

*CLINs 100000 through 199999 are reserved for MWR.

Table B.2.5-2a Overall System Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for GETN

Table B.2.5-2b Detailed Price Table: Government Education and Training Network (GETN)

Government Education and Training Network (GETN)
[redacted]

*CLINs 200000 through 299999 are reserved for MWR.

Table B.2.5-3a Overall System Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)
[redacted]

*CLINs 300000 through 399999 are reserved for BPT

Table B.2.5-3b Detailed Price Table: Blue Personnel Tracking (BPT)

Blue Personnel Tracking (BPT)	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

*CLINs 300000 through 399999 are reserved for BPT

B.3 MAXIMUM CONTRACT VALUE AND MINIMUM REVENUE GUARANTEE

The total maximum value of all services under the Basic Contract (for all awardees combined) shall not exceed $2.6 Billion, including the Options.

The minimum revenue guarantee (MRG) amount for each award will be $1,000.

B.4 GSA MANAGEMENT FEE

The GSA Management Fee is 2% to be applied to the total price for Contractor performance as billed to the Government.

Contractors must include the fee in their proposed prices on all Orders.

The Contractor remits the fee to GSA in accordance with Section G.4.2.

B.5 ORDER TYPE

Orders under the Basic Contract will be firm fixed price.

Orders must be Task Orders in compliance with FAR 16.505.

Task Orders may be multi-year and/or include options as defined in FAR Part 17 and agency-specific FAR Part 17 supplements.

B.6 PERFORMANCE BASED PREFERENCE

Pursuant to FAR 37.102(a), the Ordering Contracting Officer (OCO) (See Section G.1) should use performance-based acquisition methods to the maximum extent practicable.

B.7 ORDER PRICING

The OCO is responsible for the determination of price reasonableness for each Order. The OCO must determine fair and reasonable pricing for all Orders in accordance with FAR Subpart 15.4, Contract Pricing, and FAR 16.202, Firm-fixed-price contracts.

B.8 TRAVEL PRICING

Travel will be reimbursed at actual cost in accordance with the limitations set forth in FAR 31.205-46 and the Federal Travel Regulation.

B.9 LABOR SUBJECT TO THE SERVICE CONTRACT ACT (SCA)

To the extent that any labor is subject to the SCA and within scope of an Order and the Basic Contract, the OCO must identify such work on the Order and apply wages in accordance with FAR Subpart 22.10, Service Contract Act Wage Determinations.

Each Order must be tailored to include the appropriate SCA clauses.

(END OF SECTION B)

SECTION C
DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

C.1 OVERVIEW

C.1.1 CONTRACT OBJECTIVE

Contractors are sought who will provide worldwide commercial satellite communications (COMSATCOM) End-to-End Solutions. End-to-End Solutions comprise complete, customized engineered solutions to meet customers’ unique COMSATCOM needs. These solutions may include any combination of fixed satellite services and/or mobile satellite services, components, and/or service enabling components and ancillary equipment such as terminals, teleports, terrestrial tail circuits, Subscriber Identity Module (SIM) cards, and peripherals. End-to-End Solutions may also include, but are not limited to, licensing, integration, installation, testing, network management, engineering and training. Examples of the types of COMSATCOM solutions the Contractor shall have the capability to deliver are included in this section; however, the specific COMSATCOM solutions to be procured will be defined in subsequent Task Orders.

C.2 SUMMARY OF REQUIREMENTS

Unless otherwise stated, the Contractor is solely responsible for all requirements stated herein.

C.2.1 MANAGEMENT

C.2.1.1 The Contractor shall furnish the project management processes and resources needed to plan, direct, coordinate, and implement the contract as well as control the requirements contained in the contract and priced Task Orders.

C.2.1.2 The Contractor shall have the capability to manage multiple simultaneous Task Orders of varying complexity at worldwide locations.

C.2.1.3 The Contractor shall have the capability to develop a Service Plan for each Task Order as part of the Task Order proposal, outlining what is necessary to successfully execute the Task Order. For each Service Plan, the Contractor shall:

C.2.1.3.1 Develop and document an engineered solution that addresses all requirements as outlined in this contract and the specific Task Order.

C.2.1.3.2 Develop and document an engineered solution that identifies all equipment and resources proposed to satisfy the Task Order.

C.2.1.3.3 Develop and document an engineered solution that provides the Contractor's recommended plans to replace equipment and resources in case of failure, except in those cases where the Government has specific sparing requirements.

C.2.1.3.4 Develop and document an engineered solution that addresses the use of Government furnished materials and resources as specified in the Task Order.

C.2.1.3.5 Develop and document an engineered solution that identifies the applicable performance standards, specifies the set of performance metrics for the services the Contractor proposes to use, and describes in detail the methods and measurements with which the Contractor proposes to establish compliance with the performance standards. The Government reserves the right, on a Task Order basis, to identify the performance standards, specify the performance metrics, and describe the methods and measurements to establish compliance with the performance standards.

C.2.1.3.6 Update the Service Plan to reflect all Task Order modifications as required.

C.2.1.4 The Contractor shall have the capability to manage the operations of each proposed subcontractor.

C.2.1.5 The Contractor shall have the capability to provide customers with timely and accurate invoicing, and provide account information as defined in subsequent Task Orders to the Ordering Contracting Officer, Contracting Officers Representative, and Task Monitors.

C.2.2 GENERAL TECHNICAL REQUIREMENTS

C.2.2.1 The Contractor shall provide complete, customized engineered COMSATCOM End-to-End Solutions to meet customers' unique satellite communications needs. These solutions may include any combination of fixed satellite services or mobile satellite services components, and/or service enabling components such as terminals, teleport, and terrestrial interface tail circuits. The Contractor shall also have the ability to supply licensing, integration, network management and engineering services.

C.2.2.2 The Contractor shall provide the COMSATCOM system engineering design, configuration, installation, implementation, training, and on-going maintenance and operational support necessary to deliver a COMSATCOM solution. The Contractor shall have the ability to provide at least, but not limited to, the services identified below:

C.2.2.2.1 Design and Engineering Services including, but not limited to, site surveys, developing specifications, drawings, reports, schedules and other related work products, configuration, implementation and installation;

C.2.2.2.2 Ongoing Maintenance and Operational Support Services including, but not limited to, operations support, maintenance plans, and repair services;

C.2.2.2.3 Customer Care and Helpdesk Support including, but not limited to, identifying the methods of customer access and hours of operation. The Contractor shall have the capability to respond to trouble calls and complaints, with identified points of contact, availability, and procedures for problem resolution, information flow, and escalation;

C.2.2.2.4 Training, including, but not limited to, equipment operations and maintenance training.

C.2.3 REQUIRED COMSATCOM END-TO-END SOLUTION TYPES

C.2.3.1 COMSATCOM End-to-End Solutions include, but are not limited to, any combination of bandwidth, throughput, terminals, other user equipment, teleports, tail circuits, networks, other terrestrial infrastructure, integration and engineering services, and installation, operations, and maintenance.

C.2.3.2 The Contractor's solutions shall meet the Information Assurance, Responsiveness, Portability, Flexibility/Optimization, Capacity, Coverage, Net Ready (Interoperability), Network Monitoring (Net Ops), Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) Identification, Characterization, and Geo-location, and Security requirements outlined in Section C.2.4 as assigned by the Ordering Activity on a Task Order basis.

C.2.3.3 The Contractor shall have the capability to deploy the necessary terminals, teleports, tail circuits, networks, Integration Services, Engineering Services, Licensing, Certification & Accreditation, Network Management, Operations & Maintenance, and Training required by the Ordering Activity.

C.2.3.4 The Contractor shall have the capability to deliver COMSATCOM End-to-End Solutions within each Solution Type meeting or exceeding the following parameters:

C.2.3.4.1 Coverage: COMSATCOM end-to-end solutions delivered to coverage areas involving multiple satellites and associated ground stations and terrestrial infrastructure.

C.2.3.4.2 User/Network Size: COMSATCOM end-to-end solutions comprised of at least 500 end-user locations or points of presence.

C.2.3.4.3 Capacity: COMSATCOM end-to-end solutions requiring at least a total of 3 Transponder Equivalent (TPE) of bandwidth or 100 Mbps committed information rate (CIR) over the satellite links.

C.2.3.4.4 Terminal Types: COMSATCOM end-to-end solutions with terminal populations consisting of multiple variants of fixed land, mobile land, maritime, and/or airborne terminals.

C.2.3.4.5 Network Management: COMSATCOM end-to-end solutions with network management tailored to capture and deliver data elements most relevant to the customer’s requirements.

C.2.3.5 The Contractor shall demonstrate its capability to provide solutions of the scope herein, in response to requirements aligning with each of the following COMSATCOM End-to-End Solution types:

C.2.3.5.1 Interactive Services. The Contractor shall have the capability to provide complete, customized engineering solutions to support 24x7 Interactive Services requirements. Interactive Services involve the ability to connect multiple locations into a real-time two-way interactive network, mostly involving audio and video. Interactive Services includes Distance Learning and Telemedicine type requirements. Interactive Services are often characterized by distribution of a common information stream to multiple locations, scheduling components and conditional access management, changes to the information stream, distribution locations, and network configurations based upon parameters both known and scheduled in advance and in reaction to changing circumstances, integration with terrestrial communication components and systems, and customer tolerance for latency, delay, jitter, and packet loss.

C.2.3.5.2 Continuity of Operations (COOP). The Contractor shall have the capability to provide complete, customized engineering solutions to support COOP requirements. COOP involves the pre-planned establishment and deployment of a backup or alternative communications infrastructure in anticipation that a natural or human caused event disables or destroys the normal, primary communications infrastructure and is focused on reconstitution of the critical communications functionality to continue minimal essential and/or normal operations. When the COOP capability is required, activation is required immediately, often 24 hours or less. COOP includes developing an alternative for portions of, or the entirety of, the normal, primary communications infrastructure, and can be as simple as a set of new Internet Protocol addresses or as complex as replicating the functionality of the entire primary, terrestrial infrastructure. COOP can include requiring a completely different set of hardware, personnel, and network paths, and associated terrestrial infrastructure as an ancillary component of the COMSATCOM based solution.

C.2.3.5.3 Broadcast Satellite Service (BSS). The Contractor shall have the capability to provide complete, customized engineering solutions to support BSS requirements. Broadcast Satellite Services (BSS) involves the collection of voice, video, and/or data into one central site and distribution of that information typically one-way to multiple fixed and/or mobile locations. BSS includes Streaming Media type requirements. BSS is often characterized by high bandwidth requirements, dedicated, fully utilized data streams for the duration of the broadcast, live or real-time distribution, access control for different portions of the information stream, and minimum customer tolerance for latency, delay, and jitter.

C.2.3.5.4 Emergency Responder Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Emergency Responder Operations. Emergency Responder Operations involve reconstituting a communications infrastructure in response to a natural or human caused event that disrupts or destroys the normal, pre-existing communications infrastructure. Emergency Responder Operations involves an ad-hoc, immediate need communications requirement that eventually reverts back to communications infrastructure previously used, quick responsiveness requirement of a few hours to a few days, desire for interoperability among different types of responders, transportability, quick design, implementation, and activation, and the ability to reach back into headquarters and shared information sources. Additionally, it is not uncommon for the requirement to grow significantly from a small number of users (e.g., initial responders) to a large number (e.g., coordinated large-scale humanitarian effort) within a moderate period of time (e.g., 30 days).

C.2.3.5.5 Direct Customer Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Direct Customer Operations requirements. Direct Customer Operations involve the creation of an often preplanned, enabling communications infrastructure to support specific Customer operations, typically because no pre-existing communications infrastructure is available. Direct Customer Operations include the ability to collaborate among various types of Customers, connecting Customers operating on the tactical edge back to headquarters and shared information sources, transportability and mobility requirements, personnel and facility security, information assurance, ability to reconfigure and/or reconstitute quickly in response to changing situations during prosecution of the mission, real-time insight into communications networks status, and moderate to quick responsiveness requirements with deployment required in several hours to several days. These communications solutions are typically for a short duration and mission focused, high priority with the ability to pre-empt other uses of the same communications resources, and cost of the solution as a much lower priority than the ability to utilize the solution as part of executing the mission. Additionally, it is not uncommon for the requirement to grow significantly from a small number of users (e.g., battalion) to a large number within a moderate period of time (e.g., 30 days).

C.2.3.5.6 Steady State Operations. The Contractor shall have the capability to provide complete, customized engineering solutions to support Steady State Operations requirements. Steady State Operations involve long duration, baseline communications services and infrastructure to support enduring user requirements. Steady State Operations include significant pre-planning with more time allowed for design, configuration, implementation, and activation times, ubiquitous access to collaborative and integrated users, fixed infrastructure that responds more slowly to changes, lower priority with the ability to be pre-empted by a higher priority, short term need for the same communications resources, and strong sensitivity to cost of the solution as compared to the technical capability delivered.

C.2.3.5.7 The Government reserves the right to issue requirements aligned with COMSATCOM End-to-End Solution types not included in the list above.

C.2.4 REQUIRED COMSATCOM END-TO-END SOLUTION ATTRIBUTES

C.2.4.1 Information Assurance

C.2.4.1.1 The Contractor shall comply, to the maximum extent practicable, with: The Committee on National Security Systems Policy (CNSSP)

12, "*National Information Assurance Policy for Space Systems used to Support National Security Missions*," or Department of Defense Directive (DoDD) 8581.1, "*Information Assurance (IA) Policy for Space Systems Used by the Department of Defense*."

C.2.4.1.2 The Contractor shall comply with the Federal Information Security Management Act of 2002 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "*Minimum Security Requirements for Federal Information and Information Systems*." In response to Ordering Activity requirements, at a minimum, all Contractor solutions shall meet the requirements assigned against: A low-impact information system (per FIPS 200) that is described in the current revision of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations*," or a Mission Assurance Category (MAC) III system that is described in the current revision of DoD Instruction (DoDI) 8500.2, "*Information Assurance Implementation*."

C.2.4.1.3 On a Task Order basis, the Ordering Activity shall assign an impact level (per FIPS 200 and NIST SP 800-53), or MAC level (per DoDI 8500.2) prior to issuing the initial statement of work. Task Order evaluations shall consider the extent to which the Contractor's solutions accommodates the necessary security controls based upon the assigned impact level or MAC, command encryption/authentication, and other requirements in CNSSP 12 or DoDD 8581.1.

C.2.4.1.4 The Contractor's information assurance boundary is where the Contractor's services connect to the user terminals/equipment (i.e., includes satellite command encryption (ground and space); systems used in the Satellite Operations Centers (SOCs), Network Operations Centers (NOCs) and teleport; and terrestrial infrastructure required for service delivery).

C.2.4.1.5 Ordering Activity reserves the right to independently evaluate, audit, and verify the IA compliance for any proposed or awarded COMSATCOM services. All IA certification, accreditation, and evaluation activities are the responsibility of the ordering activity.

C.2.4.2 Responsiveness

C.2.4.2.1 As specified on a Task Order basis, the Contractor shall deliver solutions in one of the following timeframes after Task Order award:

C.2.4.2.1.1 Standard Service Delivery (30 calendar days or less). Standard Service Delivery is the time required under normal conditions for COMSATCOM services to be available.

C.2.4.2.1.2 Accelerated Service Delivery (7 calendar days or less). Under Accelerated Service Task Orders, service acceptance testing unless otherwise required by the satellite provider or host nation shall be deferred until operations permit.

C.2.4.2.1.3 Time-Critical Service Delivery (4 hours or less). Under Time-Critical Service Task Orders, service acceptance testing unless otherwise required by the satellite provider or host nation shall be deferred until operations permit. Time-Critical Delivery shall be predicated on the availability of pre-planned engineering solutions, pre-planned line-up messages and transmission plans, pre-arranged Host Nation Agreements, terrestrial connectivity (if applicable), and frequency clearance, and the availability of contracted bandwidth.

C.2.4.2.1.4 Extended Service Delivery. The time required under extenuating circumstances to implement a Task Order after order award. Such extenuating circumstances may include extended time required for host nation agreements or landing rights, long-lead terrestrial connectivity, or other time intensive service delivery requirements as defined in the individual Task Order. Any such extended delivery times will be negotiated between the Ordering Activity and Contractor.

C.2.4.3 Portability

C.2.4.3.1 The Contractor shall have the capability to redeploy COMSATCOM services, subject to availability. Portability shall be provided within the COMSATCOM Contractor’s resources at any time as requested by the Ordering Activity. When portability is exercised, evidence of equivalent net present value (NPV[1]) shall be provided by the Contractor. Alternatively, prior to Task Order award, specific pre-defined terms and conditions for portability and related services including pricing and/or other contract terms may be negotiated and defined in the individual Task Order. Portability may include moving from one transponder/satellite to another, one managed service area to another, transponded capacity redeployment between beams or transponders on a single satellite, redeployment from one frequency band to another, physical

[1] For example, one-year of service for a transponder valued at $1M/year is traded for six-months of service on a transponder valued at $2M/year.

relocation of a satellite to a new orbital position, re-routing of teleport services from one teleport to another pre-defined teleport, re-routing of traffic from one terrestrial infrastructure to another pre-defined infrastructure, and movement of Network Operations Center (NOC) services from one NOC to another NOC.

C.2.4.4 Flexibility/Optimization

C.2.4.4.1 The Contractor shall have the capability to re-groom resources for spectral, operational, or price efficiencies. Flexibility/optimization shall be provided within the COMSATCOM Contractor's resources at any time as requested by the Ordering Activity. When flexibility/optimization is exercised, evidence of equivalent net present value (NPV) [2] shall be provided by the Contractor. The Contractor is encouraged to submit re-grooming approaches for Ordering Activity consideration that may increase efficiencies for existing COMSATCOM services. Alternatively, prior to Task Order award, specific pre-defined terms and conditions for re-grooming including pricing and/or other contract terms may be negotiated and defined in the individual Task Order. Re-grooming may include, but is not limited to, analysis of space segment, teleport, and network resource utilization in order to increase the number of carriers on existing allocated bandwidth and/or terminals and/or increasing the data rates on individual Task Orders through the implementation of advanced coding, modulation, and/or hardware upgrades.

C.2.4.5 Capacity

C.2.4.5.1 The Government has requirements for scalable COMSATCOM capacity in any COMSATCOM frequency band. The Contractor must be able to provide scalable capacity in any available COMSATCOM frequency band in support of US Government COMSATCOM requirements. This requirement is subject to the availability of satellite resources.

C.2.4.6 Coverage

C.2.4.6.1 The Government has requirements for COMSATCOM coverage anywhere in the world and in any COMSATCOM frequency band. The Contractor must be able to provide coverage anywhere worldwide in any available COMSATCOM frequency band, including, but not limited to, L-, S-, C-, X-, Ku-, extended Ku-, Ka-, and UHF. Specific pre-defined coverage may be negotiated and

[2] For example, one-year of service on a less efficient arrangement of contractor resources is traded for nine-months of services on a more efficient arrangement of contractor resources that provides an operational efficiency to the Ordering Activity's customers.

defined in the individual Task Order. This requirement is subject to the availability of satellite resources.

C.2.4.7 Network Monitoring (NET OPS)

C.2.4.7.1 The Contractor shall have the capability to electronically collect and deliver near real-time monitoring, fault/incident/outage reporting, and information access to ensure effective and efficient operations, performance, and availability, consistent with commercial practices. Consistent with the Contractor's standard management practices, the Net Ops information will be provided on a frequency (example: every 6 hours, daily) and format (example: SNMP, XML) as defined in a requirement to a location/entity/electronic interface defined by the Ordering Activity. Prior to Task Order award, specific pre-defined terms and conditions for Net Ops collection and delivery may be negotiated and defined in the individual Task Order.

C.2.4.8 EMI/RFI Identification, Characterization, and Geo-Location

C.2.4.8.1 The Contractor shall have the capability to collect and electronically report in near real-time Electro Magnetic Interference (EMI) / Radio Frequency Interference (RFI) identification, characterization, and geo-location, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI. The Contractor shall establish and use with the Ordering Activity a mutually agreed upon media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

C.2.4.9 Security

C.2.4.9.1 The Contractor may be required to obtain/possess varying levels of personnel and facility security clearances up to U.S. Government TOP SECRET/Sensitive Compartmented Information (TS/SCI) or equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally.

C.2.4.9.2 The Contractor may be required to provide physical security (e.g., personnel or equipment protection).

C.2.4.9.3 For incident resolution involving classified matters, the Contractor shall provide appropriately cleared staff who can affect COMSATCOM services operations (example: satellite payload operations, network operations). The Contractor shall provide a minimum of one operations staff member AND a minimum of one person with the authority to commit the company if resolution requires business impacting decisions (example: Chief Executive Officer, Chief Operations Officer, etc.).

C.2.4.9.4 When Communications Security or Transmission Security equipment or keying material is placed in the equipment/terminal shelter, the Contractor shall ensure compliance with applicable physical security directives/guidelines and that all deployed equipment/terminal operations and maintenance personnel shall possess the appropriate clearances, equal to or higher than the classification level of the data being transmitted. Where local regulations require use of foreign personnel for terminal operations and maintenance, then the Contractor shall ensure compliance with applicable security directives/guidelines and document to the U.S. Government's satisfaction that protective measures are in place and such individuals have equivalent clearances granted by the local host nation.

C.2.4.9.5 For classified operations security (OPSEC), the Contractor shall ensure that all personnel in direct contact with classified OPSEC indicators (example: the unit, location, and time of operations) have U.S. SECRET or higher personnel security clearances, or, as appropriate, equivalent clearances assigned by the National Security Authority of a NATO Member State or Major Non-NATO Ally, in accordance with applicable security directives and guidelines.

C.2.4.9.6 For classified requirements, cleared satellite operator staff must have access to secure voice communications for emergency purposes. Communications security equipment certified by the National Security Agency (NSA) to secure unclassified and up to and including SECRET communication transmissions at all operations centers is preferred. If a Contractor is unable to have access to NSA-approved communications security equipment at its operations centers, then a combination of a "Sensitive but Unclassified" (SBU) cryptographic module approved by the U.S. National Institute for Standards and Technology and pre-arranged access to NSA-approved communications security equipment at an agreed alternate facility is acceptable.

C.2.4.9.7 The Contractor shall have the capability to "mask" or "protect" users against unauthorized release of identifying information to any entity that could compromise operations security. Identifying information includes but is not limited to personal user and/or unit information including tail numbers, unit names, unit numbers, individual names, individual contact numbers, street addresses, etc.

C.2.4.10 Net Ready (Interoperability)

The Contractor shall deliver solutions that are consistent with commercial standards and practices. Contractor solutions shall have the capability to access and/or interoperate with Government or other Commercial teleports/gateways and provide enterprise service access to or among networks or enclaves. Interfaces may be identified as interoperable on the basis of participation in a sponsored interoperability program. Any such access and/or interoperability with teleports/gateways and provisioning of enterprise service access will be defined in the individual Task Order requirement.

(END OF SECTION C)

SECTION D
PACKAGING AND MARKING

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING

Preservation, packaging, packing and marking of all deliverables must conform to normal commercial packing standards to assure safe delivery at destination.
Where special or unusual packing is specified in an order, but not specifically provided for by the contract, such packing details must be the subject of an agreement independently arrived at between the Ordering Agency and the Contractor.

D.2 UNCLASSIFIED AND CLASSIFIED MARKING

Unclassified data shall be prepared for shipment in accordance with requirements set forth in the Order, or if none is specified, pursuant to industry standards.

Classified reports, data, and documentation shall be prepared for shipment in accordance with requirements set forth in the Order, or if none is specified, pursuant to the National Industrial Security Program Operating Manual (NISPOM), DOD 5220.22-M.

D.3 PACKING, MARKING, AND STORAGE OF EQUIPMENT

All packing, marking and storage incidental to shipping of equipment to be provided under this contract shall be made at the Contractor’s expense. Such packing, supervision marking and storage costs shall not be billed to the Government. Supervision of packing and unpacking of equipment shall be furnished by the Contractor.

(END OF SECTION D)

SECTION E
INSPECTION AND ACCEPTANCE

E.1 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 address: https://www.acquisition.gov/far/

(End of Clause)

E.2 FEDERAL ACQUISITION REGULATION (FAR) CLAUSES APPLICABLE AT THE ORDER LEVEL

The following clauses apply at the Order level, as applicable:

E.2.1 52.246-4 Inspection of Services—Fixed-Price (AUG 1996)

E.2.2 52.246-16 Responsibility for Supplies (APR 1984)

(END OF SECTION E)

SECTION F
DELIVERIES OR PERFORMANCE

F.1 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 address: https://www.acquisition.gov/far/

(End of Clause)

F.1.1	**52.242-15**	**Stop-Work Order (AUG 1989)**
F.1.2	**52.242-17**	**Government Delay of Work (APR 1984)**
F.1.3	**52.247-34**	**F.o.b. Destination (NOV 1991)**

F.2 FEDERAL ACQUISITION REGULATION (FAR) CLAUSES APPLICABLE AT THE ORDER LEVEL

The following clauses apply at the Order level, as applicable, subject to specific delivery and performance requirements as set forth in the Order:

F.2.1	**52.211-8**	**Time of Delivery (JUNE 1997)**
F.2.2	**52.211-8**	**Time of Delivery, Alternate I (APR 1984)**
F.2.3	**52.211-8**	**Time of Delivery, Alternate II (APR 1984)**
F.2.4	**52.211-8**	**Time of Delivery, Alternate III (APR 1984)**
F.2.5	**52.211-9**	**Desired and Required Time of Delivery (June 1997)**
F.2.6	**52.211-9**	**Desired and Required Time of Delivery, Alternate I (APR 1984)**
F.2.7	**52.211-9**	**Desired and Required Time of Delivery, Alternate II (APR 1984)**
F.2.8	**52.211-9**	**Desired and Required Time of Delivery, Alternate III (APR 1984)**
F.2.9	**52.211-11**	**Liquidated Damages–Supplies, Services, or Research and Development (SEPT 2000)**
F.2.10	**52.247-35**	**F.o.b. Destination, With Consignee's Premises (APR 1984)**

F.3 TERM OF BASIC CONTRACT

The term of this contract will be 3 years (base period) from the date of award, with two 1-year option periods.

F.4 TASK ORDER PERIOD OF PERFORMANCE

The term for each Order placed under the Basic Contract shall be specified in the individual Order. Under no circumstances may an Order be placed under the Basic Contract if the Basic Contract has expired, or has been terminated or cancelled by the Government. See Sections I.3, I.4, and I.5.

F.5 PLACE OF PERFORMANCE

The place of performance and/or delivery requirements will be specified in each individual Order.

F.6 DELIVERIES

This section identifies the items that the Contractor shall deliver to the Government and/or the Government's agent(s) under the Basic Contract. Individual orders will have additional deliverables specified in each Order. In this section, the items the Contractor delivers are called "deliverables."

The Contractor shall provide the deliverables in the media specified by the Government.

The Contractor shall provide the deliverables in "calendar" days unless otherwise specified. The deliverables include, but are not limited to, the items listed in Table F.6-1. The Government does not waive its right to request deliverables under the Basic Contract, even if such requirements are not specifically listed in this table.

Any inconsistency between Section F and Sections B, C, G, H, shall be resolved by giving Sections B, C, G and/or H precedence.

Table F.6-1 Contractor Deliverables

ID	SECTION	DELIVERABLE TITLE	FREQUENCY	DELIVER TO
1	J-2	Information Assurance Minimum Security Controls Checklist	30 days after award then annually	GSA PCO and PMO

2	G.5.1 G.5.2	Monthly Business Volume (Sales) & Monthly Revenue Reports	Monthly	GSA PMO
3	G.5.3	Annual Program Review Report	Annually	GSA PCO and PMO
4	G.5.4	Subcontracting Reports	See Clause 52.219-9	www.eSRS.gov
5	G.8	Marketing and Promotional Materials	Prior to distribution	GSA PMO
6	H.5	Redacted Contract/ Redacted Modifications	Within 15 calendar days of base contract award and all modifications	GSA PCO

(END OF SECTION F)

SECTION G
CONTRACT ADMINISTRATION

G.1 AUTHORIZED USERS

Only authorized users may place orders under the Basic Contract. In order to qualify as an authorized user, a duly warranted Contracting Officer (as that term is defined in FAR Subpart 2.1) in good standing must have an appropriate signed delegation of procurement authority (DPA) from GSA. For purposes of this Basic Contract, these authorized users are identified as Ordering Contracting Officers (OCOs).

This Basic Contract is for use by all Federal agencies, and others as listed in General Services Administration (GSA) Order ADM 4800.2F, ELIGIBILITY TO USE GSA SOURCES OF SUPPLY AND SERVICES, September 17, 2009, as modified from time to time.

G.2 ROLES AND RESPONSIBILITIES

This section describes the roles and responsibilities of Government personnel after Basic Contract award. The Government may modify the roles and responsibilities at any time during the period of performance of the Basic Contract.

G.2.1 GSA Program Manager (PM)

The Government has appointed a PM, who shall perform various programmatic functions for the overall success of the FCSA program. The PM has no actual, apparent or implied authority to bind the Government for any acts or omissions.

G.2.2 Procuring Contracting Officer (PCO)

The GSA PCO is the sole and exclusive Government Official with actual authority to award the Basic Contract. After award of the Basic Contract, the GSA PCO may delegate any or all of the contract administration functions described in FAR 42.302. The GSA PCO has made the following Administrative Contracting Officer (ACO) designation to perform administration functions described in FAR 42.302 as delegated:

Tracey Embry
GSA FAS/ITS/QTAF
10304 Eaton Place, 2nd Floor
Fairfax, VA 22030
(703) 306-7041
tracey.embry@gsa.gov

G.2.3 Ordering Contracting Officer (OCO)

As described in Section G.1, only an authorized user, who is a delegated OCO, may place and administer an Order under the Basic Contract. A Statement of Work (SOW) or Performance Work Statement (PWS) must be submitted to the GSA PCO and GSA PM for a scope review according to Section G.3.2.

The OCO for each Order is the sole and exclusive Government Official with actual authority to take actions which may bind the Government for that Order. Contractors shall ensure that an OCO has the required DPA. Contractors that accept orders from a Government representative who does not have the authorized DPA do so at their own risk. To ensure the required delegation, Contractors may request a copy of the OCO delegation prior to award of an Order if the Contractor does not have a copy of the OCO delegation.

G.2.4 Contracting Officer's Representative (COR), Contracting Officer's Technical Representative (COTR) and Task Monitor (TM)

The OCO for each Order may designate a COR, COTR or TM to provide certain assistance to the OCO for that Order. The specific rights and responsibilities of the COR, COTR or TM for each Order shall be described in writing, which upon request shall be provided to the Contractor. A COR, COTR or TM has no actual, apparent or implied authority to bind the Government.

G.2.5 Ombudsman

Pursuant to FAR 16.505 (a)(9)(i) no protest is authorized in connection with the issuance or proposed issuance of an order under a task-order contract or delivery-order contract, except for (A) a protest on the grounds that the order increases the scope, period of performance, or maximum value of the contract; or (B) a protest of an order valued in excess of $10 million.

GSA has appointed an Ombudsman to review complaints from Contractors and ensure they are afforded a fair opportunity to be considered. The Ombudsman is a senior GSA official who is independent of the GSA PCO or OCO.

The Ombudsman is:

Task and Delivery Order Ombudsman
Office of the Chief Acquisition Officer
U.S. General Services Administration

1800 F Street, N.W.

Washington, DC 20405

G.3 ORDERING PROCEDURES

G.3.1 Ordering procedures must comply with the following:

G.3.1.1 FAR 16.505;

G.3.1.2 Orders are not exempt from the development of acquisition plans (see FAR Subpart 7.1), and an information technology acquisition strategy; (see FAR Part 39);

G.3.1.3 The OCO shall include the evaluation procedures in Task Order Requests (TORs) and establish the time frame for responding to TORs, giving Offerors a reasonable proposal preparation time while taking into account the unique requirements and circumstances of the effort;

G.3.1.4 Orders shall be within the scope, issued within the period of performance, and be within the maximum value of the Basic Contract;

G.3.1.5 Contractors are required to respond to each TOR with either a proposal or a statement of “No Bid” along with the reason for not submitting a proposal;

G.3.1.6 All costs associated with the preparation, presentation, and discussion of the Offeror’s proposal in response to a TOR will be at the Offeror’s sole and exclusive expense; and

G.3.1.7 All orders placed under the Basic Contract are subject to the terms and conditions of the Basic Contract at time of order award. In the event of any conflict between the Order and the Basic Contract, the Basic Contract will take precedence.

G.3.1.8 Orders placed by OCOs may include required Agency clauses.

G.3.1.9 Orders may be issued by facsimile or by electronic commerce methods.

G.3.2 Statement of Work

A written SOW or PWS will always be used. The OCO will provide the SOW/PWS to the GSA PCO and GSA PM. The GSA PCO will provide a scope determination to the OCO.

Any changes to the SOW/PWS or expansion of the original requirement will require an additional scope review by the GSA PCO.

Scope reviews can be conducted by GSA and completed in parallel with the OCO's Task Order acquisition activities. In Task Orders requiring immediate delivery of service for an urgent requirement, the GSA scope review may be completed after the Task Order is awarded.

G.3.3 Fair Opportunity

OCOs must follow the Fair Opportunity procedures specified in FAR 16.505(b)(1) and the exceptions to Fair Opportunity in FAR 16.505(b)(2). Use of the GSA eBuy system by the OCO will ensure that all Basic contract holders are notified of each Task Order request. Information and instruction on the use of the eBuy system is furnished at www.gsa.gov/ebuy

G.3.4 Order Evaluation

FAR Subpart 15.3 does not apply to the ordering process. Formal evaluation plans or scoring of quotes or offers are not required; however, the OCO must consider price under each Order as one of the factors in the selection decision pursuant to FAR 16.505(b)(1)(ii)(E).

G.3.5 Subcontractors

The Government has not pre-approved any Subcontractors in making awards for the Basic Contract. If a Contractor proposes a Subcontractor for work performed under an Order, the Contractor must comply with FAR 52.244-2 and FAR Subpart 44.2. The Government reserves the right to determine the responsibility of prospective major Subcontractors.

G.4 BILLING AND INVOICING

The Contractor shall submit invoices directly to the address designated by the OCO on the Task Order.

G.4.1 Central Contractor Registration (CCR)

The Contractor shall register in the Central Contractor Registration (CCR) system, which is a central database of data in support of Agency missions, prior to being awarded a contract (FAR 52.204-7). The registration form is at www.ccr.gov and requires the Contractor's Data Universal Numbering System (DUNS) number.

G.4.2 GSA Management Fee

The GSA Management Fee for the CS2 contracts is 2 percent. This 2 percent fee shall be included in all prices. The Contractor shall not invoice for the GSA Management Fee as a separate line item.

The Contractor shall make Electronic Funds Transfer (EFT) arrangements for payment of the GSA management fee. The Contractor shall forward fees collected to the GSA Finance Office by EFT within 30 calendar days of the close of each calendar month for which the fees apply. Failure to pay the fee within 60 calendar days may result in termination of this contract.

G.5 REPORTING REQUIREMENTS

G.5.1 Monthly Business Volume (Sales) Report

The Contractor shall provide monthly sales/business volume reports using the format specified in Section J in Microsoft Excel 2007 format to the GSA Program Manager via e-mail. Business Volume is calculated as the total amount of a Task Order received by the Contractor that period. The reporting period shall be for the beginning through the end of the previous month and reports are due by the 15th calendar day of each month. If there are no orders received during the reporting period, the report is still required and shall state “no ordering activity” for that period.

G.5.1.1 The report shall contain at a minimum the following information:

G.5.1.1.1 **Contractor Name and Contract Number** – Company name and GSA IDIQ Contract Number.

G.5.1.1.2 **Reporting Period** – The monthly reporting period in which orders were received, usually from the 1st of the month through the last day of the month.

G.5.1.1.3 **Title - “CS2 Monthly Business Volume (Sales) Report”**

G.5.1.1.4 **For each Task Order:**

G.5.1.1.4.1 **Date of Task Order** – The date the Task Order is signed.

G.5.1.1.4.2 **Agency Name or Ordering Agency** – Name of the Agency/Organization that issued the Task Order. It also includes the name, address, agency point of contact and telephone number.

G.5.1.1.4.3 **Description of Services** – A brief description of the equipment and/or services.

G.5.1.1.4.4 **Period of Performance** – The actual date the service begins and ends. This should be identified within the Task Order.

G.5.1.1.4.5 **Task Order Number** – The order number assigned by the agency that places the order.

G.5.1.1.4.6 **Total Value (Dollar Amount) of Order Received** – Dollar amount of the Task Order, not including options.

G.5.1.1.5 **Total Sales this Month** – Cumulative total value of Orders for this month.

G.5.1.1.6 **Cumulative Sales to Date** – Cumulative total of all Task Orders since contract award.

The Contractor shall also provide copies of each Task Order received during the reporting period in Microsoft Excel 2007 format to the GSA Program Manager on the 15th calendar day of each month.

G.5.2 Monthly Revenue Report

The Contractor shall provide a monthly revenue report using the format specified in Section J via e-mail in Microsoft Excel 2007 format to the GSA Program Manager on the 15th calendar day of each month. The report shall provide detail relating back to individual Task Orders that have been invoiced and paid by the Ordering Agency.

G.5.2.1 The monthly revenue report shall contain, at a minimum, the following information:

G.5.2.1.1 **Contractor Name and Contract Number** – Company name and GSA IDIQ Contract Number.

G.5.2.1.2 **Reporting Period** – The monthly reporting period in which invoices were received, usually from 1st day of the month through the last day of the month.

G.5.2.1.3 **Title - "CS2 Monthly Revenue Report"**

G.5.2.1.4 **For each Task Order**:

G.5.2.1.4.1 **Date Payment Received** – Date the payment is received by the Contractor from the Ordering Agency. This may be in the form of a check or electronic funds transfer.

G.5.2.1.4.2 **Agency Name / Ordering Activity** – Name of the Agency/Organization that issued the Task Order. It also includes the name, address, agency, point of contact, and telephone number.

G.5.2.1.4.3 **Description of Services** – A brief description of the equipment and/or services.

G.5.2.1.4.4 **Task Order Number** – The order number assigned by the agency that places the order.

G.5.2.1.4.5 **Total Value (Dollar Amount) of Order –** Total dollar amount of the Task Order.

G.5.2.1.4.6 **Amount Received** – Total dollar amount received by the Contractor, from the Agency.

G.5.2.1.4.7 **GSA Management Fee Collected** – This fee is 2 percent of the total amount received in payment by the Agency.

G.5.2.1.4.8 **GSA Management Fee Remitted** – Total dollar amount remitted to GSA for a particular order per month. This number is calculated as a percentage of the total amount received by the Contractor from the Agency.

G.5.2.1.4.9 **Remaining Balance of Un-remitted GSA Management Fee –** This number is calculated as the difference between the total dollar amount due to GSA for a particular order per month and the total amount received by the Contractor from the Agency.

G.5.2.1.5 **EFT Number** – Transaction identification number of EFT and amount. If more than one EFT payment is submitted for the reporting period, the Contractor shall identify all EFT Numbers and Amounts for the reporting period. The total EFT Amount(s) shall total the “GSA Management Fee Remitted” identified on the report.

G.5.3 Annual Program Review Report

The Contractor shall provide an annual program report covering the topics specified below to the GSA PCO and GSA PM via e-mail. The report shall be submitted within 3 business days of the annual program review. See Section G.6.

G.5.3.1 The Annual Program Review Report shall cover the following topics:

G.5.3.1.1 Task Order Performance

G.5.3.1.1.1 Identify all Task Orders in progress and completed in the past year.

G.5.3.1.1.2 Identify the quality of performance for each Task Order and identify any issues and resolution actions/plan.

G.5.3.1.2 Additional Topics as identified by the GSA PCO.

G.5.4 Subcontracting Reports

Contractors submitting small business subcontracting plans must submit periodic reports which show compliance with the subcontracting plan.

The Individual Subcontracting Report (ISR) covers subcontract award data related to this Basic Contract. The Summary Subcontracting Report (SSR) encompasses all Contracts with GSA. The ISR and SSR shall be submitted electronically via the Electronic Subcontract Reporting System (eSRS) at www.esrs.gov

Reports are required when due regardless of whether there has been any subcontracting activity since the inception of the contract or since the previous report. See FAR 52.219-9 Small Business Subcontracting Plan (APR 2008).

G.6 PROGRAM REVIEWS

The Contractor shall attend an annual program review with the GSA Program Office. These reviews may be held at the GSA or Contractor facility. Agenda items may include, but are not limited to: Task Order and Service Level Agreement performance against Task Order metrics, contract status, projected business volume forecast, upcoming opportunities, marketing, conferences, and any other outstanding issues. Program Reviews will be conducted at no additional cost to the Government and reports submitted in accordance with Section G.5.3.

G.7 CONTRACT MANAGEMENT OF PAST PERFORMANCE AFTER AWARD

The Government will evaluate Contractor performance in accordance with the criteria under FAR Subpart 42.15.

Contractors will be required to register in the appropriate past performance assessment systems to review and respond to their surveys as prescribed by the OCO at the Order level.

G.8 MARKETING

Contractors shall develop company specific brochures for distribution at trade shows, conferences, seminars, etc. All marketing and promotional materials, including information on the Contractor webpage, shall be submitted to the GSA Program Office and approved by GSA prior to distribution. Marketing materials may be co-branded with marks owned or licensed by the Contractor and GSA, as long as they comply with GSAM 552.203-71, Restriction on Advertising.

The Contractor is responsible for ongoing sales and marketing during the life of this contract.

G.9 EQUIPMENT REMOVAL

All Contractor-owned equipment, accessories, and devices located on Government property shall be dismantled and removed from Government premises by the Contractor, at the Contractor's expense, within 90 calendar days after the service termination date. All dismantling and removal of equipment shall be performed by the Contractor during normal Government business hours at the location. Advance notice must be provided to the local Government contact to ensure that such dismantling and removal occurs with a minimum of disruption. Exceptions to this requirement shall be mutually agreed upon and written notice issued by the OCO.

G.10 CONTRACT CLOSEOUT

G.10.1 Contract closeout shall be accomplished within the guidelines set forth in:

G.10.1.1 FAR Part 4 Administrative Matters.

G.10.1.2 FAR Part 42 Contract Administration and Audit Services.

G.10.1.3 GSAM Subpart 504.8.

(END OF SECTION G)

SECTION H
SPECIAL CONTRACT REQUIREMENTS

H.1 TYPE AND TERM OF CONTRACT

This is a firm fixed price indefinite delivery, indefinite quantity type contract. All Task Orders issued against this contract will be Firm Fixed Price.

The term of this contract will be 3 years (base period) from the date of award, with two 1-year option periods. The total term of the contract will not exceed 5 years.

H.2 AUTHORIZED USERS

This Basic Contract is for use by all Federal agencies, and others as listed in General Services Administration (GSA) Order ADM 4800.2F, ELIGIBILITY TO USE GSA SOURCES OF SUPPLY AND SERVICES, September 17, 2009, as modified from time to time.

H.3 MINIMUM REVENUE GUARANTEE

The minimum revenue guarantee (MRG) amount for each award will be $1,000.

H.4 MAXIMUM CONTRACT VALUE

The total maximum contract value is $2.6 Billion.

H.5 ELECTRONIC ACCESS TO CONTRACT VIA INTERNET

The Contractor is hereby advised that a redacted version of the contract and all modifications shall be made available on the Internet. Within 15 calendar days of the base award and all modifications, the Contractor shall provide the proposed redacted contract to the GSA PCO for approval. The Contractor shall prepare the proposed redacted version in accordance with Freedom of Information Act guidance. After receiving approval from the GSA PCO, the Contractor shall post the redacted contract to its public web site. As necessary, and upon approval of the GSA PCO, the Contractor shall correct and repost redactions at no additional cost to the Government.

The redacted version of the contract shall include current contract period pricing.

H.6 NEWS RELEASES

News releases pertaining to this contract shall not be made without prior written approval of the GSA PCO. Five business days notice is required for approval.

H.7 U.S. CITIZENSHIP REQUIREMENTS

Contractors are hereby placed on notice that work on some orders, especially those requiring site visits to some U.S. Government locations or work on some Government Furnished Property, may require Contractor personnel performing the work to have U.S. citizenship and to be able to provide proof of that citizenship. This shall be provided at no additional cost to the Government.

H.8 CONFIDENTIALITY

In providing information in response to Task Orders or other Government requests for information, the Contractor may wish to claim confidentiality status for information submitted on the basis that it is a trade secret, or that it is confidential commercial or financial information. To claim confidentiality status, the Contractor must include the following statement on the title page of its proposal or other information submitted:

"The data included in this proposal shall not be disclosed outside the Government or duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate the information; provided that if a Contract is awarded to the Offeror as a result of or in connection with the submission of the data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the contract. This restriction does not limit the Government's right to use information contained in such data if it is obtained from another source without restrictions. The data subject to the restriction is contained in sheets marked with the following legend:

Use or disclosure of data contained on this page is subject to the restriction on the title page of this document."

H.9 CONTRACT MODIFICATIONS AND NEW OR IMPROVED SERVICES

Within scope changes to the contract may be proposed at any time by the Contractor or the Government. Based on Government needs, market research, industry trends, or discussions with Contractors, GSA may incorporate new or enhanced services to the contract throughout its life, provided such modifications are within the scope of the contract. Under such circumstances, GSA will issue a request for proposal stating what the Government's needs are and the Contractor will be encouraged to respond.

The Contractor at any time during the life of the contract may also submit proposals for new services or enhanced services within the scope of the contract, and the GSA PCO will consider those proposals.

H.10 SECTION 508 COMPLIANCE

The Contractor shall ensure that any Electronic and Information Technology (EIT) procured at the Task Order level shall meet the applicable accessibility standards at 36 CFR 1194, if applicable. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended. This standard is viewable at www.section508.gov.

H.11 GOVERNMENT PROPERTY

Any equipment, property, or facilities furnished by the Government or any Contractor-acquired property must be specified on individual Task Orders and follow the policies and procedures of FAR Part 45 for providing Government property to Contractors, Contractors' use and management of Government property, and reporting, redistributing, and disposing of Contractor inventory.

H.12 INCORPORATION OF SUBCONTRACTING PLAN

The Individual Small Business Subcontracting Plan, dated June 7, 2012, and submitted in accordance with FAR 52.219-9, is hereby approved and incorporated herein.

H.13 LIABILITY

The Basic Contract strictly prohibits the use of lease-like payment arrangements, which purport to permit the Government to receive delivery of items and then pay for the full cost of the items over time, even if such arrangements are not technically a lease transaction because the Government is not the lessee.

H.14 ORGANIZATIONAL CONFLICT OF INTEREST

The guidelines and procedures of FAR Subpart 9.5 will be used in identifying and resolving any issues of organizational conflict of interest at the Task Order level.

In the event that a Task Order requires activity that would create an actual or potential conflict of interest, the Contractor shall:

(a) Notify the OCO of the actual or potential conflict, and not commence work on any Task Order that involves a potential or actual conflict of interest until specifically notified by the OCO to proceed;

(b) Identify the conflict and recommend to the OCO an alternate tasking approach which would avoid the conflict;

If the OCO determines that it is in the best interest of the Government to issue the Task Order, notwithstanding a conflict of interest, a request for waiver shall be submitted in accordance with FAR Section 9.503.

(END OF SECTION H)

SECTION I
CONTRACT CLAUSES

I.1 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 these addresses:

FEDERAL ACQUIISITION REGULATION:
https://www.acquisition.gov/far/

GENERAL SERVICE ADMINISTRATION ACQUISITION MANUAL:
http://www.acquisition.gov/GSAM/gsam.html

(End of Clause)

RFP Section	FAR Clause No.	Title and Date
I.1.1	52.202-1	Definitions (JAN 2012)
I.1.2	52.203-3	Gratuities (APR 1984)
I.1.3	52.203-5	Covenant Against Contingent Fees (APR1984)
I.1.4	52.203-6	Restrictions on Subcontractor Sales to the Government (SEP 2006)
I.1.5	52.203-7	Anti-Kickback Procedures (OCT 2010)
I.1.6	52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity (JAN 1997)
I.1.7	52.203-10	Price or Fee Adjustment for Illegal or Improper Activity (JAN 1997)
I.1.8	52.203-12	Limitation on Payments to Influence Certain Federal Transactions (OCT 2010)
I.1.9	52.203-13	Contractor Code of Business Ethics and Conduct (APR 2010)
I.1.10	52.204-2	Security Requirements (AUG 1996)

I.1.11	52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper (MAY 2010)
I.1.12	52.204-7	Central Contractor Registration (FEB 2012)
I.1.13	52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards (FEB 2012)
I.1.14	52.209-6	Protecting the Government's Interest when Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (DEC 2010)
I.1.15	52.209.10	Prohibition on Contracting with Inverted Domestic Corporations (May 2012)
I.1.16	52.211-5	Material Requirements (AUG 2000)
I.1.17	52.215-2	Audit and Records - Negotiation (OCT 2010)
I.1.18	52.215-8	Order of Precedence - Uniform Contract Format (OCT 1997)
I.1.19	52.215-10	Price Reduction for Defective Cost or Pricing Data (AUG 2010)
I.1.20	52.215-11	Price Reduction for Defective Cost or Pricing Data - Modifications (AUG 2011)
I.1.21	52.215-12	Subcontractor Cost or Pricing Data (OCT 2010)
I.1.22	52.215-13	Subcontractor Cost or Pricing Data - Modifications (OCT 2010)
I.1.23	52.215-14	Integrity of Unit Prices (OCT 2010)
I.1.24	52.215-17	Waiver of Facilities Capital Cost of Money (OCT 1997)
I.1.25	52.217-2	Cancellation Under Multiyear Contracts (OCT 1997)

I.1.26	52.219-8	Utilization of Small Business Concerns (JAN 2011)
I.1.27	52.219-9	Small Business Subcontracting Plan (JAN 2011)
I.1.28	52.219-16	Liquidated Damages - Subcontracting Plan (JAN 1999)
I.1.29	52.222-1	Notice to the Government of Labor Disputes (FEB 1997)
I.1.30	52.222-3	Convict Labor (JUN 2003)
I.1.31	52.222-21	Prohibition of Segregated Facilities (FEB 1999)
I.1.32	52.222-26	Equal Opportunity (MAR 2007)
I.1.33	52.222-29	Notification of Visa Denial (JUNE 2003)
I.1.34	52.222-35	Equal Opportunity for Veterans (SEP 2010)
I.1.35	52.222-36	Affirmative Action for Workers with Disabilities (OCT 2010)
I.1.36	52.222-37	Employment Reports for Veterans (SEP 2010)
I.1.37	52.222-43	Fair Labor Standards Act and Service Contract Act—Price Adjustment (Multiple Year and Option Contracts) (SEP 2009)
I.1.38	52.222-50	Combating Trafficking in Persons (FEB 2009)
I.1.39	52.222-54	Employment Eligibility Verification (JUL 2012)
I.1.40	52.223-5	Pollution Prevention and Right-to-Know Information (MAY 2011)
I.1.41	52.223-6	Drug-Free Workplace (MAY 2001)
I.1.42	52.223-14	Toxic Chemical Release Reporting (AUG 2003)
I.1.43	52.224-1	Privacy Act Notification (APR 1984)

I.1.44	52.224-2	Privacy Act (APR 1984)
I.1.45	52.225-1	Buy American Act – Supplies (FEB 2009)
I.1.46	52.225-13	Restrictions on Certain Foreign Purchases (JUNE 2008)
I.1.47	52.227-1	Authorization and Consent (DEC 2007)
I.1.48	52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement (DEC 2007)
I.1.49	52.227-3	Patent Indemnity (APR 1984)
I.1.50	52.227-10	Filing of Patent Applications – Classified Subject Matter (DEC 2007)
I.1.51	52.227-14	Rights in Data - General (DEC 2007)
I.1.52	52.228-5	Insurance - Work on a Government Installation (JAN 1997)
I.1.53	52.229-3	Federal, State, and Local Taxes (APR 2003)
I.1.54	52.229-6	Taxes - Foreign Fixed-Price Contracts (JUN 2003)
I.1.55	52.232-1	Payments (APR 1984)
I.1.56	52.232-8	Discounts for Prompt Payment (FEB 2002)
I.1.57	52.232-11	Extras (APR 1984)
I.1.58	52.232-17	Interest (OCT 2010)
I.1.59	52.232-23	Assignment of Claims (JAN 1986)
I.1.60	52.232-25	Prompt Payment (OCT 2008)
I.1.61	52.232-33	Payment by Electronic Funds Transfer-Central Contract or Registration (OCT 2003)
I.1.62	52.232-37	Multiple Payment Arrangements (MAY 1999)
I.1.63	52.233-1	Disputes (JUL 2002), Alternate I (DEC 1991)

I.1.64	52.233-3	Protest After Award (AUG 1996)
I.1.65	52.233-4	Applicable Law for Breach of Contract Claim (OCT 2004)
I.1.66	52.237-2	Protection of Government Buildings, Equipment, and Vegetation (APR 1984)
I.1.67	52.237-3	Continuity of Services (JAN 1991)
I.1.68	52.239-1	Privacy or Security Safeguards (AUG 1996)
I.1.69	52.242-13	Bankruptcy (JUL 1995)
I.1.70	52.243-1	Changes - Fixed Price (AUG 1987), Alternate II (APR 1984)
I.1.71	52.244-2	Subcontracts (OCT 2010)
I.1.72	52.244-6	Subcontracts for Commercial Items (DEC 2010)
I.1.73	52.246-25	Limitation of Liability - Services (FEB 1997)
I.1.74	52.249-2	Termination for Convenience of the Government (Fixed-Price) (APR 2012)
I.1.75	52.249-8	Default (Fixed-Price Supply and Service) (APR 1984)
I.1.76	52.253-1	Computer Generated Forms (JAN 1991)

I.2 52.209-9 UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS (FEB 2012)

(a) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of the contract, by posting the required information in the Central Contractor Registration database via https://www.acquisition.gov.

(b) As required by section 3010 of the Supplemental Appropriations Act, 2010 (Pub. L. 111-212), all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available. FAPIIS consists of two segments—

(1) The non-public segment, into which Government officials and the Contractor post information, which can only be viewed by—

(i) Government personnel and authorized users performing business on behalf of the Government; or

(ii) The Contractor, when viewing data on itself; and

(2) The publicly-available segment, to which all data in the non-public segment of FAPIIS is automatically transferred after a waiting period of 14 calendar days, except for—

(i) Past performance reviews required by subpart 42.15;

(ii) Information that was entered prior to April 15, 2011; or

(iii) Information that is withdrawn during the 14-calendar-day waiting period by the Government official who posted it in accordance with paragraph (c)(1) of this clause.

(c) The Contractor will receive notification when the Government posts new information to the Contractor's record.

(1) If the Contractor asserts in writing within 7 calendar days, to the Government official who posted the information, that some of the information posted to the non-public segment of FAPIIS is covered by a disclosure exemption under the Freedom of Information Act, the Government official who posted the information must within 7 calendar days remove the posting from FAPIIS and resolve the issue in accordance with agency Freedom of Information procedures, prior to reposting the releasable information. The contractor must cite 52.209-9 and request removal within 7 calendar days of the posting to FAPIIS.

(2) The Contractor will also have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, i.e., for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.

(3) As required by section 3010 of Pub. L. 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

(d) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.

(End of clause)

I.3 52.215-19 NOTIFICATION OF OWNERSHIP CHANGES (OCT 1997)

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the Administrative Contracting Officer (ACO) within 30 days.

(2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall —

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

(End of Clause)

I.4 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 date of award through the life of this contract.

(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)

I.5 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 $50 for the first three years and $100 for each option year of the contract, 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 the following:

(1) Any order for a single item in excess of $10,000,000 in annual value;

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

(3) A series of orders from the same ordering office within 0 days that together call for quantities exceeding the limitation in subparagraph (b) (1) or (2) above.

(c) Notwithstanding paragraph (b) 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 five 5 working days after issuance, with written notice stating the Contractor's intent not to supply 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)

I.6 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 contract. The quantities of supplies and services specified in the contract 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 contract up to and including the quantity designated in the contract as the "maximum." The Government is responsible only for the minimum dollar guarantee designated in the contract.

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

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; *provided*, that the Contractor shall not be required to make any deliveries under this contract after 12 months after the expiration of this contract.

(End of Clause)

I.7 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 period of performance end date.

(End of Clause)

I.8 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of the expiration of the contract; 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)

I.9 52.222-40 NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEC 2010)

(a) During the term of this contract, the Contractor shall post an employee notice, of such size and in such form, and containing such content as prescribed by the Secretary of Labor, in conspicuous places in and about its plants and offices where employees covered by the National Labor Relations Act engage in activities relating to the performance of the contract, including all places where notices to employees are customarily posted both physically and electronically, in the languages employees speak, in accordance with 29 CFR 471.2 (d) and (f).

(1) Physical posting of the employee notice shall be in conspicuous places in and about the Contractor's plants and offices so that the notice is prominent and readily seen by employees who are covered by the National Labor Relations Act and engage in activities related to the performance of the contract.

(2) If the Contractor customarily posts notices to employees electronically, then the Contractor shall also post the required notice electronically by displaying prominently, on any website that is maintained by the Contractor and is customarily used for notices to employees about terms and conditions of employment, a link to the Department of Labor's website that contains the full text of the poster. The link to the Department's website, as referenced in (b)(3) of this section, must read, "Important Notice about Employee Rights to Organize and Bargain Collectively with Their Employers."

(b) This required employee notice, printed by the Department of Labor, may be—

(1) Obtained from the Division of Interpretations and Standards, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, NW., Room N-5609, Washington, DC 20210, (202) 693-0123, or from any field office of the Office of Labor–Management Standards or Office of Federal Contract Compliance Programs;

(2) Provided by the Federal contracting agency if requested;

(3) Downloaded from the Office of Labor–Management Standards Web site at www.dol.gov/olms/regs/compliance/EO13496.htm; or

(4) Reproduced and used as exact duplicate copies of the Department of Labor's official poster.

(c) The required text of the employee notice referred to in this clause is located at Appendix A, Subpart A, 29 CFR Part 471.

(d) The Contractor shall comply with all provisions of the employee notice and related rules, regulations, and orders of the Secretary of Labor.

(e) In the event that the Contractor does not comply with the requirements set forth in paragraphs (a) through (d) of this clause, this contract may be terminated or suspended in whole or in part, and the Contractor may be suspended or debarred in accordance with 29 CFR 471.14 and subpart 9.4. Such other sanctions or remedies may be imposed as are provided by 29 CFR part 471, which implements Executive Order 13496 or as otherwise provided by law.

(f) Subcontracts.

(1) The Contractor shall include the substance of this clause, including this paragraph (f), in every subcontract that exceeds $10,000 and will be performed wholly or partially in the United States, unless exempted by the rules, regulations, or orders of the Secretary of Labor issued pursuant to section 3 of Executive Order 13496 of January 30, 2009, so that such provisions will be binding upon each subcontractor.

(2) The Contractor shall not procure supplies or services in a way designed to avoid the applicability of Executive Order 13496 or this clause.

(3) The Contractor shall take such action with respect to any such subcontract as may be directed by the Secretary of Labor as a means of enforcing such provisions, including the imposition of sanctions for noncompliance.

(4) However, if the Contractor becomes involved in litigation with a subcontractor, or is threatened with such involvement, as a result of such direction, the Contractor may request the United States, through the Secretary of Labor, to enter into such litigation to protect the interests of the United States.

(End of clause)

I.10 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES

I.10.1 552.203-71 RESTRICTION ON ADVERTISING (SEP 1999)

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the White House, the Executive Office of the President, or any other element of the Federal Government, or is considered by these entities to be superior to other products or services. Any advertisement by the Contractor, including price-off coupons, that refers to a military resale activity shall contain the following statement: “This advertisement is neither paid for nor sponsored, in whole or in part, by any element of the United States Government.”

(End of Clause)

I.10.2 552.215-70 EXAMINATION OF RECORDS BY GSA (FEB 1996)

The Contractor agrees that the Administrator of General Services or any duly authorized representatives shall, until the expiration of 3 years after final payment under this contract, or of the time periods for the particular records specified in Subpart 4.7 of the Federal Acquisition Regulation (48 CFR 4.7), whichever expires earlier, have access to and the right to examine any books, documents, papers, and records of the Contractor involving transactions related to this contract or compliance with any clauses thereunder. The Contractor further agrees to include in all its subcontracts hereunder a provision to the effect that the Subcontractor agrees that the Administrator of General Services or any authorized representatives shall, until the expiration of 3 years after final payment under the subcontract, or of the time periods for the particular records specified in Subpart 4.7 of the Federal Acquisition Regulation (48 CFR 4.7), whichever expires earlier, have access to and the right to examine any books, documents, papers, and records of such Subcontractor involving transactions related to the subcontract or compliance with any clauses thereunder. The term “subcontract” as used in this clause excludes (a) purchase orders not exceeding $100,000 and (b) subcontracts or purchase orders for public utility services at rates established for uniform applicability to the general public.

(End of Clause)

I.10.3 552.229-71 FEDERAL EXCISE TAX—DC GOVERNMENT (SEP 1999)

If the District of Columbia cites an Internal Revenue Tax Exempt Certificate Number on orders placed under this contract, the Contractor shall bill shipments to the District of Columbia at prices exclusive of Federal excise tax and show the amount of such tax on the invoice.

(End of Clause)

I.10.4 552.232-23 ASSIGNMENT OF CLAIMS (SEP 1999)

Because this is a requirements or indefinite quantity contract under which more than one agency may place orders, paragraph (a) of the Assignment of Claims clause (FAR 52.232-23) is inapplicable and the following is substituted therefore:

In order to prevent confusion and delay in making payment, the Contractor shall not assign any claim(s) for amounts due or to become due under this contract. However, the Contractor is permitted to assign separately to a bank, trust company, or other financial institution, including any Federal lending agency, under the provisions of the Assignment of Claims Act, as amended, 31 U.S.C. 3727, 41 U.S.C. 15 (hereinafter referred to as "the Act"), all amounts due or to become due under any order amounting to $1,000 or more issued by any Government agency under this contract. Any such assignment takes effect only if and when the assignee files written notice of the assignment together with a true copy of the instrument of assignment with the contracting officer issuing the order and the finance office designated in the order to make payment. Unless otherwise stated in the order, payments to an assignee of any amounts due or to become due under any order assigned may, to the extent specified in the Act, be subject to reduction or set-off.

(End of Clause)

I.10.5 552.232-77 PAYMENT BY GOVERNMENT CHARGE CARD (NOV 2009)

(a) *Definitions*. “Governmentwide commercial purchase card” means a uniquely numbered charge card issued by a Contractor under the GSA SmartPay® program contract for Fleet, Travel, and Purchase Card Services to named individual Government employees or entities to pay for official Government purchases.

“Oral order” means an order placed orally either in person or by telephone.

(b) At the option of the Government and if agreeable to the Contractor, payments of $100,000 or less for oral or written orders may be made using the Governmentwide commercial purchase card.

(c) The Contractor shall not process a transaction for payment using the charge card until the purchased supplies have been shipped or services performed. Unless the cardholder requests correction or replacement of a defective or faulty item under other contract requirements, the Contractor must immediately credit a cardholder’s account for items returned as defective or faulty.

(d) Payments made using the Governmentwide commercial purchase card are not eligible for any negotiated prompt payment discount. Payment made using a Government debit card will receive the applicable prompt payment discount.

(End of Clause)

I.10.6 552.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (SEP 1999)

(a) *Deviations to FAR clauses*.

(1) This solicitation or contract indicates any authorized deviation to a Federal Acquisition Regulation (48 CFR Chapter 1) clause by the addition of “(DEVIATION)” after the date of the clause, if the clause is not published in the General Services Administration Acquisition Regulation (48 CFR Chapter 5).

(2) This solicitation indicates any authorized deviation to a Federal Acquisition Regulation (FAR) clause that is published in the General Services Administration Acquisition Regulation by the addition of “(DEVIATION (FAR clause no.))” after the date of the clause.

(b) *Deviations to GSAR clauses*. This solicitation indicates any authorized deviation to a General Services Administration Acquisition Regulation clause by the addition of "(DEVIATION)" after the date of the clause.

(c) *"Substantially the same as" clauses*. Changes in wording of clauses prescribed for use on a "substantially the same as" basis are not considered deviations.

(End of Clause)

I.11 FEDERAL ACQUISITION REGULATION (FAR) CLAUSES APPLICABLE AT THE ORDER LEVEL

The following clauses apply at the Order level, as applicable:

RFP Section	FAR Clause No.	Title and Date
I.11.1	52.222-41	Service Contract Act of 1965 (NOV 2007)
I.11.2	52.223-2	Affirmative Procurement of Biobased Products Under Service and Construction Contracts (JUL 2012)
I.11.3	52.223-3	Hazardous Material Identification and Material Safety Data (JAN 1997)
I.11.4	52.223-3	Hazardous Material Identification and Material Safety Data (JAN 1997), Alternate I (July 1995)
I.11.5	52.223-10	Waste Reduction Program (MAY 2011)
I.11.6	52.223-12	Refrigeration Equipment and Air Conditioners (MAY 1995)
I.11.7	52.223-15	Energy Efficiency in Energy-Consuming Products (DEC 2007)
I.11.8	52.223-16	IEEE 1680 Standard for the Environmental Assessment of Personal Computer Products (DEC 2007)
I.11.9	52.223-17	Affirmative Procurement of EPA-designated Items in Service and Construction Contracts (MAY 2008)

I.11.10 52.222-42 STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES (MAY 1989)

In compliance with the Service Contract Act of 1965, as amended, and the regulations of the Secretary of Labor (29 CFR Part 4), this clause identifies the classes of service employees expected to be employed under the contract and states the wages and fringe benefits payable to each if they were employed by the contracting agency subject to the provisions of 5 U.S.C. 5341 or 5332.

This Statement is for Information Only:
It is not a Wage Determination

Employee Class Monetary Wage—Fringe Benefits

______________ ______________________________

______________ ______________________________

______________ ______________________________

______________ ______________________________

(End of Clause)

I.11.11 52.223-7 NOTICE OF RADIOACTIVE MATERIALS (JAN 1997)

a) The Contractor shall notify the Contracting Officer or designee, in writing, ______________* days prior to the delivery of, or prior to completion of any servicing required by this contract of, items containing either (1) radioactive material requiring specific licensing under the regulations issued pursuant to the Atomic Energy Act of 1954, as amended, as set forth in Title 10 of the Code of Federal Regulations, in effect on the date of this contract, or (2) other radioactive material not requiring specific licensing in which the specific activity is greater than 0.002 microcuries per gram or the activity per item equals or exceeds 0.01 microcuries. Such notice shall specify the part or parts of the items which contain radioactive materials, a description of the materials, the name and activity of the isotope, the manufacturer of the materials, and any other information known to the Contractor which will put users of the items on notice as to the hazards involved (OMB No. 9000-0107).

* The Contracting Officer shall insert the number of days required in advance of delivery of the item or completion of the servicing to assure that required licenses are obtained and appropriate personnel are notified to institute any necessary safety and health precautions. See FAR 23.601(d).

(b) If there has been no change affecting the quantity of activity, or the characteristics and composition of the radioactive material from deliveries under this contract or prior contracts, the Contractor may request that the Contracting Officer or designee waive the notice requirement in paragraph (a) of this clause. Any such request shall—

(1) Be submitted in writing;

(2) State that the quantity of activity, characteristics, and composition of the radioactive material have not changed; and

(3) Cite the contract number on which the prior notification was submitted and the contracting office to which it was submitted.

(c) All items, parts, or subassemblies which contain radioactive materials in which the specific activity is greater than 0.002 microcuries per gram or activity per item equals or exceeds 0.01 microcuries, and all containers in which such items, parts or subassemblies are delivered to the Government shall be clearly marked and labeled as required by the latest revision of MIL-STD 129 in effect on the date of the contract.

(d) This clause, including this paragraph (d), shall be inserted in all subcontracts for radioactive materials meeting the criteria in paragraph (a) of this clause.

(End of Clause)

I.11.12 52.223-9 ESTIMATE OF PERCENTAGE OF RECOVERED MATERIAL CONTENT FOR EPA-DESIGNATED ITEMS (MAY 2008)

(a) Definitions. As used in this clause—

“Postconsumer material” means a material or finished product that has served its intended use and has been discarded for disposal or recovery, having completed its life as a consumer item. Postconsumer material is a part of the broader category of “recovered material.”

“Recovered material” means waste materials and by-products recovered or diverted from solid waste, but the term does not include those materials and by-products generated from, and commonly reused within, an original manufacturing process.

(b) The Contractor, on completion of this contract, shall—

(1) Estimate the percentage of the total recovered material content for EPA-designated item(s) delivered and/or used in contract performance, including, if applicable, the percentage of post-consumer material content; and

(2) Submit this estimate to ______________________ [Contracting Officer complete in accordance with agency procedures].

(End of Clause)

I.11.13 52.223-11 OZONE-DEPLETING SUBSTANCES (MAY 2001)

(a) Definition. “Ozone-depleting substance,” as used in this clause, means any substance the Environmental Protection Agency designates in 40 CFR Part 82 as—

(1) Class I, including, but not limited to, chlorofluorocarbons, halons, carbon tetrachloride, and methyl chloroform; or

(2) Class II, including, but not limited to, hydrochlorofluorocarbons.

(b) The Contractor shall label products which contain or are manufactured with ozone-depleting substances in the manner and to the extent required by 42 U.S.C. 7671j (b), (c), and (d) and 40 CFR Part 82, Subpart E, as follows:

Warning

Contains (or manufactured with, if applicable) *_______, a substance(s) which harm(s) public health and environment by destroying ozone in the upper atmosphere.

* The Contractor shall insert the name of the substance(s).

(End of Clause)

(END OF SECTION I)

ATTACHMENT J-1
ACRONYMS AND ABBREVIATIONS

ACO	Administrative Contracting Officer
AF	Air Force
AFRICOM	African Command
ANG	Air National Guard
AOR	Areas of Responsibility
ARNG	Army National Guard
ASD/NII	Assistant Secretary of Defense, Network &Information Integration
BIOT	British Indian Ocean Trust
BPT	Blue Personnel Tracking
BSS	Broadcast Satellite Services
CAMS	Conditional Access Management System
CBA	Cost Benefit Analysis
CCR	Central Contract Registration
CENTCOM	Central Command
CEO	Chief Executive Officer
CIR	Committed Information Rate
CLIN	Contract Line Item Number
CO	Contracting Officer
COO	Chief Operating Officer
COR	Contracting Officer’s Representative
COTR	Contracting Officer’s Technical Representative
CNSSP	Committee on National Security Systems Policy
COMSATCOM	Commercial Satellite Communications
COOP	Continuity of Operations
COTS	Commercial Off The Shelf
CS2	Custom SATCOM Solutions
CTO	Chief Technology Officer
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DLA	Defense Logistics Agency
DLTS	Distance Learning Training System
DOC	Department of Commerce
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DOE	Department of Energy
DOJ	Department of Justice
DPAS	Defense Priorities and Allocation System
DSTS-G	DISN Satellite Transmission Services-Global
DUNS	Data Universal Numbering System
DVB-MPEG 2	Digital Video Broadcast-Moving Pictures Expert Group

DVB-S2-MPEG 4	Digital Video Broadcast-2nd Generation Satellite-Moving Pictures Expert Group
EIT	Electronic and Information Technology
EMI	Electromagnetic Interference
ETF	Electronic Funds Transfer
EUCOM	European Command
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FAS	Federal Acquisition Service
FBI	Federal Bureau of Investigation
FedBizOps	Federal Business Opportunities
FCSA	Future COMSATCOM Services Acquisition
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOC	Full Operational Capability
FOIA	Freedom of Information Act
GETN	Government Education and Training Network
GIG	Global Information Grid
GOTS	Government Off The Shelf
GSA	General Services Administration
GSA PCO	GSA Procuring Contracting Officer
HNA	Host Nation Agreements
IAW	In Accordance With
ID/IQ	Indefinite Delivery/Indefinite Quantity
IGCE	Independent Government Cost Estimates
IOC	Initial Operating Capability
IP	Internet Protocol
IRD	Integrated Receiver Decoder
ISR	Individual Subcontracting Report
IT	Information Technology
LNA	Low-Noise Amplifier
LRDU	Large Remote Deployable Unit
MAC	Mission Assurance Category
MBPS	Megabits Per Second
MCPC	Multiple Channels Per Carrier
MDLS	Modernized Distance Learning System
MRG	Minimum Revenue Guarantee
MWR	Morale, Welfare, and Recreation
MRG	Minimum Revenue Guarantee
NATO	North Atlantic Treaty Organization
NC FCB	Net Centric Functional Capabilities Board
NISPOM	National Industry Security Program Operating Manual
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPV	Net Present Value
NSA	National Security Agency

NTSC	National Television System Committee
O&M	Operations and Maintenance
OCO	Ordering Contracting Officer
ODC	Other Direct Costs
OPSEC	Operations Security
ORDU	Outpost Remote Deployable Unit
OSD	Office of the Secretary of Defense
PACOM	Pacific Command
PCO	Procuring Contracting Officer
PoP	Period of Performance
PM	Program Manager
PMO	Program Management Office
PPIRS	Past Performance Information Retrieval System
PWS	Performance Work Statements
QoS	Quality of Service
RDU	Remote Deployable Unit
RFI	Radio Frequency Interference
RFQ	Request for Quote
RFP	Request for Proposal
SAT Ops	Satellite Operations
SATCOM	Satellite Communications
SBU	Sensitive but Unclassified
SCA	Service Contract Act
SDB	Small Disadvantaged Business
SDVOSB	Service-Disabled Veteran-Owned Small Business
SME	Subject Matter Expert
SIM	Subscriber Identity Module
SIN	Special Item Number
SMS	Scheduling Management System
SNMP	Signaling Network Management Protocol
SOC	Satellite Operations Center
SOW	Statement of Work
SP	Special Publication
SSA	Source Selection Authority
SSAC	Source Selection Advisory Council
SSD	Source Selection Decision
SSEB	Source Selection Evaluation Board
SSP	Source Selection Plan
STO	Sample Task Order
TOR	Task Order Request
TPE	Transponder Equivalent
TS/SCI	TOP SECRET/Sensitive Compartmented Information
TT&C	Telemetry, Tracking, and Commanding
TM	Task Monitor
USFA	U. S. Federal Agency
USF&W	United States Fish and Wildlife

USG	United States Government
USN	United States Navy
VoIP	Voice over Internet Protocol
VOSB	veteran-owned small business
VSAT	Very Small Aperture Terminal
WiFi	Wireless Fidelity (IEEE 802.11)
WOSB	Women-Owned Small Business
XML	eXtensible Markup Language

(END OF ATTACHMENT J-1)

ATTACHMENT J-10
Sample Task Order (STO) #2 - GOVERNMENT EDUCATION AND TRAINING NETWORK (GETN)

1 GETN BACKGROUND

1.1 The Government Education and Training Network (GETN) is a network of Federal Government agencies using a common satellite carrier[1] for interactive standard definition television (1-way video, 2-way audio). The existing Distance Learning Training System (DLTS) for GETN currently supports 12 agencies to provide training to over 2,200 fixed-dish[2] downlink sites located throughout the CONUS, Alaska, Hawaii, Virgin Islands and Puerto Rico. GETN meets a wide variety of training & education needs, supporting these agencies in offering courses in subjects such as contract law, acquisition management, environmental law, hazardous waste management, air pollution, safeguards & security, aircraft maintenance, professional military education, professional continuing education, communication courses, air traffic control, equal opportunity training, medical continuing education, terrorism response, veteran health issues, management, and leadership.

1.2 For the encoding and decoding of satellite signals at their remote classroom sites, two standards are currently in use: Digital Video Broadcast – Moving Picture Experts Group (DVB-MPEG 2) for National Television System Committee (NTSC) output, and DVB-S2-MPEG 4 for Internet Protocol (IP) output[3]. User agencies currently use Scientific Atlanta's PowerVu series of encoders[4] and decoders. Several agencies have already begun migrating their DVB-S1 system to DVB-S2. Video is typically broadcast at a rate of 1.5 Mbps, and data throughput may reach 6 Mbps. Some agencies reduce required bandwidth per channel by using multiple channels per carrier (MCPC) technology. To provide the above capabilities, the current system requires 32MHz of dedicated bandwidth. The audio return path from the remote classrooms to the broadcast studio is currently implemented using a wireline- link, and is satisfied under separate contracts.

1.3 Uplinks are capable of being remotely operated from a central Network Operations Center (NOC) by the service provider. Through a conditional access management system (CAMS), downlinks are capable of remote activation by the same NOC. The NOC provides toll-free help lines for each Federal Government Agency user experiencing technical problems during broadcasts, and the NOC is able to respond immediately to troubleshooting problems during a broadcast.

[1] Ku-band frequency

[2] Sizes range from 1.8m to 2.4m. Dishes are various makes/models configured to receive-only (RO).

[3] IP used for both packetized video and data transport

[4] PowerVu & PowerVu Plus encoders, and IRDs: 9235, 9234, 0934, 9865. The PowerVu Command Center 2000 is being used for management of the GETN system.

1.4 The CAMS includes a provision for the forced tuning of downlinks and receive sites. A downlink may service more than one receive site through the use of multiple integrated receiver decoders (IRDs) at that downlink. The service provider has the capability to remotely activate and deactivate downlinks to ensure downlink sites receive only the broadcast they are authorized to receive.

1.5 To receive a broadcast, a downlink site is authorized to receive that broadcast by the agency controlling the site. A receive site must receive only the broadcast for which it has been authorized and no other broadcast.

1.6 The CAMS allows for any agency to centrally control the scheduling of its own downlinks as a group and any number of subgroups as needed within 24 hours of broadcast, without penalty. CAMS also allows for on-the-spot addition of sites to any reception group.

1.7 The CAMS is able to group for reception any number of specified downlinks from any number of agencies to receive programming from one or more uplinks in the GETN community.

1.8 Additionally, the capability of the uplink locations to control the downlinks is included in the technical solution. This allows uplink locations to activate and deactivate receive site IRDs without going through the NOC.

1.9 The existing service provider is able to operate and conduct remote diagnostics on the satellite uplink equipment. Uplinks are controlled from the central Network Operations Center (NOC) to include forced tuning of downlink receive sites. The NOC has the capability of ensuring that downlink sites receive only the broadcast they are authorized to receive. Government users are provided a centralized capability that is accessible through the Internet to schedule bandwidth.

2 GETN REQUIREMENTS

2.1 A requirement exists for the Contractor to provide a continuing training capability for the existing GETN organization. Starting with the current system capabilities as a baseline, it is required that the Contractor develop, install, and maintain a satellite-based Modernized Distance Learning System (MDLS). Each Federal Agency currently has one or more broadcast studios with an installed set of equipment, and each studio has the capability of producing multiple broadcasts at any time. Instructors must have the ability to transmit video and audio of live courses to the remote sites and receive audio from remote sites (currently, the return audio is received by wireline services under various contracts). Although each agency typically conducts courses internally, the system shall also support the capability of any agency to provide broadcasts to any number of sites belonging to other GETN user agencies. The Contractor shall provide a home channel 24 x 7 that will be viewed by all GETN downlink receive sites when not viewing agency broadcasts.

2.2 Performance will take place at the Contractor's facilities (CONUS), Government facilities within CONUS including Alaska, Hawaii, Puerto Rico and Virgin Islands. The base period of performance shall be for three (3) years with two one (1) year option periods for a possible total period of performance of 5 years.

2.3 This effort shall require a solution to requirements as part of the following documentation:

<u>Service Plan</u> - A Service Plan, in accordance with Section C, is required for this initiative. As part of your plan, provide a description of the Systems, Procedures and Performance Metrics which you propose to put in place to assure successful and timely completion of the Task. Additionally, include a description of the process(es) which you as the Contractor will use to interface with the appropriate Government Representative(s), select/partition work among your subcontractors (as applicable), monitor/control cost and the work of your subcontractors (as applicable) and assure timely/complete submission of Task Order Invoices. Your Service Plan shall address all risks and resultant mitigation plans associated with your MDLS solution.

<u>GETN Communications Infrastructure</u> - Develop and implement the requisite communications infrastructure to support the GETN mission. Identify chosen systems and explain rationale for selection including life cycle cost considerations. Provide a detailed architecture and explain operation and performance of all required interfaces. The Contractor shall provide link budgets, as applicable. A Network Operations Center (NOC) shall be employed to manage connectivity and network assets for the period of performance. The NOC shall provide direct interface and reports to GETN Network Operations staff. The Contractor shall explain what network monitoring and status information will be provided to the Government on a recurring basis, how often it will be provided, and in what format. The Contractor's solution shall address reliability, availability, maintainability, and security.

2.4 The GETN Communications Infrastructure shall incorporate the following at a minimum:

<u>Audio and Video Support</u> - Video and audio shall be broadcast over satellite from agency uplink broadcast centers to remote downlink receive sites. Using the current return audio solution via wireline as a baseline, capabilities to provide or migrate individual agencies to a 2-way audio over satellite system shall be proposed**.** The Contractor shall clearly identify and provide all equipment and software required to fully implement the proposed capability.

<u>Anticipated Usage Profiles</u> - Anticipated typical usage profiles for organizations supported by GETN are listed in Table J-10.1. Actual usage demands may differ.

Table J-10.1: Anticipated Usage Profiles (Typical Day)

Organization	Anticipated Typical Peak Usage	Anticipated Typical Off-Peak Usage
AF	M-F, 6-18 hours/day	None
ANG	M-F, 3-6 hours/day	Sat/Sun, 6-14 hours/day
ARNG	M-F, 3-6 hours/day	Sat/Sun, 6-14 hours/day
DOJ	M-F, 1-6 hours/day	None
FAA	M-F, 3-8 hours/day	None
USF&W	M-F, 2-5 hours/day	None
NPS	M-F, 4-8 hours/day	None
US Courts	M-F, 1-4 hours/day	None
DLA	M-F, 2-7 hours/day	None
FBI	M-F, 3-12 hours/day	Sat/Sun, 1-4 hours/day
DOE	M-F, 1-8 hours/day	None
USN	M-F, 1-8 hours/day	None

Digital Compression - The Contractor shall explain how the MDLS will employ digital compression to minimize bandwidth usage.

Scheduling Management System (SMS) - The Contractor shall propose a centrally located SMS which is to be used by Federal Agencies to schedule training broadcasts. The SMS shall also incorporate security mechanisms to ensure that only authorized agency representatives can schedule or view a specific training session. The SMS shall allow each Agency to schedule training course broadcasts between 24 hours and 18 months prior to the start of the session. The SMS shall allow each Agency to delete broadcasts at any time. The SMS shall allow each agency to add additional receive sites ad-hoc. When reservations are made, the system shall immediately provide email confirmation to the using agency.

Availability - The MDLS shall have a system availability of at least 99.5%.

Billing System - The Contractor shall provide a billing system that allows direct billing to each Federal Agency for services used.

FISMA Compliance - The Contractor shall demonstrate the ability to comply with the Federal Information Security Management Act (FISMA) of 2002 as implemented by Federal Information Processing Standards Publication 200 (FIPS 200), "*Minimum Security Requirements for Federal Information and Information Systems and Organizations*" for a low impact information system specifically addressing the following controls: AC-17, CP-9 and IR-5. Regarding CP-9, the Agency specification for backups is at least daily incremental and weekly full. The Contractor shall demonstrate the ability comply with Committee on National Security Systems Policy (CNSSP) 12, to the maximum extent practicable. See attachment J-3 for additional details on Information Assurance.

Bandwidth Access - The system shall be designed such that a minimum of 7 courses can be conducted simultaneously during typical peak usage periods and a minimum of 2 courses during typical off-peak usage periods. The Contractor shall assess scheduling algorithm alternatives versus the cost of bandwidth and propose a recommendation covering instances where additional simultaneous sessions are requested (e.g. block or schedule using ad-hoc bandwidth) that maximizes system capabilities while minimizing typical monthly costs.

Site Locations - A file containing the locations of sites and organizational assignments is included as Section J, Attachment J-11. The contractor shall provide a portability plan for relocation of any broadcast uplink and associated downlink receive sites to other teleports or satellites within the current regions, in the event an Agency has the need to relocate.

2.5 Engineering Support - Contractor shall engineer the GETN communications architecture, including capacity planning and preparing and developing designs, plans, and reports. Contractor shall implement configuration management, prepare engineering documents and reference manuals, and provide engineering, installation, configuration and testing services for the GETN communications infrastructure. The Contractor is encouraged to use non-proprietary solutions when possible.

2.6 Sustainment - Contractor shall implement and execute logistics, fielding, training, and O&M support. A phased approach can be considered. The sustainment concept must take into account any existing sustainment capabilities/strategies using both COTS and GOTS. The Contractor shall provide an approach for full lifecycle management.

Integrated Logistics Support - Develop and implement a maintenance and supply concept necessary to insure the order, receipt, delivery and accountability of systems required materials necessary to support delivery of the project within the schedule identified by the Government. Logistics support shall include all hardware/software elements and ancillary items necessary for maintaining an operational schedule. The Contractor shall use available commercial and other materials to the maximum extent possible.

Training – Provide training to downlink managers of newly installed receive sites and to agency uplink engineers for any newly purchased equipment or service.

Operations and Maintenance - Provide qualified technical support for the duration of the task's period of performance. Maintenance support shall include the replacement of defective components, upgrades to include COTS technology insertion, and any software updates, as required. The maximum allowed time to replace defective components from the time it is reported or diagnosed is 24 hours, with critical spare components located onsite. Operations support includes 24/7 NOC support. The Contractor shall address the ability to identify and resolve EMI/RFI issues as the Government places a high priority on training since this impacts operational mission capabilities.

- Migration Plan - The Contractor shall clearly articulate its migration plan for providing encrypted, compressed digital satellite service for the Federal Government. This solution shall clearly outline a detailed migration plan for existing system components to a technologically current solution, including costs and milestones. The Contractor should reference lessons learned when possible.

- Recovery Plan - Provide a recovery plan to describe the process and timeline in the event that the communications path being used by the Contractor suffers any failure that disrupts service to Federal Government users.

2.7 Delivery Schedule - The Contractor shall implement the core architecture and transition at least the Air Force users (see Section J, Attachment J-11) to the MDLS within the standard 30 day delivery schedule. All agencies shall be transitioned within 4 months.

2.8 Priced Line Items: At a minimum, pricing is required for the following line items. The Contractor shall note if certain line items are not separately priced**.** All prices shall be fixed price.

- Commercial satellite communications infrastructure per unit cost. For space segment pricing, proposals shall include monthly recurring pricing (on a per year basis) in 0.5 and 1 MHz increments as applicable.

- Network operations center (NOC) operations cost

- Gateway Site terminal cost

- Remote Site terminals cost per unit

- Engineering Support cost per month

- Sustainment support cost per month

- Travel can be charged as ODC and is not required as part of the STO pricing.

(END OF ATTACHMENT J-10)

GETN Central Classroom Sites

STATE	ZIP CODE	CITY/BASE/ POST	AGENCY	SITE CODE
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.S
GA	31098	Warner Robins	ANG	AG.098.D
NE	68524-1898	Lincoln	ARNG	AN.096.B
DC	20001	Washington	DOJ	DJ.177.B
OK	73169	Oklahoma City	FAA	FA.001.A
VA	22204	Arlington	ARNG	AN.001.B
DC	20020	Washington	NPS	NP.220.A
DC	20004	Washington	USCourts	UC.707.A
GA	31098	Warner Robins	DLA	DA.022.A
VA	22135	Quantico	FBI	FB.001.A
WA	99352	Richland	DOE	DE.001.B
MD	20670	Patuxent River	USN	NY.001.B

GETN Remote Classroom Sites

STATE	ZIP CODE	CITY/BASE/POST	AGENCY	SITE CODE
AK	99702	Eielson AFB	USAF	AF.035.A
AK	99702	Eielson AFB	USAF	AF.035.B
AK	99506	Elmendorf AFB	USAF	AF.037.A
AK	99506	Elmendorf AFB	USAF	AF.037.A
AK	99502	Anchorage	ANG	AG.006.A
AK	99502	Anchorage	ANG	AG.006.A
AK	99502	Anchorage	ANG	AG.006.B
AK	99502	Anchorage	ANG	AG.006.C
AK	99502	Anchorage	ANG	AG.006.D
AK	99702	Eielson AFB	ANG	AG.097.A
AK	99702	Eielson AFB	ANG	AG.097.B
AK	99702	Eielson AFB	ANG	AG.097.C
AK	99702	Eielson AFB	ANG	AG.097.D
AK	99701	Fairbanks	ARNG	AN.004.A
AK	99701	Fairbanks	ARNG	AN.004.B
AK	99801	Juneau	ARNG	AN.006.A
AK	99801	Juneau	ARNG	AN.006.B
AK	99701	Fairbanks	DOJ	DJ.026.A
AK	99513	Anchorage	DOJ	DJ.800.B
AK	99513	Anchorage	FAA	FA.002.A
AK	99513	Anchorage	FAA	FA.002.B
AK	99709	Fairbanks	FAA	FA.092.A
AK	99503	Anchorage	USF&W	FW.007.A
AK	99755	Denali National Park	NPS	NP.065.A
AK	99501	Anchorage	NPS	NP.083.A
AK	99501	Anchorage	NPS	NP.083.A
AK	99701	Fairbanks	NPS	NP.169.A
AK	99573	Copper Center	NPS	NP.188.A
AK	99501	Anchorage	USCourts	UC.227.A
AK	99501	Anchorage	USCourts	UC.227.B
AL	36112	Maxwell AFB	USAF	AF.003.A
AL	36112	Maxwell AFB	USAF	AF.003.A
AL	36112	Maxwell AFB	USAF	AF.003.B
AL	36112	Maxwell AFB	USAF	AF.003.C
AL	36112	Maxwell AFB	USAF	AF.003.D
AL	36112	Maxwell AFB	USAF	AF.003.E
AL	36112	Maxwell AFB	USAF	AF.003.F
AL	36112	Maxwell AFB	USAF	AF.003.G
AL	36114	Montgomery	USAF	AF.043.A
AL	36114	Montgomery	USAF	AF.043.B
AL	36112	Maxwell AFB	USAF	AF.099.A
AL	36112	Maxwell AFB	USAF	AF.137.A
AL	36118	Gunter AFB	USAF	AF.143.1
AL	36118	Gunter AFB	USAF	AF.143.A
AL	36112	Maxwell AFB	USAF	AF.AUTV.A
AL	36112	Maxwell AFB	USAF	AF.AUTV.B
AL	36112	Maxwell AFB	USAF	AF.AUTV.C
AL	36108	Montgomery	ANG	AG.004.A
AL	36108	Montgomery	ANG	AG.004.A
AL	36108	Montgomery	ANG	AG.004.B
AL	36108	Montgomery	ANG	AG.004.C
AL	35217	Birmingham	ANG	AG.005.A
AL	35217	Birmingham	ANG	AG.005.B
AL	35217	Birmingham	ANG	AG.005.C
AL	35217	Birmingham	ANG	AG.005.D
AL	36109	Montgomery	ANG	AG.100.A
AL	35904	Gadsden	ANG	AG.210.A
AL	35904	Gadsden	ANG	AG.210.B
AL	36108	Montgomery	ANG	AG.211.A
AL	36108	Montgomery	ANG	AG.211.B
AL	36303	Dothan	ANG	AG.213.A
AL	36303	Dothan	ANG	AG.213.B
AL	36362	Fort Rucker	ARNG	AN.009.A

AL	36362	Fort Rucker	ARNG	AN.009.B
AL	36109	Montgomery	ARNG	AN.700.A
AL	36109	Montgomery	ARNG	AN.700.B
AL	35476	Northport	ARNG	AN.701.A
AL	35476	Northport	ARNG	AN.701.B
AL	36608	Mobile	ARNG	AN.704.A
AL	36608	Mobile	ARNG	AN.704.B
AL	36043	Hope Hull	ARNG	AN.705.A
AL	36043	Hope Hull	ARNG	AN.705.B
AL	35217	Birmingham	ARNG	AN.706.A
AL	35217	Birmingham	ARNG	AN.706.B
AL	35202	Birmingham	ARNG	AN.707.A
AL	35202	Birmingham	ARNG	AN.707.B
AL	36108	Montgomery	ARNG	AN.708.A
AL	36108	Montgomery	ARNG	AN.708.B
AL	36201	Anniston	USA	AY.001.A
AL	35898	Huntsville	USA	AY.015.A
AL	36362	Fort Rucker	USA	AY.045.A
AL	36201	Anniston	DLA	DA.024.A
AL	35801	Huntsville	DOJ	DJ.003.A
AL	36602	Mobile	DOJ	DJ.004.A
AL	36104	Montgomery	DOJ	DJ.005.A
AL	35203	Birmingham	DOJ	DJ.151.A
AL	35242	Vestavia Hills	FAA	FA.065.A
AL	36526	Daphne	USF&W	FW.011.A
AL	36526	Daphne	USF&W	FW.011.A
AL	35601	Decatur	USF&W	FW.021.B
AL	36088	Tuskegee	NPS	NP.183.A
AL	36256	Daviston	NPS	NP.216.A
AL	36104	Montgomery	USCourts	UC.002.A
AL	35203	Birmingham	USCourts	UC.112.A
AL	35203	Birmingham	USCourts	UC.113.A
AL	36201	Anniston	USCourts	UC.114.A
AL	35801	Huntsville	USCourts	UC.115.A
AL	36602	Mobile	USCourts	UC.181.A
AL	36602	Mobile	USCourts	UC.181.B
AL	35601	Decatur	USCourts	UC.342.A
AL	35403	Tuscaloosa	USCourts	UC.343.A
AR	72099	Little Rock AFB	USAF	AF.049.A
AR	72099	Little Rock AFB	USAF	AF.049.B
AR	72099	Little Rock AFB	ANG	AG.009.A
AR	72099	Little Rock AFB	ANG	AG.009.B
AR	72099	Little Rock AFB	ANG	AG.009.C
AR	72099	Little Rock AFB	ANG	AG.009.D
AR	72903	Fort Smith	ANG	AG.010.A
AR	72903	Fort Smith	ANG	AG.010.B
AR	72903	Fort Smith	ANG	AG.010.C
AR	72903	Fort Smith	ANG	AG.010.D
AR	72119	North Little Rock	ANG	AG.103.A
AR	71914	Hot Springs National	ANG	AG.214.A
AR	71914	Hot Springs National	ANG	AG.214.B
AR	72701	Fayetteville	ARNG	AN.010.A
AR	72701	Fayetteville	ARNG	AN.010.B
AR	72905	Fort Chaffee	ARNG	AN.011.A
AR	72905	Fort Chaffee	ARNG	AN.011.B
AR	72199	North Little Rock	ARNG	AN.012.A
AR	72199	North Little Rock	ARNG	AN.012.B
AR	72201	Little Rock	USA	AY.070.A
AR	72201	Little Rock	DOJ	DJ.007.A
AR	72901	Fort Smith	DOJ	DJ.142.A
AR	72202	Little Rock	FAA	FA.087.A
AR	72902	Fort Smith	NPS	NP.017.A
AR	72601	Harrison	NPS	NP.038.A
AR	71901	Hot Springs	NPS	NP.069.A
AR	72732	Garfield	NPS	NP.222.A
AR	72201	Little Rock	USCourts	UC.151.A
AR	72201	Little Rock	USCourts	UC.152.A

AR	72201	Little Rock	USCourts	UC.152.A
AR	72201	Little Rock	USCourts	UC.152.B
AR	72901	Fort Smith	USCourts	UC.153.A
AR	71901	Hot Springs	USCourts	UC.154.A
AR	72702	Fayetteville	USCourts	UC.155.A
AR	71730	El Dorado	USCourts	UC.184.A
AZ	85707	Davis Monthan AFB	USAF	AF.032.A
AZ	85707	Davis Monthan AFB	USAF	AF.032.B
AZ	85309	Luke AFB	USAF	AF.050.A
AZ	85309	Luke AFB	USAF	AF.050.B
AZ	85309	Luke AFB	USAF	AF.097.A
AZ	85707	Davis Monthan AFB	USAF	AF.098.A
AZ	85613	Fort Huachuca	USAF	AF.122.A
AZ	85034	Phoenix	ANG	AG.007.A
AZ	85034	Phoenix	ANG	AG.007.A
AZ	85034	Phoenix	ANG	AG.007.B
AZ	85034	Phoenix	ANG	AG.007.C
AZ	85034	Phoenix	ANG	AG.007.D
AZ	85706	Tucson	ANG	AG.008.A
AZ	85706	Tucson	ANG	AG.008.B
AZ	85706	Tucson	ANG	AG.008.C
AZ	85706	Tucson	ANG	AG.008.D
AZ	85008	Phoenix	ANG	AG.102.A
AZ	85008	Phoenix	ANG	AG.261.A
AZ	85008	Phoenix	ANG	AG.261.B
AZ	85653	Marana	ARNG	AN.013.A
AZ	85653	Marana	ARNG	AN.013.B
AZ	85653	Marana	ARNG	AN.014.A
AZ	85653	Marana	ARNG	AN.014.B
AZ	85008	Phoenix	ARNG	AN.015.A
AZ	85008	Phoenix	ARNG	AN.015.B
AZ	85284	Tempe	ARNG	AN.016.A
AZ	85008	Phoenix	ARNG	AN.098.A
AZ	85365	Yuma	USA	AY.064.A
AZ	85701	Tucson	DOJ	DJ.009.A
AZ	85004	Phoenix	DOJ	DJ.138.A
AZ	85365	Yuma	DOJ	DJ.187.A
AZ	86001	Flagstaff	DOJ	DJ.804.B
AZ	85255	Scottsdale	FAA	FA.058.A
AZ	85012	Phoenix	FBI	FB.003.B
AZ	85051	Phoenix	USF&W	FW.013.A
AZ	86023	Grand Canyon	NPS	NP.001.A
AZ	86322	Camp Verde	NPS	NP.015.A
AZ	86028	Petrified Forest	NPS	NP.027.A
AZ	86004	Flagstaff	NPS	NP.039.A
AZ	85730	Tucson	NPS	NP.118.A
AZ	85321	Ajo	NPS	NP.127.A
AZ	86022	Fredonia	NPS	NP.138.A
AZ	85643	Wilcox	NPS	NP.140.A
AZ	86040	Page	NPS	NP.142.A
AZ	86429	Bullhead City	NPS	NP.154.A
AZ	85545	Roosevelt	NPS	NP.190.A
AZ	86023	Grand Canyon	NPS	NP.204.A
AZ	85745	Tucson	NPS	NP.208.A
AZ	86503	Chinle	NPS	NP.214.A
AZ	85003	Phoenix	USCourts	UC.040.A
AZ	85701	Tucson	USCourts	UC.163.A
AZ	86001	Flagstaff	USCourts	UC.316.A
AZ	85364	Yuma	USCourts	UC.317.A
AZ	85004	Phoenix	USCourts	UC.349.A
AZ	85701	Tucson	USCourts	UC.366.A
AZ	85025	Phoenix	USCourts	UC.368.A
CA	90245	Los Angeles AFB	USAF	AF.012.A
CA	90245	Los Angeles AFB	USAF	AF.012.B
CA	93524	Edwards AFB	USAF	AF.020.A
CA	93524	Edwards AFB	USAF	AF.020.B
CA	93524	Edwards AFB	USAF	AF.020.C

CA	93437	Vandenberg AFB	USAF	AF.022.A
CA	93437	Vandenberg AFB	USAF	AF.022.B
CA	93437	Vandenberg AFB	USAF	AF.022.C
CA	95903	Beale AFB	USAF	AF.026.A
CA	95903	Beale AFB	USAF	AF.026.B
CA	94535	Travis AFB	USAF	AF.068.A
CA	94535	Travis AFB	USAF	AF.068.B
CA	94535	Travis AFB	USAF	AF.082.A
CA	94535	Travis AFB	USAF	AF.082.B
CA	94535	Travis AFB	USAF	AF.082.C
CA	92518	March AFB	USAF	AF.083.A
CA	92518	March AFB	USAF	AF.083.B
CA	92518	March AFB	USAF	AF.083.C
CA	92518	March AFB	USAF	AF.083.D
CA	95903	Beale AFB	USAF	AF.086.A
CA	95903	Beale AFB	USAF	AF.086.B
CA	94535	Travis AFB	USAF	AF.114.A
CA	93043	Port Hueneme	USAF	AF.123.A
CA	94535	Travis AFB	USAF	AF.140.A
CA	94089	Sunnyvale	USAF	AF.142.A
CA	94089	Sunnyvale	USAF	AF.142.B
CA	93727	Fresno	ANG	AG.011.A
CA	93727	Fresno	ANG	AG.011.B
CA	93727	Fresno	ANG	AG.011.C
CA	93727	Fresno	ANG	AG.011.D
CA	94035	Mountain View	ANG	AG.012.A
CA	94035	Mountain View	ANG	AG.012.B
CA	94035	Mountain View	ANG	AG.012.C
CA	94035	Mountain View	ANG	AG.012.D
CA	92518	March AFB	ANG	AG.013.A
CA	92518	March AFB	ANG	AG.013.B
CA	92518	March AFB	ANG	AG.013.C
CA	92518	March AFB	ANG	AG.013.D
CA	93041	Port Hueneme	ANG	AG.014.A
CA	93041	Port Hueneme	ANG	AG.014.A
CA	93041	Port Hueneme	ANG	AG.014.B
CA	93041	Port Hueneme	ANG	AG.014.D
CA	95826	Sacramento	ANG	AG.104.A
CA	95826	Sacramento	ANG	AG.104.B
CA	92111	San Diego	ANG	AG.215.A
CA	92111	San Diego	ANG	AG.215.B
CA	95660	North Highlands	ANG	AG.217.A
CA	95660	North Highlands	ANG	AG.217.B
CA	92627	Costa Mesa	ANG	AG.218.A
CA	92627	Costa Mesa	ANG	AG.218.B
CA	94545	Hayward	ANG	AG.219.A
CA	94545	Hayward	ANG	AG.219.B
CA	91406	Van Nuys	ANG	AG.220.A
CA	91406	Van Nuys	ANG	AG.220.B
CA	90720	Los Alamitos	ARNG	AN.017.A
CA	90720	Los Alamitos	ARNG	AN.017.B
CA	92310	Fort Irwin	USA	AY.039.A
CA	95304	Tracy	DLA	DA.010.A
CA	92136	San Diego	DLA	DA.034.A
CA	95304	Tracy	DLA	DA.036.A
CA	92311	Barstow	DLA	DA.037.A
CA	94089	Sunnyvale	DLA	DA.039.A
CA	90746	Carson	DLA	DA.043.A
CA	95113	San Jose	DOJ	DJ.042.A
CA	95113	San Jose	DOJ	DJ.042.B
CA	92101	San Diego	DOJ	DJ.135.A
CA	90012	Los Angeles	DOJ	DJ.140.A
CA	90012	Los Angeles	DOJ	DJ.141.A
CA	94612	Oakland	DOJ	DJ.149.A
CA	92101	San Diego	DOJ	DJ.161.A
CA	92501	Riverside	DOJ	DJ.166.A
CA	92243	El Centro	DOJ	DJ.806.B

CA	93721	Fresno	DOJ	DJ.807.B
CA	95814	Sacramento	DOJ	DJ.810.B
CA	94102	San Francisco	DOJ	DJ.811.B
CA	92701	Santa Ana	DOJ	DJ.813.B
CA	90261	Lawndale	FAA	FA.050.A
CA	90261	Lawndale	FAA	FA.050.B
CA	93550	Palmdale	FAA	FA.051.A
CA	93550	Palmdale	FAA	FA.051.B
CA	94536	Fremont	FAA	FA.052.A
CA	94536	Fremont	FAA	FA.052.B
CA	90712	Lakewood	FAA	FA.053.A
CA	93550	Mather	FAA	FA.054.A
CA	90261	Burlingame	FAA	FA.055.A
CA	92126	San Diego	FAA	FA.057.A
CA	92504	Riverside	FAA	FA.089.A
CA	91406	Van Nuys	FAA	FA.090.A
CA	93727	Fresno	FAA	FA.096.A
CA	92582	Sacramento	FAA	FA.097.A
CA	92123	San Diego	FAA	FA.098.A
CA	94502	Alameda	FAA	FA.099.A
CA	94014	Daly City	FAA	FA.100.A
CA	95110	San Jose	FAA	FA.102.A
CA	90815	Long Beach	FAA	FA.103.A
CA	95825	Sacramento	USF&W	FW.014.A
CA	92008	Carlsbad	USF&W	FW.018.A
CA	92311	Barstow	NPS	NP.012.A
CA	92277	Twentynine Palms	NPS	NP.024.A
CA	92328	Death Valley	NPS	NP.058.A
CA	95318	El Portal	NPS	NP.073.A
CA	91360-4207	Thousand Oaks	NPS	NP.085.A
CA	96063	Mineral	NPS	NP.092.A
CA	95555	Orick	NPS	NP.096.A
CA	94123	San Francisco	NPS	NP.113.A
CA	93271	Three Rivers	NPS	NP.117.A
CA	94956	Point Reyes Station	NPS	NP.121.A
CA	94607	Oakland	NPS	NP.122.A
CA	92106	San Diego	NPS	NP.163.A
CA	93001	Ventura	NPS	NP.164.A
CA	96134	Tulelake	NPS	NP.173.A
CA	96095	Whiskeytown	NPS	NP.185.A
CA	95043	Paicines	NPS	NP.206.A
CA	93526	Independence	NPS	NP.211.A
CA	92136	San Diego	USN	NY.004.A
CA	92136	San Diego	USN	NY.004.B
CA	92101	San Diego	USCourts	UC.035.A
CA	92101	San Diego	USCourts	UC.035.B
CA	92101	San Diego	USCourts	UC.035.B
CA	90012	Los Angeles	USCourts	UC.037.A
CA	90012	Los Angeles	USCourts	UC.037.B
CA	90012	Los Angeles	USCourts	UC.037.C
CA	92701	Santa Ana	USCourts	UC.039.A
CA	91105	Pasadena	USCourts	UC.145.A
CA	94103	San Francisco	USCourts	UC.146.A
CA	94102	San Francisco	USCourts	UC.180.A
CA	92101	San Diego	USCourts	UC.183.B
CA	92101	San Diego	USCourts	UC.183.C
CA	95814	Sacramento	USCourts	UC.197.A
CA	93721	Fresno	USCourts	UC.220.A
CA	93721	Fresno	USCourts	UC.220.A
CA	92101	San Diego	USCourts	UC.232.A
CA	95113	San Jose	USCourts	UC.240.A
CA	95113	San Jose	USCourts	UC.240.B
CA	92243	El Centro	USCourts	UC.251.A
CA	94104	San Francisco	USCourts	UC.282.A
CA	94612	Oakland	USCourts	UC.286.A
CA	95404	Santa Rosa	USCourts	UC.322.A
CA	92502	Riverside	USCourts	UC.344.A

CA	92501	Riverside	USCourts	UC.704.A
CA	91367	Woodland Hills	USCourts	UC.705.A
CA	93101	Santa Barbara	USCourts	UC.706.A
CA	90012	Los Angeles	USCourts	UC.804.B
CO	80914	Peterson AFB	USAF	AF.018.A
CO	80914	Peterson AFB	USAF	AF.018.B
CO	80840	U S A F Academy	USAF	AF.069.A
CO	80840	U S A F Academy	USAF	AF.069.B
CO	80011	Aurora	USAF	AF.079.A
CO	80914	Peterson AFB	USAF	AF.108.A
CO	80914	Peterson AFB	USAF	AF.108.B
CO	80914	Peterson AFB	USAF	AF.108.C
CO	80914	Peterson AFB	USAF	AF.108.D
CO	80011	Aurora	ANG	AG.015.A
CO	80011	Aurora	ANG	AG.015.B
CO	80011	Aurora	ANG	AG.015.C
CO	80011	Aurora	ANG	AG.015.D
CO	80112	Centennial	ANG	AG.105.A
CO	80631	Greeley	ANG	AG.221.A
CO	80631	Greeley	ANG	AG.221.B
CO	80913	Fort Carson	USA	AY.033.A
CO	81301	Durango	DOJ	DJ.013.A
CO	81501	Grand Junction	DOJ	DJ.014.A
CO	80202	Denver	DOJ	DJ.139.A
CO	80501	Longmont	FAA	FA.028.A
CO	80501	Longmont	FAA	FA.028.B
CO	80249	Denver	FAA	FA.030.A
CO	80215	Lakewood	USF&W	FW.008.A
CO	80215	Lakewood	USF&W	FW.008.A
CO	81330-0008	Mesa Verde National Park	NPS	NP.040.A
CO	80225	Denver	NPS	NP.060.A
CO	81146	Mosca	NPS	NP.094.A
CO	81050	La Junta	NPS	NP.098.A
CO	81610	Dinosaur	NPS	NP.101.A
CO	80517	Estes Park	NPS	NP.130.A
CO	81521	Fruita	NPS	NP.132.A
CO	80447	Grand Lake	NPS	NP.133.A
CO	80816	Florissant	NPS	NP.166.A
CO	80525	Fort Collins	NPS	NP.224.A
CO	80294	Denver	USCourts	UC.127.A
CO	80294	Denver	USCourts	UC.211.A
CO	80294	Denver	USCourts	UC.211.B
CT	06026	East Granby	ANG	AG.016.A
CT	06026	East Granby	ANG	AG.016.B
CT	06026	East Granby	ANG	AG.016.C
CT	06026	East Granby	ANG	AG.016.D
CT	06105	Hartford	ANG	AG.106.A
CT	06477	Orange	ANG	AG.222.A
CT	06477	Orange	ANG	AG.222.A
CT	06477	Orange	ANG	AG.222.B
CT	06108	East Hartford	DLA	DA.019.A
CT	06103	Hartford	DOJ	DJ.012.A
CT	06510	New Haven	DOJ	DJ.015.A
CT	06096	Windsor Locks	FAA	FA.104.A
CT	06103	Hartford	USCourts	UC.034.A
CT	06103	Hartford	USCourts	UC.034.B
CT	06103	Hartford	USCourts	UC.034.C
CT	06510	New Haven	USCourts	UC.164.A
CT	06510	New Haven	USCourts	UC.164.B
CT	06604	Bridgeport	USCourts	UC.255.A
CT	06604	Bridgeport	USCourts	UC.255.B
DC	20332	Bolling AFB	USAF	AF.027.A
DC	20332	Bolling AFB	USAF	AF.027.B
DC	20003	Washington	ANG	AG.107.A
DC	20003	Washington	ANG	AG.107.B
DC	20001	Washington	DOJ	DJ.016.A
DC	20001	Washington	DOJ	DJ.016.B

DC	20002	Washington	DOJ	DJ.017.A
DC	20003	Washington	DOJ	DJ.018.A
DC	20004	Washington	DOJ	DJ.019.A
DC	20001	Washington	DOJ	DJ.177.A
DC	20001	Washington	DOJ	DJ.177.B
DC	20001	Washington	DOJ	DJ.183.A
DC	20591	Washington	FAA	FA.012.A
DC	20591	Washington	FAA	FA.012.B
DC	20531	Washington	DOJ	JP.001.A
DC	20005	Washington	NPS	NP.007.A
DC	20242	Washington	NPS	NP.009.A
DC	20242	Washington	NPS	NP.037.A
DC	20008-1207	Washington	NPS	NP.074.A
DC	20020	Washington	NPS	NP.220.A
DC	20240	Washington	NPS	NP.221.A
DC	20004	Washington	DOJ	PR.001.A
DC	20001	Washington	USCourts	UC.121.A
DC	20439	Washington	USCourts	UC.150.A
DC	20544	Washington	USCourts	UC.199.A
DC	20004	Washington	USCourts	UC.707.A
DE	19902	Dover AFB	USAF	AF.033.A
DE	19902	Dover AFB	USAF	AF.033.B
DE	19902	Dover AFB	USAF	AF.033.C
DE	19902	Dover AFB	USAF	AF.089.A
DE	19902	Dover AFB	USAF	AF.089.B
DE	19720	New Castle	ANG	AG.017.A
DE	19720	New Castle	ANG	AG.017.A
DE	19720	New Castle	ANG	AG.017.A
DE	19720	New Castle	ANG	AG.017.C
DE	19720	New Castle	ANG	AG.017.D
DE	19930	Bethany Beach	ANG	AG.108.A
DE	19720	New Castle	ARNG	AN.021.A
DE	19720	New Castle	ARNG	AN.021.B
DE	19801	Wilmington	DOJ	DJ.020.A
DE	19801	Wilmington	USCourts	UC.003.A
FL	32403	Tyndall AFB	USAF	AF.007.A
FL	32403	Tyndall AFB	USAF	AF.007.B
FL	32403	Tyndall AFB	USAF	AF.007.C
FL	32542	Eglin AFB	USAF	AF.009.A
FL	32542	Eglin AFB	USAF	AF.009.B
FL	32542	Eglin AFB	USAF	AF.009.C
FL	32544	Hurlburt Field	USAF	AF.045.A
FL	32544	Hurlburt Field	USAF	AF.045.B
FL	33621	MacDill AFB	USAF	AF.051.A
FL	33621	MacDill AFB	USAF	AF.051.B
FL	33621	MacDill AFB	USAF	AF.051.B
FL	32925	Patrick AFB	USAF	AF.062.A
FL	33621	MacDill AFB	USAF	AF.074.A
FL	32542	Eglin AFB	USAF	AF.080.A
FL	32542	Eglin AFB	USAF	AF.080.B
FL	32542	Eglin AFB	USAF	AF.080.C
FL	33039	Homestead AFB	USAF	AF.094.A
FL	33039	Homestead AFB	USAF	AF.094.B
FL	32925	Patrick AFB	USAF	AF.107.A
FL	32925	Patrick AFB	USAF	AF.107.B
FL	32925	Patrick AFB	USAF	AF.107.C
FL	33621	MacDill AFB	USAF	AF.112.A
FL	32508-5142	Pensacola	USAF	AF.125.A
FL	32508	Pensacola	USAF	AF.125.B
FL	32403	Panama City	ANG	AG.019.A
FL	32403	Panama City	ANG	AG.019.B
FL	32403	Panama City	ANG	AG.019.C
FL	32403	Panama City	ANG	AG.019.D
FL	32218	Jacksonville	ANG	AG.020.A
FL	32218	Jacksonville	ANG	AG.020.B
FL	32218	Jacksonville	ANG	AG.020.C
FL	32218	Jacksonville	ANG	AG.020.C

FL	32218	Jacksonville	ANG	AG.020.D
FL	32085	St Augustine	ANG	AG.109.A
FL	33621	MacDill AFB	ANG	AG.258.A
FL	33621	MacDill AFB	ANG	AG.258.B
FL	32091	Stark	ANG	AG.260.A
FL	32091	Stark	ANG	AG.260.B
FL	32403	Panama City	ANG	AG.999.A
FL	32403	Panama City	ANG	AG.999.B
FL	32403	Panama City	ANG	AG.999.C
FL	32826	Orlando	USA	AY.053.A
FL	32212-0103	Jacksonville	DLA	DA.018.A
FL	32803	Orlando	DLA	DA.027.A
FL	33394	Fort Lauderdale	DOJ	DJ.021.A
FL	34950	Fort Pierce	DOJ	DJ.022.A
FL	32601	Gainesville	DOJ	DJ.023.A
FL	32202	Jacksonville	DOJ	DJ.024.A
FL	33132	Miami	DOJ	DJ.025.A
FL	32501	Pensacola	DOJ	DJ.027.A
FL	33602	Tampa	DOJ	DJ.029.A
FL	33401	West Palm Beach	DOJ	DJ.030.A
FL	32805	Orlando	DOJ	DJ.178.A
FL	33901	Fort Myers	DOJ	DJ.817.B
FL	32801	Orlando	DOJ	DJ.818.B
FL	32301	Tallahassee	DOJ	DJ.819.B
FL	32925	Patrick AFB	DEOMI	DM.001.A
FL	32046	Hilliard	FAA	FA.035.A
FL	32046	Hilliard	FAA	FA.035.B
FL	33166	Miami	FAA	FA.036.A
FL	33166	Miami	FAA	FA.036.B
FL	32137	Palm Coast	FAA	FA.037.A
FL	32137	Palm Coast	FAA	FA.037.B
FL	32822	Orlando	FAA	FA.042.A
FL	33811	Lakeland	FAA	FA.061.A
FL	33166	Miami	FAA	FA.066.A
FL	33609	Tampa	FAA	FA.068.A
FL	32561	Gulf Breeze	NPS	NP.018.A
FL	32225	Jacksonville	NPS	NP.021.A
FL	32796	Titusville	NPS	NP.030.A
FL	34141	Ochopee	NPS	NP.076.A
FL	32310	Tallahassee	NPS	NP.082.A
FL	33034	Homestead	NPS	NP.108.A
FL	32084	St Augustine	NPS	NP.189.A
FL	33130	Miami	USCourts	UC.032.A
FL	33128	Miami	USCourts	UC.033.A
FL	33602	Tampa	USCourts	UC.116.A
FL	32501	Pensacola	USCourts	UC.117.A
FL	32801	Orlando	USCourts	UC.166.A
FL	33401	West Palm Beach	USCourts	UC.167.A
FL	33401	West Palm Beach	USCourts	UC.167.B
FL	33301	Fort Lauderdale	USCourts	UC.210.A
FL	33301	Fort Lauderdale	USCourts	UC.210.A
FL	33901	Fort Myers	USCourts	UC.263.A
FL	32301	Tallahassee	USCourts	UC.287.A
FL	34475	Ocala	USCourts	UC.302.A
FL	32601	Gainesville	USCourts	UC.314.A
FL	32501	Pensacola	USCourts	UC.341.A
FL	32401	Panama City	USCourts	UC.348.A
FL	33602	Tampa	USCourts	UC.356.A
FL	32801	Orlando	USCourts	UC.709.A
FL	32202	Jacksonville	USCourts	UC.805.B
FL	32202	Jacksonville	USCourts	UC.805.C
GA	31098	Robins AFB	USAF	AF.013.A
GA	31098	Robins AFB	USAF	AF.013.B
GA	31098	Robins AFB	USAF	AF.013.B
GA	31098	Robins AFB	USAF	AF.013.C
GA	31098	Robins AFB	USAF	AF.013.D
GA	31699	Moody AFB	USAF	AF.057.A

GA	31699	Moody AFB	USAF	AF.057.A
GA	31699	Moody AFB	USAF	AF.057.A
GA	31699	Moody AFB	USAF	AF.057.A
GA	30905	Fort Gordon	USAF	AF.075.A
GA	30069	Dobbins AFB	USAF	AF.088.A
GA	31098	Robins AFB	USAF	AF.093.A
GA	31905	Fort Benning	USAF	AF.124.A
GA	31098	Robins AFB	USAF	AF.138.A
GA	31098	Robins AFB	USAF	AF.138.B
GA	31098	Robins AFB	USAF	AF.138.C
GA	31098	Robins AFB	USAF	AF.138.D
GA	31098	Robins AFB	USAF	AF.138.E
GA	31098	Robins AFB	USAF	AF.138.F
GA	31098	Robins AFB	USAF	AF.138.G
GA	30069	Dobbins AFB	USAF	AF.139.A
GA	30069	Dobbins AFB	USAF	AF.139.B
GA	30060	Dobbins AFB	ANG	AG.021.A
GA	30060	Dobbins AFB	ANG	AG.021.B
GA	30060	Dobbins AFB	ANG	AG.021.C
GA	30060	Dobbins AFB	ANG	AG.021.D
GA	31408	Garden City	ANG	AG.022.A
GA	31408	Garden City	ANG	AG.022.B
GA	31408	Garden City	ANG	AG.022.C
GA	31408	Garden City	ANG	AG.022.D
GA	31408	Garden City	ANG	AG.022.E
GA	31098	Warner Robins	ANG	AG.098.A
GA	31098	Warner Robins	ANG	AG.098.B
GA	31098	Warner Robins	ANG	AG.098.C
GA	31098	Warner Robins	ANG	AG.098.D
GA	31098	Warner Robins	ANG	AG.098.E
GA	31409	Savannah	ANG	AG.223.A
GA	31409	Savannah	ANG	AG.223.B
GA	31297	Macon	ANG	AG.225.A
GA	31297	Macon	ANG	AG.225.B
GA	31525	Brunswick	ANG	AG.226.A
GA	31525	Brunswick	ANG	AG.226.B
GA	31905	Fort Benning	USA	AY.006.A
GA	31905	Fort Benning	USA	AY.006.B
GA	31314	Fort Stewart	USA	AY.047.A
GA	31704	Albany	DLA	DA.020.A
GA	31098	Warner Robins	DLA	DA.022.A
GA	30060	Marietta	DLA	DA.040.A
GA	30901	Augusta	DOJ	DJ.032.A
GA	31901-4298	Columbus	DOJ	DJ.033.A
GA	31401	Savannah	DOJ	DJ.034.A
GA	31701	Albany	DOJ	DJ.148.A
GA	31201	Macon	DOJ	DJ.189.A
GA	30303	Atlanta	DOJ	DJ.820.B
GA	30337	College Park	FAA	FA.033.A
GA	30337	College Park	FAA	FA.033.B
GA	30228	Hampton	FAA	FA.034.A
GA	30228	Hampton	FAA	FA.034.B
GA	30345	Atlanta	USF&W	FW.009.A
GA	30303	Atlanta	NPS	NP.002.A
GA	31711	Andersonville	NPS	NP.041.A
GA	31711	Andersonville	NPS	NP.041.A
GA	30742	Fort Oglethorpe	NPS	NP.042.A
GA	30350	Atlanta	NPS	NP.091.A
GA	31525	Brunswick	NPS	NP.126.A
GA	31558	St Marys	NPS	NP.192.A
GA	31217	Macon	NPS	NP.196.A
GA	30303	Atlanta	USCourts	UC.004.A
GA	30303	Atlanta	USCourts	UC.004.B
GA	30303	Atlanta	USCourts	UC.118.A
GA	31401	Savannah	USCourts	UC.119.A
GA	30901	Augusta	USCourts	UC.120.A
GA	31901	Columbus	USCourts	UC.141.A

GA	31202	Macon	USCourts	UC.142.A
GA	31202	Macon	USCourts	UC.142.A
GA	31202	Macon	USCourts	UC.142.A
GA	31202	Macon	USCourts	UC.237.A
GA	31520	Brunswick	USCourts	UC.244.A
GA	31201	Macon	USCourts	UC.264.A
HI	96853	Hickam AFB	USAF	AF.044.A
HI	96709	Kapolei	USAF	AF.141.A
HI	96853	Hickam AFB	ANG	AG.023.A
HI	96853	Hickam AFB	ANG	AG.023.B
HI	96853	Hickam AFB	ANG	AG.023.C
HI	96853	Hickam AFB	ANG	AG.023.D
HI	96853	Hickam AFB	ANG	AG.023.D
HI	96816	Honolulu	ANG	AG.111.A
HI	96796	Waimea	ANG	AG.201.A
HI	96796	Waimea	ANG	AG.201.B
HI	96854	Wheeler AAF	ANG	AG.203.A
HI	96854	Wheeler AAF	ANG	AG.203.B
HI	96721	Hilo	ANG	AG.204.A
HI	96721	Hilo	ANG	AG.204.B
HI	96732	Kahului	ANG	AG.205.A
HI	96732	Kahului	ANG	AG.205.B
HI	96752	Kekaha	ANG	AG.206.A
HI	96752	Kekaha	ANG	AG.206.B
HI	96862	Barbers Point	ANG	AG.207.A
HI	96862	Barbers Point	ANG	AG.207.B
HI	96720	Hilo	ARNG	AN.024.A
HI	96720	Hilo	ARNG	AN.024.B
HI	96854	Honolulu	ARNG	AN.025.A
HI	96854	Honolulu	ARNG	AN.025.B
HI	96860-4544	Pearl Harbor	DLA	DA.042.A
HI	96850	Honolulu	DOJ	DJ.011.A
HI	96819	Honolulu	FAA	FA.059.A
HI	96769	Makawao	NPS	NP.119.A
HI	96785	Volcano	NPS	NP.123.A
HI	96740	Kailua Kona	NPS	NP.148.A
HI	96850	Honolulu	USCourts	UC.005.A
IA	50321	Des Moines	ANG	AG.030.A
IA	50321	Des Moines	ANG	AG.030.B
IA	50321	Des Moines	ANG	AG.030.C
IA	50321	Des Moines	ANG	AG.030.D
IA	51111	Sioux City	ANG	AG.031.A
IA	51111	Sioux City	ANG	AG.031.B
IA	51111	Sioux City	ANG	AG.031.C
IA	51111	Sioux City	ANG	AG.031.D
IA	50131	Johnston	ANG	AG.115.A
IA	50501	Fort Dodge	ANG	AG.228.A
IA	50501	Fort Dodge	ANG	AG.228.B
IA	50036	Boone	ARNG	AN.026.A
IA	50036	Boone	ARNG	AN.026.B
IA	52806	Davenport	ARNG	AN.027.A
IA	52806	Davenport	ARNG	AN.027.B
IA	50703	Waterloo	ARNG	AN.028.A
IA	50703	Waterloo	ARNG	AN.028.B
IA	52401	Cedar Rapids	DOJ	DJ.035.A
IA	50309	Des Moines	DOJ	DJ.036.A
IA	51101	Sioux City	DOJ	DJ.186.A
IA	52801	Davenport	DOJ	DJ.188.A
IA	50021	Ankeny	FAA	FA.076.A
IA	52358	West Branch	NPS	NP.172.A
IA	52146	Harpers Ferry	NPS	NP.203.A
IA	50309	Des Moines	USCourts	UC.022.A
IA	51101	Sioux City	USCourts	UC.023.A
IA	52401	Cedar Rapids	USCourts	UC.024.A
ID	83648	Mountain Home AFB	USAF	AF.058.A
ID	83648	Mountain Home AFB	USAF	AF.058.B
ID	83705	Boise	ANG	AG.024.A

ID	83705	Boise	ANG	AG.024.B
ID	83705	Boise	ANG	AG.024.C
ID	83705	Boise	ANG	AG.024.D
ID	83705	Boise	ARNG	AN.029.A
ID	83705	Boise	ARNG	AN.029.B
ID	83713	Boise	ARNG	AN.048.A
ID	83713	Boise	ARNG	AN.048.B
ID	83401	Idaho Falls	DOE	DE.041.A
ID	83712	Boise	DOJ	DJ.037.A
ID	83814	Coeur D Alene	DOJ	DJ.824.B
ID	83201	Pocatello	DOJ	DJ.825.B
ID	83705	Boise	FAA	FA.105.A
ID	83540	Spalding	NPS	NP.043.A
ID	83332	Hagerman	NPS	NP.171.A
ID	83213	Arco	NPS	NP.229.A
ID	83724	Boise	USCourts	UC.101.A
ID	83724	Boise	USCourts	UC.101.B
ID	83201	Pocatello	USCourts	UC.229.A
ID	83814	Coeur D Alene	USCourts	UC.283.A
IL	62225	Scott AFB	USAF	AF.006.A
IL	62225	Scott AFB	USAF	AF.006.B
IL	62225	Scott AFB	USAF	AF.111.A
IL	62225	Scott AFB	ANG	AG.025.A
IL	62225	Scott AFB	ANG	AG.025.B
IL	62225	Scott AFB	ANG	AG.025.B
IL	62225	Scott AFB	ANG	AG.025.C
IL	62225	Scott AFB	ANG	AG.025.D
IL	61607	Peoria	ANG	AG.026.A
IL	61607	Peoria	ANG	AG.026.B
IL	61607	Peoria	ANG	AG.026.C
IL	61607	Peoria	ANG	AG.026.D
IL	62707	Springfield	ANG	AG.027.A
IL	62707	Springfield	ANG	AG.027.A
IL	62707	Springfield	ANG	AG.027.A
IL	62707	Springfield	ANG	AG.027.B
IL	62707	Springfield	ANG	AG.027.C
IL	62707	Springfield	ANG	AG.027.C
IL	62707	Springfield	ANG	AG.027.D
IL	62707	Springfield	ANG	AG.113.A
IL	62707	Springfield	ANG	AG.113.B
IL	62707	Springfield	ANG	AG.113.C
IL	61607	Bartonville	ARNG	AN.031.A
IL	61607	Bartonville	ARNG	AN.031.B
IL	62521	Decatur	ARNG	AN.032.A
IL	62521	Decatur	ARNG	AN.032.B
IL	61115	Machesney Park	ARNG	AN.033.A
IL	61115	Machesney Park	ARNG	AN.033.B
IL	60638	Chicago	ARNG	AN.034.A
IL	60638	Chicago	ARNG	AN.034.B
IL	61299	Rock Island	USA	AY.018.A
IL	60439	Lemont	DOE	DE.008.A
IL	60439	Lemont	DOE	DE.008.B
IL	62208	Fairview Heights	DOJ	DJ.039.A
IL	61201	Rock Island	DOJ	DJ.040.A
IL	61101	Rockford	DOJ	DJ.041.A
IL	61602	Peoria	DOJ	DJ.136.A
IL	62701	Springfield	DOJ	DJ.158.A
IL	62201	East St Louis	DOJ	DJ.814.B
IL	60604	Chicago	DOJ	DJ.826.B
IL	61801	Urbana	DOJ	DJ.828.B
IL	60018	Des Plaines	FAA	FA.014.A
IL	60018	Des Plaines	FAA	FA.014.B
IL	60506	Aurora	FAA	FA.015.A
IL	60506	Aurora	FAA	FA.015.B
IL	60123	Elgin	FAA	FA.022.A
IL	62707	Springfield	FAA	FA.082.A
IL	60185	West Chicago	FAA	FA.106.A

IL	62701	Springfield	NPS	NP.029.A
IL	60604	Chicago	USCourts	UC.028.A
IL	61602	Peoria	USCourts	UC.029.A
IL	61602	Peoria	USCourts	UC.029.B
IL	61801	Urbana	USCourts	UC.030.A
IL	62701	Springfield	USCourts	UC.031.A
IL	62701	Springfield	USCourts	UC.031.B
IL	62701	Springfield	USCourts	UC.031.C
IL	62201	East St Louis	USCourts	UC.090.A
IL	62812	Benton	USCourts	UC.201.A
IL	61832	Danville	USCourts	UC.223.A
IL	61101	Rockford	USCourts	UC.270.A
IN	46971	Grissom AFB	USAF	AF.092.A
IN	46971	Grissom AFB	USAF	AF.129.A
IN	46809	Fort Wayne	ANG	AG.028.A
IN	46809	Fort Wayne	ANG	AG.028.B
IN	46809	Fort Wayne	ANG	AG.028.C
IN	46809	Fort Wayne	ANG	AG.028.D
IN	47803	Terre Haute	ANG	AG.029.A
IN	47803	Terre Haute	ANG	AG.029.B
IN	47803	Terre Haute	ANG	AG.029.C
IN	47803	Terre Haute	ANG	AG.029.D
IN	46241	Indianapolis	ANG	AG.114.A
IN	46176	Shelbyville	ARNG	AN.035.A
IN	46176	Shelbyville	ARNG	AN.035.B
IN	46249	Indianapolis	USA	AY.030.A
IN	46320	Hammond	DOJ	DJ.043.A
IN	46204	Indianapolis	DOJ	DJ.044.A
IN	47708	Evansville	DOJ	DJ.153.A
IN	46802	Fort Wayne	DOJ	DJ.829.B
IN	46601	South Bend	DOJ	DJ.831.B
IN	46241	Indianapolis	FAA	FA.017.A
IN	46241	Indianapolis	FAA	FA.017.B
IN	46628	South Bend	FAA	FA.069.A
IN	46241	Indianapolis	FAA	FA.107.A
IN	46304	Chesterton	NPS	NP.010.A
IN	47552	Lincoln City	NPS	NP.124.A
IN	46204	Indianapolis	USCourts	UC.006.A
IN	46802	Fort Wayne	USCourts	UC.025.A
IN	46320	Hammond	USCourts	UC.026.A
IN	46320	Hammond	USCourts	UC.026.B
IN	46634	South Bend	USCourts	UC.027.A
IN	46601	South Bend	USCourts	UC.043.A
IN	47708	Evansville	USCourts	UC.230.A
IN	47150	New Albany	USCourts	UC.231.A
KS	67221	McConnell AFB	USAF	AF.054.A
KS	67221	McConnell AFB	USAF	AF.054.B
KS	67221	McConnell AFB	USAF	AF.101.A
KS	66619	Topeka	ANG	AG.032.A
KS	66619	Topeka	ANG	AG.032.B
KS	66619	Topeka	ANG	AG.032.C
KS	66619	Topeka	ANG	AG.032.D
KS	67221	McConnell AFB	ANG	AG.033.A
KS	67221	McConnell AFB	ANG	AG.033.B
KS	67221	McConnell AFB	ANG	AG.033.C
KS	67221	McConnell AFB	ANG	AG.033.D
KS	66611	Topeka	ANG	AG.116.A
KS	66027	Fort Leavenworth	ARNG	AN.036.A
KS	66027	Fort Leavenworth	ARNG	AN.036.B
KS	67401	Salina	ARNG	AN.037.A
KS	67401	Salina	ARNG	AN.037.B
KS	66027	Fort Leavenworth	USA	AY.040.A
KS	66442	Fort Riley	USA	AY.046.A
KS	67202	Wichita	DOJ	DJ.045.A
KS	66101	Kansas City	DOJ	DJ.832.B
KS	66683	Topeka	DOJ	DJ.833.B
KS	66062	Olathe	FAA	FA.004.A

KS	66062	Olathe	FAA	FA.004.B
KS	67209	Wichita	FAA	FA.006.A
KS	66612	Topeka	NPS	NP.146.A
KS	67550	Larned	NPS	NP.167.A
KS	66845	Cottonwood Falls	NPS	NP.228.A
KS	66845	Cottonwood Falls	NPS	NP.228.A
KS	66101	Kansas City	USCourts	UC.019.A
KS	67202	Wichita	USCourts	UC.020.A
KS	66683	Topeka	USCourts	UC.021.A
KY	40213	Louisville	ANG	AG.034.A
KY	40213	Louisville	ANG	AG.034.B
KY	40213	Louisville	ANG	AG.034.C
KY	40213	Louisville	ANG	AG.034.D
KY	40601	Frankfort	ANG	AG.117.A
KY	40601	Frankfort	ARNG	AN.038.A
KY	40601	Frankfort	ARNG	AN.038.B
KY	40121	Fort Knox	USA	AY.010.A
KY	42223	Fort Campbell	USA	AY.094.A
KY	41011	Covington	DOJ	DJ.046.A
KY	40507	Lexington	DOJ	DJ.047.A
KY	40202	Louisville	DOJ	DJ.049.A
KY	42001	Paducah	DOJ	DJ.156.A
KY	40218	Louisville	FAA	FA.062.A
KY	40965	Middlesboro	NPS	NP.104.A
KY	42259	Mammoth Cave	NPS	NP.109.A
KY	40965	Middlesboro	NPS	NP.112.A
KY	42748	Hodgenville	NPS	NP.161.A
KY	40507	Lexington	USCourts	UC.007.A
KY	40202	Louisville	USCourts	UC.008.A
KY	41011	Covington	USCourts	UC.017.A
KY	40741	London	USCourts	UC.018.A
KY	40741	London	USCourts	UC.018.A
KY	40741	London	USCourts	UC.018.A
KY	40507	Lexington	USCourts	UC.257.A
KY	40602	Frankfort	USCourts	UC.273.A
KY	42001	Paducah	USCourts	UC.311.A
KY	42301	Owensboro	USCourts	UC.312.A
KY	41104	Ashland	USCourts	UC.357.A
KY	41104	Ashland	USCourts	UC.357.A
LA	71110	Barksdale AFB	USAF	AF.025.A
LA	71110	Barksdale AFB	USAF	AF.025.B
LA	71110	Barksdale AFB	USAF	AF.085.A
LA	70143	New Orleans	USAF	AF.105.A
LA	70143	New Orleans	USAF	AF.105.B
LA	70143	New Orleans	USAF	AF.105.C
LA	71110	Barksdale AFB	USAF	AF.136.A
LA	70143	New Orleans	ANG	AG.035.A
LA	70143	New Orleans	ANG	AG.035.B
LA	70143	New Orleans	ANG	AG.035.C
LA	70143	New Orleans	ANG	AG.035.D
LA	70117	New Orleans	ANG	AG.118.A
LA	70117	New Orleans	ANG	AG.118.B
LA	70401	Hammond	ANG	AG.229.A
LA	70401	Hammond	ANG	AG.229.B
LA	71360	Pineville	ANG	AG.230.A
LA	71360	Pineville	ANG	AG.230.B
LA	70501	LaFayette	DOJ	DJ.050.A
LA	70130	New Orleans	DOJ	DJ.051.A
LA	70801	Baton Rouge	DOJ	DJ.834.B
LA	71101	Shreveport	DOJ	DJ.835.B
LA	70062	Kenner	FAA	FA.048.A
LA	70808	Baton Rouge	FAA	FA.086.A
LA	70445	Lacombe	USF&W	FW.019.A
LA	70130	New Orleans	NPS	NP.095.A
LA	71457	Natchitoches	NPS	NP.136.A
LA	70801	Baton Rouge	USCourts	UC.009.A
LA	71101	Shreveport	USCourts	UC.041.A

LA	70130	New Orleans	USCourts	UC.042.A
LA	71301	Alexandria	USCourts	UC.259.A
LA	70501	Lafayette	USCourts	UC.260.A
MA	01731	Hanscom AFB	USAF	AF.021.A
MA	01731	Hanscom AFB	USAF	AF.021.B
MA	01022	Westover AFB	USAF	AF.115.A
MA	01022	Westover AFB	USAF	AF.147.A
MA	01022	Westover AFB	USAF	AF.147.A
MA	01022	Westover AFB	USAF	AF.147.A
MA	01022	Westover AFB	USAF	AF.148.A
MA	02542	Buzzards Bay	ANG	AG.038.A
MA	02542	Buzzards Bay	ANG	AG.038.B
MA	02542	Buzzards Bay	ANG	AG.038.C
MA	02542	Buzzards Bay	ANG	AG.038.D
MA	01085	Westfield	ANG	AG.039.A
MA	01085	Westfield	ANG	AG.039.B
MA	01085	Westfield	ANG	AG.039.C
MA	01085	Westfield	ANG	AG.039.D
MA	01757	Milford	ANG	AG.121.A
MA	01757	Milford	ANG	AG.121.B
MA	01757	Milford	ANG	AG.121.C
MA	01550	Southbridge	DFAS	DF.001.A
MA	01103	Springfield	DOJ	DJ.053.A
MA	02210	Boston	DOJ	DJ.145.A
MA	01608	Worcester	DOJ	DJ.837.B
MA	01803	Burlington	FAA	FA.023.A
MA	01803	Burlington	FAA	FA.023.B
MA	02421	Lexington	FAA	FA.108.A
MA	01035	Hadley	USF&W	FW.004.A
MA	01850	Lowell	NPS	NP.008.A
MA	02667	Wellfleet	NPS	NP.032.A
MA	02129	Boston	NPS	NP.100.A
MA	01970	Salem	NPS	NP.103.A
MA	01105	Springfield	NPS	NP.182.A
MA	02109	Boston	USCourts	UC.194.A
MA	02222	Boston	USCourts	UC.266.A
MA	01608	Worcester	USCourts	UC.267.A
MD	20762	Andrews AFB	USAF	AF.023.A
MD	20762	Andrews AFB	USAF	AF.023.B
MD	21005	Aberdeen Proving G	USAF	AF.030.A
MD	20762	Andrews AFB	USAF	AF.084.A
MD	20762	Andrews AFB	ANG	AG.018.A
MD	20762	Andrews AFB	ANG	AG.018.B
MD	20762	Andrews AFB	ANG	AG.018.B
MD	20762	Andrews AFB	ANG	AG.018.C
MD	21220	Baltimore	ANG	AG.037.A
MD	21220	Baltimore	ANG	AG.037.B
MD	21220	Baltimore	ANG	AG.037.C
MD	21220	Baltimore	ANG	AG.037.C
MD	21220	Baltimore	ANG	AG.037.D
MD	20762	Andrews AFB	ANG	AG.120.A
MD	20762	Andrews AFB	ANG	AG.120.B
MD	20762	Andrews AFB	ANG	AG.900.B
MD	21010	EdgeWood	ARNG	AN.039.A
MD	21010	EdgeWood	ARNG	AN.039.B
MD	20854	Rockville	DOJ	DJ.180.A
MD	20854	Rockville	DOJ	DJ.180.B
MD	21201	Baltimore	DOJ	DJ.185.A
MD	20770	Greenbelt	DOJ	DJ.839.B
MD	20769	Glen Dale	FAA	FA.075.A
MD	20910	Silver Spring	FAA	FA.077.A
MD	21061	Glen Burnie	FAA	FA.109.A
MD	20785	Landover	NPS	NP.025.A
MD	21704	Frederick	NPS	NP.089.A
MD	21811	Berlin	NPS	NP.090.A
MD	21740	Hagerstown	NPS	NP.149.A
MD	21230	Baltimore	NPS	NP.168.A

MD	21780	Sabillasville	NPS	NP.191.A
MD	20670	Patuxent River	USN	NY.001.A
MD	20670	Patuxent River	USN	NY.001.B
MD	21201	Baltimore	USCourts	UC.185.A
MD	20770	Greenbelt	USCourts	UC.186.A
MD	21201	Baltimore	USCourts	UC.359.A
MD	20770	Greenbelt	USCourts	UC.367.A
ME	04401	Bangor	ANG	AG.036.A
ME	04401	Bangor	ANG	AG.036.B
ME	04401	Bangor	ANG	AG.036.C
ME	04401	Bangor	ANG	AG.036.D
ME	04333	Augusta	ANG	AG.119.A
ME	04106	South Portland	ANG	AG.231.A
ME	04106	South Portland	ANG	AG.231.B
ME	04402	Bangor	DOJ	DJ.055.A
ME	04101	Portland	DOJ	DJ.056.A
ME	O2421	Portland	FAA	FA.083.A
ME	04609	Bar Harbor	NPS	NP.003.A
ME	04101	Portland	USCourts	UC.052.A
ME	04401	Bangor	USCourts	UC.217.A
ME	04401	Bangor	USCourts	UC.217.A
ME	04101	Portland	USCourts	UC.218.A
MI	48045	Harrison Township	USAF	AF.078.A
MI	48045	Harrison Township	USAF	AF.078.B
MI	48045	Selfridge AFB	ANG	AG.040.A
MI	48045	Selfridge AFB	ANG	AG.040.B
MI	48045	Selfridge AFB	ANG	AG.040.C
MI	48045	Selfridge AFB	ANG	AG.040.D
MI	49015	Battle Creek	ANG	AG.041.A
MI	49015	Battle Creek	ANG	AG.041.B
MI	49015	Battle Creek	ANG	AG.041.C
MI	49015	Battle Creek	ANG	AG.041.D
MI	49707	Alpena	ANG	AG.042.A
MI	49707	Alpena	ANG	AG.042.B
MI	49707	Alpena	ANG	AG.042.C
MI	49707	Alpena	ANG	AG.042.D
MI	48910	Lansing	ANG	AG.122.A
MI	48837	Grand Ledge	ARNG	AN.040.A
MI	48837	Grand Ledge	ARNG	AN.040.B
MI	48397	Warren	USA	AY.020.A
MI	48397	Warren	USA	AY.020.B
MI	49017	Battle Creek	DLA	DA.028.A
MI	48708	Bay City	DOJ	DJ.057.A
MI	48226	Detroit	DOJ	DJ.058.A
MI	49503	Grand Rapids	DOJ	DJ.059.A
MI	48502	Flint	DOJ	DJ.840.B
MI	48933	Lansing	DOJ	DJ.841.B
MI	48111	Belleville	FAA	FA.019.A
MI	48111	Belleville	FAA	FA.093.A
MI	49512	Grand Rapids	FAA	FA.110.A
MI	49855	Marquette	USF&W	FW.015.A
MI	49431	Ludington	USF&W	FW.017.A
MI	49630	Empire	NPS	NP.016.A
MI	49862	Munising	NPS	NP.044.A
MI	49862	Munising	NPS	NP.044.A
MI	49913	Calumet	NPS	NP.105.A
MI	48226	Detroit	USCourts	UC.078.A
MI	49503	Grand Rapids	USCourts	UC.079.A
MI	49007	Kalamazoo	USCourts	UC.187.A
MI	48933	Lansing	USCourts	UC.188.A
MI	49855	Marquette	USCourts	UC.189.A
MI	49855	Marquette	USCourts	UC.189.A
MI	49855	Marquette	USCourts	UC.189.B
MI	48502	Flint	USCourts	UC.200.A
MI	48107	Ann Arbor	USCourts	UC.353.A
MI	48107	Ann Arbor	USCourts	UC.353.B
MI	48107	Ann Arbor	USCourts	UC.353.C

MI	48075	Southfield	USCourts	UC.354.A
MI	48708	Bay City	USCourts	UC.355.A
MI	48708	Bay City	USCourts	UC.355.B
MI	49503	Grand Rapids	USCourts	UC.708.A
MN	55450	Minneapolis	USAF	AF.103.A
MN	55450	Minneapolis	USAF	AF.103.B
MN	55450	Minneapolis	USAF	AF.103.C
MN	55811	Duluth	ANG	AG.043.A
MN	55811	Duluth	ANG	AG.043.B
MN	55811	Duluth	ANG	AG.043.C
MN	55811	Duluth	ANG	AG.043.D
MN	55111	St Paul	ANG	AG.044.A
MN	55111	St Paul	ANG	AG.044.B
MN	55111	St Paul	ANG	AG.044.C
MN	55111	St Paul	ANG	AG.044.D
MN	55155	St Paul	ANG	AG.123.A
MN	55107	St Paul	ARNG	AN.041.A
MN	55107	St Paul	ARNG	AN.041.B
MN	55111	Fort Snelling	DLA	DA.021.A
MN	55415	Minneapolis	DOJ	DJ.842.B
MN	55024	Farmington	FAA	FA.016.A
MN	55024	Farmington	FAA	FA.016.B
MN	55450	Minneapolis	FAA	FA.080.A
MN	55425	Bloomington	FAA	FA.111.A
MN	55111	Fort Snelling	USF&W	FW.006.A
MN	56649-8904	International Falls	NPS	NP.045.A
MN	56649-8904	International Falls	NPS	NP.045.A
MN	55063	Pine City	NPS	NP.055.A
MN	55605	Grand Portage	NPS	NP.213.A
MN	55415	Minneapolis	USCourts	UC.091.A
MN	55415	Minneapolis	USCourts	UC.091.B
MN	55802	Duluth	USCourts	UC.092.A
MN	55101	St Paul	USCourts	UC.178.A
MO	65305	Whiteman AFB	USAF	AF.071.A
MO	65305	Whiteman AFB	USAF	AF.116.A
MO	65473	Fort Leonard Wood	USAF	AF.121.A
MO	64503	St Joseph	ANG	AG.048.A
MO	64503	St Joseph	ANG	AG.048.B
MO	64503	St Joseph	ANG	AG.048.C
MO	64503	St Joseph	ANG	AG.048.D
MO	63044	Bridgeton	ANG	AG.049.A
MO	63044	Bridgeton	ANG	AG.049.B
MO	63044	Bridgeton	ANG	AG.049.C
MO	63044	Bridgeton	ANG	AG.049.D
MO	65101	Jefferson City	ANG	AG.124.A
MO	63125	St Louis	ANG	AG.240.A
MO	63125	St Louis	ANG	AG.240.B
MO	65101	Jefferson City	ARNG	AN.042.A
MO	65101	Jefferson City	ARNG	AN.042.B
MO	63125	St Louis	USA	AY.011.A
MO	65473	Fort Leonard Wood	USA	AY.012.A
MO	63103	St Louis	DLA	DA.017.A
MO	63701	Cape Girardeau	DOJ	DJ.061.A
MO	65102	Jefferson City	DOJ	DJ.062.A
MO	65806	Springfield	DOJ	DJ.063.A
MO	64106	Kansas City	DOJ	DJ.843.B
MO	63102	St Louis	DOJ	DJ.844.B
MO	64106	Kansas City	FAA	FA.003.A
MO	64106	Kansas City	FAA	FA.003.B
MO	63074	St Ann	FAA	FA.005.A
MO	63965	Van Buren	NPS	NP.031.A
MO	65738	Republic	NPS	NP.034.A
MO	63102	St Louis	NPS	NP.115.A
MO	64840	Diamond	NPS	NP.170.A
MO	65101	Jefferson City	USCourts	UC.093.A
MO	65806	Springfield	USCourts	UC.094.A
MO	63102	St Louis	USCourts	UC.122.A

MO	63102	St Louis	USCourts	UC.122.B
MO	63102	St Louis	USCourts	UC.122.B
MO	64106	Kansas City	USCourts	UC.215.A
MO	63701	Cape Girardeau	USCourts	UC.320.A
MS	39710	Columbus AFB	USAF	AF.031.A
MS	39710	Columbus AFB	USAF	AF.031.B
MS	39534	Keesler AFB	USAF	AF.046.A
MS	39534	Keesler AFB	USAF	AF.046.B
MS	39534	Keesler AFB	USAF	AF.046.C
MS	39534	Keesler AFB	USAF	AF.090.A
MS	39534	Keesler AFB	USAF	AF.095.A
MS	39534	Keesler AFB	USAF	AF.126.A
MS	39534	Keesler AFB	USAF	AF.126.B
MS	39534	Keesler AFB	USAF	AF.KETV.A
MS	39534	Keesler AFB	USAF	AF.KETV.B
MS	39534	Keesler AFB	USAF	AF.KETV.C
MS	39507	Gulfport	ANG	AG.045.A
MS	39507	Gulfport	ANG	AG.045.B
MS	39507	Gulfport	ANG	AG.045.C
MS	39507	Gulfport	ANG	AG.045.D
MS	39208	Jackson	ANG	AG.046.A
MS	39208	Jackson	ANG	AG.046.A
MS	39307	Meridian	ANG	AG.047.A
MS	39307	Meridian	ANG	AG.047.A
MS	39307	Meridian	ANG	AG.047.B
MS	39307	Meridian	ANG	AG.047.C
MS	39307	Meridian	ANG	AG.047.D
MS	39202	Jackson	ANG	AG.126.A
MS	39202	Jackson	ANG	AG.126.A
MS	39208	Jackson	ANG	AG.126.B
MS	39208	Jackson	ANG	AG.126.C
MS	39208	Jackson	ANG	AG.126.D
MS	39209	Jackson	ARNG	AN.044.A
MS	39209	Jackson	ARNG	AN.044.B
MS	39501	Gulfport	DOJ	DJ.064.A
MS	39201	Jackson	DOJ	DJ.065.A
MS	38655	Oxford	DOJ	DJ.066.A
MS	39208	Jackson	FAA	FA.041.A
MS	38901	Grenada	USF&W	FW.016.A
MS	39183	Vicksburg	NPS	NP.046.A
MS	39564	Ocean Springs	NPS	NP.079.A
MS	39564	Ocean Springs	NPS	NP.079.A
MS	38804	Tupelo	NPS	NP.099.A
MS	39201	Jackson	USCourts	UC.132.A
MS	39730	Aberdeen	USCourts	UC.174.A
MS	38655	Oxford	USCourts	UC.235.A
MS	39501	Gulfport	USCourts	UC.271.A
MS	39401	Hattiesburg	USCourts	UC.272.A
MS	39201	Jackson	USCourts	UC.300.A
MS	39201	Jackson	USCourts	UC.300.B
MS	39201	Jackson	USCourts	UC.300.B
MS	39201	Jackson	USCourts	UC.300.B
MS	39201	Jackson	USCourts	UC.300.C
MS	38701	Greenville	USCourts	UC.347.A
MS	39730	Aberdeen	USCourts	UC.370.A
MT	59402	Malmstrom AFB	USAF	AF.052.A
MT	59402	Malmstrom AFB	USAF	AF.052.B
MT	59402	Malmstrom AFB	USAF	AF.052.C
MT	59404	Great Falls	ANG	AG.050.A
MT	59404	Great Falls	ANG	AG.050.A
MT	59404	Great Falls	ANG	AG.050.B
MT	59404	Great Falls	ANG	AG.050.C
MT	59404	Great Falls	ANG	AG.050.D
MT	59601	Helena	ANG	AG.125.A
MT	59604	Helena	ARNG	AN.045.A
MT	59604	Helena	ARNG	AN.045.B
MT	59101	Billings	DOJ	DJ.067.A

MT	59401	Great Falls	DOJ	DJ.068.A
MT	59601	Helena	DOJ	DJ.069.A
MT	59802	Missoula	DOJ	DJ.070.A
MT	59701	Butte	DOJ	DJ.845.B
MT	59602	Helena	FAA	FA.032.A
MT	59715	Bozeman	USF&W	FW.022.A
MT	59936	West Glacier	NPS	NP.033.A
MT	59761	Wisdom	NPS	NP.078.A
MT	59035	Yellowtail	NPS	NP.159.A
MT	59722	Deer Lodge	NPS	NP.200.A
MT	59703	Butte	USCourts	UC.179.A
MT	59801	Missoula	USCourts	UC.324.A
MT	59401	Great Falls	USCourts	UC.325.A
MT	59101	Billings	USCourts	UC.326.A
MT	59601	Helena	USCourts	UC.362.A
NC	28308	Pope AFB	USAF	AF.063.A
NC	28308	Pope AFB	USAF	AF.063.B
NC	27531	Seymour Johnson AFB	USAF	AF.065.A
NC	27531	Seymour Johnson AFB	USAF	AF.113.A
NC	27531	Seymour Johnson AFB	USAF	AF.113.B
NC	27531	Seymour Johnson AFB	USAF	AF.132.A
NC	27531	Seymour Johnson AFB	USAF	AF.133.A
NC	28308	Pope AFB	USAF	AF.145.A
NC	28308	Pope AFB	USAF	AF.145.A
NC	28208	Charlotte	ANG	AG.062.A
NC	28208	Charlotte	ANG	AG.062.B
NC	28208	Charlotte	ANG	AG.062.C
NC	28208	Charlotte	ANG	AG.062.D
NC	27607	Raleigh	ANG	AG.132.A
NC	28009	Badin	ANG	AG.235.A
NC	28009	Badin	ANG	AG.235.B
NC	27560	Morrisville	ARNG	AN.046.A
NC	27560	Morrisville	ARNG	AN.046.B
NC	28145	Salisbury	ARNG	AN.047.A
NC	28145	Salisbury	ARNG	AN.047.B
NC	28307	Fort Bragg	USA	AY.031.A
NC	28533	Cherry Point	DLA	DA.016.A
NC	28202	Charlotte	DOJ	DJ.071.A
NC	27401	Greensboro	DOJ	DJ.146.A
NC	28801	Asheville	DOJ	DJ.846.B
NC	27601	Raleigh	DOJ	DJ.848.B
NC	27101	Winston Salem	DOJ	DJ.849.B
NC	28273	Charlotte	FAA	FA.063.A
NC	27409	Greensboro	FAA	FA.064.A
NC	28531	Harkers Island	NPS	NP.070.A
NC	27954	Manteo	NPS	NP.071.A
NC	28803	Asheville	NPS	NP.162.A
NC	27410	Greensboro	NPS	NP.195.A
NC	28202	Charlotte	USCourts	UC.010.A
NC	27858	Greenville	USCourts	UC.065.A
NC	28401	Wilmington	USCourts	UC.066.A
NC	27893	Wilson	USCourts	UC.067.A
NC	27601	Raleigh	USCourts	UC.126.A
NC	27401	Greensboro	USCourts	UC.129.A
NC	27101	Winston Salem	USCourts	UC.130.A
NC	27401	Greensboro	USCourts	UC.131.A
NC	27602	Raleigh	USCourts	UC.236.A
NC	28601	Hickory	USCourts	UC.247.A
NC	28801	Asheville	USCourts	UC.248.A
NC	28801	Asheville	USCourts	UC.248.B
NC	28301	Fayetteville	USCourts	UC.265.A
NC	28202	Charlotte	USCourts	UC.365.A
NC	28677	Statesville	USCourts	UC.372.A
NC	28560	New Bern	USCourts	UC.711.A
ND	58204	Grand Forks AFB	USAF	AF.041.A
ND	58204	Grand Forks AFB	USAF	AF.041.B
ND	58705	Minot AFB	USAF	AF.056.A

ND	58102	Fargo	ANG	AG.063.A
ND	58102	Fargo	ANG	AG.063.B
ND	58102	Fargo	ANG	AG.063.C
ND	58102	Fargo	ANG	AG.063.D
ND	58506	Bismarck	ANG	AG.133.A
ND	58703	Minot	ANG	AG.236.A
ND	58703	Minot	ANG	AG.236.B
ND	58504	Bismarck	ARNG	AN.023.A
ND	58504	Bismarck	ARNG	AN.023.B
ND	58506	Bismarck	ARNG	AN.030.A
ND	58506	Bismarck	ARNG	AN.030.B
ND	58102	Fargo	DOJ	DJ.072.A
ND	58501	Bismarck	DOJ	DJ.171.A
ND	58504	Bismarck	FAA	FA.021.A
ND	58103	Fargo	FAA	FA.112.A
ND	58645	Medora	NPS	NP.047.A
ND	58571	Stanton	NPS	NP.125.A
ND	58501	Bismarck	USCourts	UC.096.A
ND	58102	Fargo	USCourts	UC.097.A
ND	58102	Fargo	USCourts	UC.097.B
NE	68113	Offutt AFB	USAF	AF.004.A
NE	68113	Offutt AFB	USAF	AF.004.B
NE	68524	Lincoln	ANG	AG.051.A
NE	68524	Lincoln	ANG	AG.051.A
NE	68524	Lincoln	ANG	AG.051.B
NE	68524	Lincoln	ANG	AG.051.C
NE	68524	Lincoln	ANG	AG.051.D
NE	68508	Lincoln	ANG	AG.127.A
NE	68524-1898	Lincoln	ARNG	AN.096.A
NE	68524-1898	Lincoln	ARNG	AN.096.B
NE	68508	Lincoln	ARNG	AN.703.A
NE	68508	Lincoln	ARNG	AN.703.B
NE	68102	Omaha	DOJ	DJ.073.A
NE	68508	Lincoln	DOJ	DJ.851.B
NE	68524	Lincoln	FAA	FA.071.A
NE	68102	Omaha	NPS	NP.036.A
NE	69341	Gering	NPS	NP.181.A
NE	69346	Harrison	NPS	NP.199.A
NE	68508	Lincoln	USCourts	UC.147.A
NE	68102	Omaha	USCourts	UC.148.A
NH	03803	Portsmouth	ANG	AG.053.A
NH	03803	Portsmouth	ANG	AG.053.A
NH	03803	Portsmouth	ANG	AG.053.B
NH	03803	Portsmouth	ANG	AG.053.C
NH	03803	Portsmouth	ANG	AG.053.D
NH	03301	Concord	ANG	AG.128.A
NH	03301	Concord	DOJ	DJ.008.A
NH	03062	Nashua	FAA	FA.024.A
NH	03062	Nashua	FAA	FA.024.B
NH	03062	Nashua	FAA	FA.074.A
NH	03062	Nashua	FAA	FA.074.B
NH	03745	Cornish	NPS	NP.048.A
NH	03301	Concord	USCourts	UC.053.A
NH	03101	Manchester	USCourts	UC.243.A
NJ	08641	McGuire AFB	USAF	AF.055.A
NJ	08641	McGuire AFB	USAF	AF.055.B
NJ	08640	Fort Dix	USAF	AF.072.A
NJ	08641	McGuire AFB	USAF	AF.102.A
NJ	08234	Egg Harbor Township	ANG	AG.054.A
NJ	08234	Egg Harbor Township	ANG	AG.054.A
NJ	08234	Egg Harbor Township	ANG	AG.054.B
NJ	08234	Egg Harbor Township	ANG	AG.054.B
NJ	08234	Egg Harbor Township	ANG	AG.054.C
NJ	08234	Egg Harbor Township	ANG	AG.054.D
NJ	08641	Trenton	ANG	AG.055.A
NJ	08641	Trenton	ANG	AG.055.B
NJ	08641	Trenton	ANG	AG.055.C

NJ	08641	Trenton	ANG	AG.055.D
NJ	08640	Trenton	ANG	AG.129.A
NJ	08640	Trenton	ANG	AG.129.A
NJ	08401	Atlantic City	ARNG	AN.049.A
NJ	08401	Atlantic City	ARNG	AN.049.B
NJ	08648	Lawrenceville	ARNG	AN.050.A
NJ	08648	Lawrenceville	ARNG	AN.050.B
NJ	08640	Fort Dix	ARNG	AN.051.A
NJ	07102	Newark	ARNG	AN.052.A
NJ	07102	Newark	ARNG	AN.052.B
NJ	08873	Somerset	ARNG	AN.053.A
NJ	08873	Somerset	ARNG	AN.053.B
NJ	07457	Riverdale	ARNG	AN.054.A
NJ	07457	Riverdale	ARNG	AN.054.B
NJ	08096	Woodbury	ARNG	AN.055.A
NJ	08096	Woodbury	ARNG	AN.055.B
NJ	08750	Sea Girt	ARNG	AN.056.A
NJ	08750	Sea Girt	ARNG	AN.056.B
NJ	08360	Vineland	ARNG	AN.057.A
NJ	08360	Vineland	ARNG	AN.057.B
NJ	08628	West Trenton	ARNG	AN.058.A
NJ	08628	West Trenton	ARNG	AN.058.B
NJ	07806	Picatinny	USA	AY.022.A
NJ	08640	Fort Dix	USA	AY.036.A
NJ	08608	Trenton	DOJ	DJ.006.A
NJ	08101	Camden	DOJ	DJ.147.A
NJ	O8405	Atlantic City	FAA	FA.011.A
NJ	08405	Atlantic City	FAA	FA.011.B
NJ	07102	Newark	FBI	FB.007.A
NJ	07052	West Orange	NPS	NP.151.A
NJ	08101	Camden	USCourts	UC.059.A
NJ	07102	Newark	USCourts	UC.060.A
NJ	07102	Newark	USCourts	UC.060.B
NJ	08608	Trenton	USCourts	UC.061.A
NJ	08608	Trenton	USCourts	UC.061.B
NJ	08101	Camden	USCourts	UC.301.A
NM	88330	Holloman AFB	USAF	AF.015.A
NM	88330	Holloman AFB	USAF	AF.015.B
NM	87117	Kirtland AFB	USAF	AF.019.A
NM	87117	Kirtland AFB	USAF	AF.019.B
NM	87117	Kirtland AFB	USAF	AF.019.C
NM	88103	Cannon AFB	USAF	AF.028.A
NM	88103	Cannon AFB	USAF	AF.028.B
NM	87117	Kirtland AFB	ANG	AG.056.A
NM	87117	Kirtland AFB	ANG	AG.056.A
NM	87117	Kirtland AFB	ANG	AG.056.B
NM	87117	Kirtland AFB	ANG	AG.056.C
NM	87117	Kirtland AFB	ANG	AG.056.D
NM	87505	Santa Fe	ANG	AG.134.A
NM	87747	Springer	ARNG	AN.060.A
NM	87747	Springer	ARNG	AN.060.B
NM	87505	Santa Fe	ARNG	AN.095.A
NM	87505	Santa Fe	ARNG	AN.095.B
NM	87102	Albuquerque	DOJ	DJ.075.A
NM	88011	Las Cruces	DOJ	DJ.076.A
NM	87109	Albuquerque	FAA	FA.047.A
NM	87109	Albuquerque	FAA	FA.047.B
NM	87106	Albuquerque	FAA	FA.113.A
NM	87102	Albuquerque	USF&W	FW.002.A
NM	87501	Santa Fe	NPS	NP.006.A
NM	87110	Albuquerque	NPS	NP.116.A
NM	88310	Alamogordo	NPS	NP.128.A
NM	88220	Carlsbad	NPS	NP.153.A
NM	87410	Aztec	NPS	NP.155.A
NM	87544	Los Alamos	NPS	NP.158.A
NM	87552	Pecos	NPS	NP.177.A
NM	88414	Capulin	NPS	NP.201.A

NM	87020	Grants	NPS	NP.202.A
NM	87102	Albuquerque	USCourts	UC.111.A
NM	88001	Las Cruces	USCourts	UC.256.A
NM	88001	Las Cruces	USCourts	UC.361.A
NM	87102	Albuquerque	USCourts	UC.369.A
NV	89191	Nellis AFB	USAF	AF.059.A
NV	89191	Nellis AFB	USAF	AF.059.B
NV	89502	Reno	ANG	AG.052.A
NV	89502	Reno	ANG	AG.052.B
NV	89502	Reno	ANG	AG.052.C
NV	89502	Reno	ANG	AG.052.D
NV	89701	Carson City	ANG	AG.130.A
NV	89501	Reno	DOJ	DJ.078.A
NV	90815	Las Vegas	FAA	FA.056.A
NV	89502	Reno	FAA	FA.088.A
NV	89119	Las Vegas	FAA	FA.114.A
NV	89005	Boulder City	NPS	NP.143.A
NV	89311	Baker	NPS	NP.147.A
NV	89005	Boulder City	NPS	NP.150.A
NV	89101	Las Vegas	USCourts	UC.102.A
NV	89501	Reno	USCourts	UC.168.A
NV	89101	Las Vegas	USCourts	UC.329.A
NV	89101	Las Vegas	USCourts	UC.351.A
NV	89101	Las Vegas	USCourts	UC.351.B
NY	13441	Rome	USAF	AF.042.A
NY	14304	Niagara Falls	USAF	AF.106.A
NY	14304	Niagara Falls	USAF	AF.106.B
NY	14304	Niagara Falls	USAF	AF.106.C
NY	11978	Westhampton Beach	ANG	AG.057.A
NY	11978	Westhampton Beach	ANG	AG.057.B
NY	11978	Westhampton Beach	ANG	AG.057.C
NY	11978	Westhampton Beach	ANG	AG.057.D
NY	14304	Niagara Falls	ANG	AG.058.A
NY	14304	Niagara Falls	ANG	AG.058.B
NY	14304	Niagara Falls	ANG	AG.058.C
NY	14304	Niagara Falls	ANG	AG.058.D
NY	12302	Schenectady	ANG	AG.059.A
NY	12302	Schenectady	ANG	AG.059.A
NY	12302	Schenectady	ANG	AG.059.A
NY	12302	Schenectady	ANG	AG.059.B
NY	12302	Schenectady	ANG	AG.059.C
NY	12302	Schenectady	ANG	AG.059.D
NY	13211	Syracuse	ANG	AG.060.A
NY	13211	Syracuse	ANG	AG.060.B
NY	13211	Syracuse	ANG	AG.060.C
NY	13211	Syracuse	ANG	AG.060.D
NY	12550	Newburgh	ANG	AG.061.A
NY	12550	Newburgh	ANG	AG.061.B
NY	12550	Newburgh	ANG	AG.061.C
NY	12550	Newburgh	ANG	AG.061.D
NY	13441	Rome	ANG	AG.096.A
NY	13441	Rome	ANG	AG.096.B
NY	13441	Rome	ANG	AG.096.C
NY	13441	Rome	ANG	AG.096.D
NY	12110	Latham	ANG	AG.131.A
NY	12110	Latham	ARNG	AN.061.A
NY	12110	Latham	ARNG	AN.061.B
NY	14624	Rochester	ARNG	AN.062.A
NY	14624	Rochester	ARNG	AN.062.B
NY	11779	Ronkonkoma	ARNG	AN.063.A
NY	11779	Ronkonkoma	ARNG	AN.063.B
NY	11530	Garden City	DLA	DA.003.A
NY	11973	Upton	DOE	DE.020.A
NY	11973	Upton	DOE	DE.020.B
NY	11201	Brooklyn	DOJ	DJ.079.A
NY	14202	Buffalo	DOJ	DJ.080.1
NY	10007	New York	DOJ	DJ.083.A

NY	11201	Brooklyn	DOJ	DJ.160.A
NY	10007	New York	DOJ	DJ.174.A
NY	11722	Central Islip	DOJ	DJ.805.1
NY	12207	Albany	DOJ	DJ.856.B
NY	14614	Rochester	DOJ	DJ.858.B
NY	13261	Syracuse	DOJ	DJ.859.B
NY	10601	White Plains	DOJ	DJ.860.B
NY	11434	Jamaica	FAA	FA.008.A
NY	11434	Jamaica	FAA	FA.008.B
NY	11779	Ronkonkoma	FAA	FA.009.A
NY	11779	Ronkonkoma	FAA	FA.009.B
NY	11530	Garden City	FAA	FA.010.A
NY	11590	Westbury	FAA	FA.070.A
NY	11590	Westbury	FAA	FA.070.B
NY	12110	Latham	FAA	FA.078.A
NY	14626	Rochester	FAA	FA.079.A
NY	11735	Farmingdale	FAA	FA.115.A
NY	10305	Staten Island	NPS	NP.013.A
NY	12538	Hyde Park	NPS	NP.019.A
NY	12106	Kinderhook	NPS	NP.023.A
NY	11771	Oyster Bay	NPS	NP.144.A
NY	13440	Rome	NPS	NP.152.A
NY	13440	Rome	NPS	NP.152.A
NY	12170	Stillwater	NPS	NP.180.A
NY	13148	Seneca Falls	NPS	NP.187.A
NY	10004	New York	NPS	NP.215.A
NY	10305	Staten Island	NPS	NP.230.A
NY	11234	Brooklyn	NPS	NP.231.A
NY	14202	Buffalo	USCourts	UC.056.A
NY	13261	Syracuse	USCourts	UC.143.A
NY	10007	New York	USCourts	UC.156.A
NY	10007	New York	USCourts	UC.156.B
NY	10007	New York	USCourts	UC.156.C
NY	10004	New York	USCourts	UC.161.A
NY	12207	Albany	USCourts	UC.169.A
NY	12207	Albany	USCourts	UC.169.B
NY	12207	Albany	USCourts	UC.169.C
NY	10601	White Plains	USCourts	UC.170.A
NY	10601	White Plains	USCourts	UC.170.B
NY	13502	Utica	USCourts	UC.176.A
NY	10278	New York	USCourts	UC.224.A
NY	10278	New York	USCourts	UC.224.B
NY	11201	Brooklyn	USCourts	UC.241.A
NY	11201	Brooklyn	USCourts	UC.241.B
NY	13901	Binghamton	USCourts	UC.242.A
NY	14614	Rochester	USCourts	UC.250.A
NY	11201	Brooklyn	USCourts	UC.252.A
NY	11201	Brooklyn	USCourts	UC.252.A
NY	11201	Brooklyn	USCourts	UC.252.B
NY	11201	Brooklyn	USCourts	UC.252.C
NY	11722	Central Islip	USCourts	UC.319.A
NY	12601	Poughkeepsie	USCourts	UC.373.A
NY	11201	Brooklyn	USCourts	UC.375.A
OH	45433	Wright Patterson AFB	USAF	AF.017.A
OH	45433	Wright Patterson AFB	USAF	AF.017.B
OH	45433	Wright Patterson AFB	USAF	AF.017.C
OH	45433	Wright Patterson AFB	USAF	AF.017.D
OH	43056	Heath	USAF	AF.061.A
OH	44473	Youngstown AFB	USAF	AF.077.A
OH	44473	Youngstown AFB	USAF	AF.077.B
OH	44473	Youngstown AFB	USAF	AF.077.C
OH	45433	Wright Patterson AFB	USAF	AF.118.A
OH	45433	Wright Patterson AFB	USAF	AF.118.B
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.A
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.B
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.C
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.D

OH	45433	Wright Patterson AFB	USAF	AF.ATNO.E
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.F
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.G
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.H
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.I
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.J
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.K
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.L
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.M
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.N
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.O
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.Q
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.R
OH	45433	Wright Patterson AFB	USAF	AF.ATNO.S
OH	43217	Columbus	ANG	AG.064.A
OH	43217	Columbus	ANG	AG.064.B
OH	43217	Columbus	ANG	AG.064.C
OH	43217	Columbus	ANG	AG.064.D
OH	44903	Mansfield	ANG	AG.065.A
OH	44903	Mansfield	ANG	AG.065.B
OH	44903	Mansfield	ANG	AG.065.C
OH	44903	Mansfield	ANG	AG.065.D
OH	45502	Springfield	ANG	AG.066.A
OH	45502	Springfield	ANG	AG.066.A
OH	45502	Springfield	ANG	AG.066.B
OH	45502	Springfield	ANG	AG.066.C
OH	45502	Springfield	ANG	AG.066.D
OH	43558	Swanton	ANG	AG.067.A
OH	43558	Swanton	ANG	AG.067.B
OH	43558	Swanton	ANG	AG.067.C
OH	43558	Swanton	ANG	AG.067.D
OH	43235	Columbus	ANG	AG.135.A
OH	45242	Cincinnati	ANG	AG.237.A
OH	45242	Cincinnati	ANG	AG.237.B
OH	43452	Port Clinton	ANG	AG.238.A
OH	43452	Port Clinton	ANG	AG.238.B
OH	43701	Zanesville	ANG	AG.239.A
OH	43701	Zanesville	ANG	AG.239.B
OH	43217	Columbus	ARNG	AN.064.A
OH	43217	Columbus	ARNG	AN.064.B
OH	44720	Canton	ARNG	AN.065.A
OH	44720	Canton	ARNG	AN.065.B
OH	43219	Columbus	DLA	DA.006.A
OH	45433	Dayton	DLA	DA.008.A
OH	44108	Cleveland	DLA	DA.023.A
OH	45202	Cincinnati	DOJ	DJ.010.A
OH	43215	Columbus	DOJ	DJ.085.A
OH	43604	Toledo	DOJ	DJ.086.A
OH	44503	Youngstown	DOJ	DJ.087.A
OH	44114	Cleveland	DOJ	DJ.103.A
OH	44308	Akron	DOJ	DJ.861.B
OH	45402	Dayton	DOJ	DJ.863.B
OH	44074	Oberlin	FAA	FA.018.A
OH	44074	Oberlin	FAA	FA.018.B
OH	43219	Columbus	FAA	FA.020.A
OH	45245	Cincinnati	FAA	FA.060.A
OH	44070	North Olmsted	FAA	FA.116.A
OH	43456	Put In Bay	NPS	NP.049.A
OH	44264	Peninsula	NPS	NP.111.A
OH	45402	Dayton	NPS	NP.165.A
OH	45202	Cincinnati	USCourts	UC.011.A
OH	44503	Youngstown	USCourts	UC.080.A
OH	43624	Toledo	USCourts	UC.081.A
OH	44308	Akron	USCourts	UC.082.A
OH	44702	Canton	USCourts	UC.083.A
OH	44114	Cleveland	USCourts	UC.084.A

OH	44114	Cleveland	USCourts	UC.084.B
OH	43215	Columbus	USCourts	UC.085.A
OH	45402	Dayton	USCourts	UC.087.A
OH	45402	Dayton	USCourts	UC.303.A
OH	45202	Cincinnati	USCourts	UC.304.A
OH	43215	Columbus	USCourts	UC.305.A
OH	44501	Youngstown	USCourts	UC.360.A
OH	44114	Cleveland	USCourts	UC.802.B
OK	73145	Tinker AFB	USAF	AF.014.A
OK	73145	Tinker AFB	USAF	AF.014.B
OK	73523	Altus AFB	USAF	AF.024.A
OK	73523	Altus AFB	USAF	AF.024.B
OK	73705	Vance AFB	USAF	AF.070.A
OK	73705	Vance AFB	USAF	AF.070.B
OK	73145	Tinker AFB	USAF	AF.076.A
OK	73145	Tinker AFB	USAF	AF.076.B
OK	73145	Tinker AFB	USAF	AF.076.C
OK	73179	Oklahoma City	ANG	AG.068.A
OK	73179	Oklahoma City	ANG	AG.068.B
OK	73179	Oklahoma City	ANG	AG.068.C
OK	73179	Oklahoma City	ANG	AG.068.D
OK	74115	Tulsa	ANG	AG.069.A
OK	74115	Tulsa	ANG	AG.069.B
OK	74115	Tulsa	ANG	AG.069.C
OK	74115	Tulsa	ANG	AG.069.D
OK	73111	Oklahoma City	ANG	AG.136.A
OK	74501	McAlester	USA	AY.068.A
OK	73145	Oklahoma City	DLA	DA.029.A
OK	74401	Muskogee	DOJ	DJ.088.A
OK	73102	Oklahoma City	DOJ	DJ.089.A
OK	74119	Tulsa	DOJ	DJ.179.A
OK	73169	Oklahoma City	FAA	FA.001.A
OK	73086	Sulphur	NPS	NP.072.A
OK	74103	Tulsa	USCourts	UC.012.A
OK	73102	Oklahoma City	USCourts	UC.013.A
OK	74401	Muskogee	USCourts	UC.221.A
OK	74401	Muskogee	USCourts	UC.221.A
OK	74103	Tulsa	USCourts	UC.296.A
OK	74447	Okmulgee	USCourts	UC.328.A
OR	97218	Portland	USAF	AF.110.A
OR	97218	Portland	USAF	AF.110.B
OR	97603	Klamath Falls	ANG	AG.070.A
OR	97603	Klamath Falls	ANG	AG.070.A
OR	97603	Klamath Falls	ANG	AG.070.B
OR	97603	Klamath Falls	ANG	AG.070.C
OR	97603	Klamath Falls	ANG	AG.070.D
OR	97218	Portland	ANG	AG.071.A
OR	97218	Portland	ANG	AG.071.A
OR	97218	Portland	ANG	AG.071.B
OR	97218	Portland	ANG	AG.071.C
OR	97218	Portland	ANG	AG.071.D
OR	97309	Salem	ANG	AG.137.A
OR	97146	Warrenton	ANG	AG.241.A
OR	97146	Warrenton	ANG	AG.241.B
OR	97838	Hermiston	USA	AY.002.A
OR	97401	Eugene	DOJ	DJ.090.A
OR	97401	Eugene	DOJ	DJ.090.A
OR	97501	Medford	DOJ	DJ.155.A
OR	97204	Portland	DOJ	DJ.866.B
OR	97124	Hillsboro	FAA	FA.031.A
OR	97232	Portland	USF&W	FW.005.A
OR	97520	Ashland	USF&W	FW.012.A
OR	97848	Kimberly	NPS	NP.022.A
OR	97103	Astoria	NPS	NP.174.A
OR	97523	Cave Junction	NPS	NP.197.A
OR	97604	Crater Lake	NPS	NP.209.A

OR	97204	Portland	USCourts	UC.103.A
OR	97204	Portland	USCourts	UC.105.A
OR	97204	Portland	USCourts	UC.105.B
OR	97204	Portland	USCourts	UC.105.C
OR	97204	Portland	USCourts	UC.310.A
OR	97501	Medford	USCourts	UC.315.A
PA	15108	Coraopolis	USAF	AF.109.A
PA	15108	Coraopolis	USAF	AF.109.B
PA	15108	Coraopolis	USAF	AF.109.C
PA	15108	Coraopolis	USAF	AF.109.D
PA	15108	Coraopolis	USAF	AF.109.D
PA	19090	Willow Grove	USAF	AF.117.A
PA	19090	Willow Grove	USAF	AF.146.A
PA	15108	Coraopolis	ANG	AG.072.A
PA	15108	Coraopolis	ANG	AG.072.B
PA	15108	Coraopolis	ANG	AG.072.C
PA	15108	Coraopolis	ANG	AG.072.D
PA	15108	Coraopolis	ANG	AG.072.D
PA	19090	Willow Grove	ANG	AG.073.A
PA	19090	Willow Grove	ANG	AG.073.B
PA	19090	Willow Grove	ANG	AG.073.C
PA	19090	Willow Grove	ANG	AG.073.D
PA	17057	Middletown	ANG	AG.074.A
PA	17057	Middletown	ANG	AG.074.A
PA	17057	Middletown	ANG	AG.074.B
PA	17057	Middletown	ANG	AG.074.C
PA	17057	Middletown	ANG	AG.074.D
PA	17003	Annville	ANG	AG.138.A
PA	17003	Annville	ANG	AG.208.A
PA	17003	Annville	ANG	AG.208.B
PA	16803	State College	ANG	AG.242.A
PA	16803	State College	ANG	AG.242.B
PA	15904	Johnstown	ANG	AG.262.A
PA	17003	Annville	ARNG	AN.067.A
PA	17003	Annville	ARNG	AN.067.B
PA	17003	Annville	ARNG	AN.068.A
PA	17003	Annville	ARNG	AN.068.B
PA	17003	Annville	ARNG	AN.069.A
PA	17003	Annville	ARNG	AN.069.B
PA	17033	Hershey	ARNG	AN.071.A
PA	19154	Philadelphia	ARNG	AN.072.A
PA	19154	Philadelphia	ARNG	AN.072.B
PA	18510	Scranton	ARNG	AN.073.A
PA	18510	Scranton	ARNG	AN.073.B
PA	15301	Washington	ARNG	AN.074.A
PA	15301	Washington	ARNG	AN.074.B
PA	15902	Johnstown	ARNG	AN.094.A
PA	15902	Johnstown	ARNG	AN.094.B
PA	19111	Philadelphia	DLA	DA.001.A
PA	17070	New Cumberland	DLA	DA.004.A
PA	17070	New Cumberland	DLA	DA.004.A
PA	18466	Tobyhanna	DLA	DA.014.A
PA	17070	New Cumberland	DLA	DA.041.A
PA	15122	West Mifflin	DOE	DE.040.A
PA	15901-1622	Johnstown	DOJ	DI.800.B
PA	16501	Erie	DOJ	DJ.091.A
PA	15901	Johnstown	DOJ	DJ.092.A
PA	19106	Philadelphia	DOJ	DJ.093.A
PA	15219	Pittsburgh	DOJ	DJ.170.A
PA	17108	Harrisburg	DOJ	DJ.867.B
PA	18501	Scranton	DOJ	DJ.869.B
PA	17701	Williamsport	DOJ	DJ.870.B
PA	19113	Philadelphia	FAA	FA.117.A
PA	15227	Pittsburgh	FAA	FA.118.A
PA	17070	New Cumberland	FAA	FA.119.A
PA	18109	Allentown	FAA	FA.120.A
PA	15108	Coraopolis	FAA	FA.121.A

PA	19106	Phiiladelphia	FBI	FB.005.A
PA	19106	Philadelphia	NPS	NP.028.A
PA	18324	Bushkill	NPS	NP.050.A
PA	16641	Gallitzin	NPS	NP.093.A
PA	19106	Philadelphia	NPS	NP.102.A
PA	18503	Scranton	NPS	NP.145.A
PA	18405	Beach Lake	NPS	NP.207.A
PA	19520	Elverson	NPS	NP.210.A
PA	19113	Lester	USN	NY.003.A
PA	19113	Lester	USN	NY.003.B
PA	19113	Lester	USN	NY.003.C
PA	19106	Philadelphia	USCourts	UC.014.A
PA	16501	Erie	USCourts	UC.063.A
PA	15219	Pittsburgh	USCourts	UC.064.A
PA	17108	Harrisburg	USCourts	UC.157.A
PA	18503	Scranton	USCourts	UC.158.A
PA	17701	Williamsport	USCourts	UC.159.A
PA	19197	Philadelphia	USCourts	UC.206.A
PA	18701	Wilkes Barre	USCourts	UC.216.A
PA	15219	Pittsburgh	USCourts	UC.226.A
PA	15219	Pittsburgh	USCourts	UC.364.A
PR	00979	Carolina	ANG	AG.075.A
PR	00979	Carolina	ANG	AG.075.B
PR	00979	Carolina	ANG	AG.075.C
PR	00979	Carolina	ANG	AG.075.D
PR	00915	San Juan	ANG	AG.139.A
PR	00949	Toa Baja	ANG	AG.243.A
PR	00949	Toa Baja	ANG	AG.243.B
PR	00603	Aguadilla	ANG	AG.244.A
PR	00603	Aguadilla	ANG	AG.244.B
PR	00918	San Juan	DOJ	DJ.154.A
PR	00979	Carolina	FAA	FA.039.A
PR	00918	San Juan	FAA	FA.122.A
PR	00901	San Juan	NPS	NP.179.A
PR	00918	Hato Rey	USCourts	UC.054.A
PR	000901	San Juan	USCourts	UC.294.A
PR	000901	San Juan	USCourts	UC.294.B
RI	02852	North Kingstown	ANG	AG.076.A
RI	02852	North Kingstown	ANG	AG.076.B
RI	02852	North Kingstown	ANG	AG.076.C
RI	02852	North Kingstown	ANG	AG.076.D
RI	02920	Cranston	ANG	AG.140.A
RI	02896	North Smithfield	ANG	AG.245.A
RI	02896	North Smithfield	ANG	AG.245.B
RI	02816	Coventry	ANG	AG.246.A
RI	02816	Coventry	ANG	AG.246.B
RI	02852	North Kingstown	ARNG	AN.075.A
RI	02852	North Kingstown	ARNG	AN.075.B
RI	02886	Warwick	USCG	CG.011.A
RI	02903	Providence	DOJ	DJ.094.A
RI	02841	Newport	USN	NY.002.A
RI	02903	Providence	USCourts	UC.015.A
RI	02903	Providence	USCourts	UC.219.A
SC	29404	Charleston AFB	USAF	AF.029.A
SC	29404	Charleston AFB	USAF	AF.029.B
SC	29152	Shaw AFB	USAF	AF.066.A
SC	29404	Charleston AFB	USAF	AF.087.A
SC	29605	Greenville	USAF	AF.144.A
SC	29044	Eastover	ANG	AG.077.A
SC	29044	Eastover	ANG	AG.077.A
SC	29044	Eastover	ANG	AG.077.B
SC	29044	Eastover	ANG	AG.077.C
SC	29044	Eastover	ANG	AG.077.D
SC	29201	Columbia	ANG	AG.141.A
SC	29207	Fort Jackson	USA	AY.009.A
SC	29401	Charleston	DOJ	DJ.095.A
SC	29201	Columbia	DOJ	DJ.096.A

SC	29201	Columbia	DOJ	DJ.096.B
SC	29201	Columbia	DOJ	DJ.097.A
SC	29201	Columbia	DOJ	DJ.097.B
SC	29201	Columbia	DOJ	DJ.098.A
SC	29601	Greenville	DOJ	DJ.099.A
SC	29201	Columbia	DOJ	DJ.164.A
SC	29501	Florence	DOJ	DJ.872.B
SC	29201	Columbia	DOJ	DJ.999.B
SC	29170	West Columbia	FAA	FA.067.A
SC	29210	Columbia	FBI	FB.002.A
SC	29482	Sullivans Island	NPS	NP.035.A
SC	29341	Gaffney	NPS	NP.066.A
SC	29061	Hopkins	NPS	NP.120.A
SC	29210	Columbia	USSS	SS.001.A
SC	29210	Columbia	USSS	SS.001.B
SC	29201	Columbia	USCourts	UC.068.A
SC	29501	Florence	USCourts	UC.291.A
SC	29401	Charleston	USCourts	UC.323.A
SC	29601	Greenville	USCourts	UC.350.A
SC	29201	Columbia	USCourts	UC.358.A
SD	57706	Ellsworth AFB	USAF	AF.036.A
SD	57706	Ellsworth AFB	USAF	AF.036.B
SD	57104	Sioux Falls	ANG	AG.078.A
SD	57104	Sioux Falls	ANG	AG.078.A
SD	57104	Sioux Falls	ANG	AG.078.B
SD	57104	Sioux Falls	ANG	AG.078.C
SD	57104	Sioux Falls	ANG	AG.078.D
SD	57702	Rapid City	ANG	AG.142.A
SD	57104	Sioux Falls	DOJ	DJ.100.A
SD	57501	Pierre	DOJ	DJ.873.B
SD	57709	Rapid City	DOJ	DJ.874.B
SD	55450	Rapid City	FAA	FA.081.A
SD	57750	Interior	NPS	NP.020.A
SD	57747	Hot Springs	NPS	NP.064.A
SD	57751	Keystone	NPS	NP.205.A
SD	57501	Pierre	USCourts	UC.098.A
SD	57104	Sioux Falls	USCourts	UC.099.A
SD	57701	Rapid City	USCourts	UC.100.A
SD	57401	Aberdeen	USCourts	UC.279.A
TN	37389	Arnold AFB	USAF	AF.001.A
TN	37389	Arnold AFB	USAF	AF.001.B
TN	37777	Louisville	ANG	AG.079.A
TN	37777	Louisville	ANG	AG.079.B
TN	37777	Louisville	ANG	AG.079.C
TN	37777	Louisville	ANG	AG.079.D
TN	38118	Memphis	ANG	AG.080.A
TN	38118	Memphis	ANG	AG.080.B
TN	38118	Memphis	ANG	AG.080.C
TN	38118	Memphis	ANG	AG.080.D
TN	37217	Nashville	ANG	AG.081.A
TN	37217	Nashville	ANG	AG.081.B
TN	37217	Nashville	ANG	AG.081.C
TN	37217	Nashville	ANG	AG.081.D
TN	37777	Louisville	ANG	AG.099.A
TN	37777	Louisville	ANG	AG.099.A
TN	37777	Louisville	ANG	AG.099.B
TN	37777	Louisville	ANG	AG.099.C
TN	37204	Nashville	ANG	AG.143.A
TN	37421	Chattanooga	ANG	AG.247.A
TN	37421	Chattanooga	ANG	AG.247.B
TN	37167	Smyrna	ARNG	AN.076.A
TN	37167	Smyrna	ARNG	AN.076.B
TN	37402	Chattanooga	DOJ	DJ.101.A
TN	37604	Johnson City	DOJ	DJ.104.A
TN	38103	Memphis	DOJ	DJ.169.A
TN	37902	Knoxville	DOJ	DJ.875.B
TN	37203	Nashville	DOJ	DJ.877.B

TN	37743	Greeneville	DOJ	DJ.900.B
TN	38118	Memphis	FAA	FA.038.A
TN	38118	Memphis	FAA	FA.038.B
TN	37217	Nashville	FAA	FA.040.A
TN	38116	Memphis	FAA	FA.043.A
TN	37841	Oneida	NPS	NP.026.A
TN	37738	Gatlinburg	NPS	NP.086.A
TN	37743	Greeneville	NPS	NP.156.A
TN	37058	Dover	NPS	NP.193.A
TN	37129	Murfreesboro	NPS	NP.198.A
TN	37902	Knoxville	USCourts	UC.088.A
TN	37203	Nashville	USCourts	UC.089.A
TN	38103	Memphis	USCourts	UC.134.A
TN	38103	Memphis	USCourts	UC.149.A
TN	37402	Chattanooga	USCourts	UC.172.A
TN	38301	Jackson	USCourts	UC.191.A
TN	37402	Chattanooga	USCourts	UC.222.A
TN	37402	Chattanooga	USCourts	UC.222.B
TN	37743	Greeneville	USCourts	UC.225.A
TN	37743	Greeneville	USCourts	UC.228.A
TN	37902	Knoxville	USCourts	UC.285.A
TX	78150	Randolph AFB	USAF	AF.005.A
TX	78150	Randolph AFB	USAF	AF.005.A
TX	78150	Randolph AFB	USAF	AF.005.B
TX	78236	Lackland AFB	USAF	AF.011.A
TX	78236	Lackland AFB	USAF	AF.011.B
TX	78235	Brooks AFB	USAF	AF.016.A
TX	78235	Brooks AFB	USAF	AF.016.B
TX	79607	Dyess AFB	USAF	AF.034.A
TX	76908	Goodfellow AFB	USAF	AF.040.A
TX	76908	Goodfellow AFB	USAF	AF.040.B
TX	78236	Lackland AFB	USAF	AF.047.A
TX	78236	Lackland AFB	USAF	AF.047.A
TX	78236	Lackland AFB	USAF	AF.047.B
TX	78840	Laughlin AFB	USAF	AF.048.A
TX	78840	Laughlin AFB	USAF	AF.048.B
TX	76311	Sheppard AFB	USAF	AF.067.A
TX	76311	Sheppard AFB	USAF	AF.067.B
TX	78236	Lackland AFB	USAF	AF.096.A
TX	76127	Fort Worth	USAF	AF.104.A
TX	76127	Fort Worth	USAF	AF.104.B
TX	76127	Fort Worth	USAF	AF.104.C
TX	78257	San Antonio	USAF	AF.119.A
TX	78236	Lackland AFB	USAF	AF.128.A
TX	78236	Lackland AFB	USAF	AF.130.A
TX	78236	Lackland AFB	USAF	AF.130.B
TX	76311	Sheppard AFB	USAF	AF.SITV.A
TX	76311	Sheppard AFB	USAF	AF.SITV.A
TX	76311	Sheppard AFB	USAF	AF.SITV.B
TX	76117	Fort Worth	ANG	AG.082.A
TX	76117	Fort Worth	ANG	AG.082.A
TX	76117	Fort Worth	ANG	AG.082.B
TX	76117	Fort Worth	ANG	AG.082.C
TX	76117	Fort Worth	ANG	AG.082.D
TX	77034	Houston	ANG	AG.083.A
TX	77034	Houston	ANG	AG.083.B
TX	77034	Houston	ANG	AG.083.C
TX	77034	Houston	ANG	AG.083.D
TX	78241	San Antonio	ANG	AG.084.A
TX	78241	San Antonio	ANG	AG.084.A
TX	78241	San Antonio	ANG	AG.084.B
TX	78241	San Antonio	ANG	AG.084.C
TX	78241	San Antonio	ANG	AG.084.D
TX	78241	San Antonio	ANG	AG.084.E
TX	78703	Austin	ANG	AG.144.A
TX	75046	Garland	ANG	AG.248.A
TX	75046	Garland	ANG	AG.248.B

TX	77571	La Porte	ANG	AG.249.A
TX	77571	La Porte	ANG	AG.249.B
TX	77705	Beaumont	ANG	AG.250.A
TX	77705	Beaumont	ANG	AG.250.B
TX	78719	Austin	ARNG	AN.077.A
TX	78719	Austin	ARNG	AN.077.B
TX	78763	Austin	ARNG	AN.078.A
TX	78763	Austin	ARNG	AN.078.B
TX	78763	Austin	ARNG	AN.079.A
TX	78763	Austin	ARNG	AN.079.B
TX	78602	Bastrop	ARNG	AN.080.A
TX	78602	Bastrop	ARNG	AN.080.B
TX	75237	Dallas	ARNG	AN.082.A
TX	75237	Dallas	ARNG	AN.082.B
TX	75237	Dallas	ARNG	AN.083.A
TX	75237	Dallas	ARNG	AN.083.B
TX	77034	Houston	ARNG	AN.084.A
TX	77034	Houston	ARNG	AN.084.B
TX	76067	Mineral Wells	ARNG	AN.085.A
TX	76067	Mineral Wells	ARNG	AN.085.B
TX	75473	Powderly	ARNG	AN.086.A
TX	75473	Powderly	ARNG	AN.086.B
TX	78218	San Antonio	ARNG	AN.087.A
TX	78218	San Antonio	ARNG	AN.087.B
TX	76108	Fort Worth	ARNG	AN.088.A
TX	76108	Fort Worth	ARNG	AN.088.B
TX	78596	Weslaco	ARNG	AN.089.A
TX	78596	Weslaco	ARNG	AN.089.B
TX	75507	Texarkana	USA	AY.019.A
TX	78419	Corpus Christi	USA	AY.024.A
TX	79916	Fort Bliss	USA	AY.032.A
TX	78234	Fort Sam Houston	USA	AY.048.A
TX	78234	Fort Sam Houston	USA	AY.093.A
TX	78234	San Antonio	DLA	DA.026.A
TX	75507	Texarkana	DLA	DA.031.A
TX	78419	Corpus Christi	DLA	DA.033.A
TX	75201	Dallas	DLA	DA.038.A
TX	79101	Amarillo	DOJ	DJ.106.A
TX	78701	Austin	DOJ	DJ.107.A
TX	77701	Beaumont	DOJ	DJ.108.A
TX	79901	El Paso	DOJ	DJ.110.A
TX	79901	El Paso	DOJ	DJ.110.A
TX	76102	Fort Worth	DOJ	DJ.111.A
TX	77002	Houston	DOJ	DJ.112.A
TX	78040	Laredo	DOJ	DJ.113.A
TX	79702	Midland	DOJ	DJ.115.A
TX	78216	San Antonio	DOJ	DJ.117.A
TX	78216	San Antonio	DOJ	DJ.117.A
TX	75090	Sherman	DOJ	DJ.118.A
TX	75702	Tyler	DOJ	DJ.119.A
TX	76706	Waco	DOJ	DJ.120.A
TX	75901	Lufkin	DOJ	DJ.150.A
TX	77901	Victoria	DOJ	DJ.173.A
TX	79830	Alpine	DOJ	DJ.181.A
TX	79830	Alpine	DOJ	DJ.181.A
TX	75074	Plano	DOJ	DJ.184.A
TX	78520	Brownsville	DOJ	DJ.878.B
TX	75242	Dallas	DOJ	DJ.879.B
TX	78840	Del Rio	DOJ	DJ.880.B
TX	79401	Lubbock	DOJ	DJ.881.B
TX	78501	McAllen	DOJ	DJ.883.B
TX	75501	Texarkana	DOJ	DJ.885.B
TX	76137	Fort Worth	FAA	FA.044.A
TX	76137	Fort Worth	FAA	FA.044.B
TX	76155	Fort Worth	FAA	FA.045.A
TX	76155	Fort Worth	FAA	FA.045.B
TX	77032	Houston	FAA	FA.046.A

TX	77032	Houston	FAA	FA.046.B
TX	78216	San Antonio	FAA	FA.049.A
TX	77058	Houston	FAA	FA.072.A
TX	76155	Fort Worth	FAA	FA.084.A
TX	75063	Irving	FAA	FA.085.A
TX	78840	Del Rio	NPS	NP.051.A
TX	78418	Corpus Christi	NPS	NP.063.A
TX	79847	Salt Flat	NPS	NP.067.A
TX	79834	Big Bend National Park	NPS	NP.081.A
TX	77625	Kountze	NPS	NP.084.A
TX	79036	Fritch	NPS	NP.107.A
TX	79905	El Paso	NPS	NP.114.A
TX	79734	Fort Davis	NPS	NP.131.A
TX	78636	Johnson City	NPS	NP.134.A
TX	78210	San Antonio	NPS	NP.141.A
TX	78520	Brownsville	NPS	NP.176.A
TX	75702	Tyler	USCourts	UC.073.A
TX	75074	Plano	USCourts	UC.074.A
TX	75242	Dallas	USCourts	UC.075.A
TX	75242	Dallas	USCourts	UC.075.A
TX	78501	McAllen	USCourts	UC.076.A
TX	77002	Houston	USCourts	UC.077.A
TX	78206	San Antonio	USCourts	UC.133.A
TX	77701	Beaumont	USCourts	UC.173.A
TX	76102	Fort Worth	USCourts	UC.177.A
TX	79401	Lubbock	USCourts	UC.196.A
TX	78520	Brownsville	USCourts	UC.203.A
TX	75090	Sherman	USCourts	UC.238.A
TX	75501	Texarkana	USCourts	UC.239.A
TX	79101	Amarillo	USCourts	UC.245.A
TX	78040	Laredo	USCourts	UC.274.A
TX	78040	Laredo	USCourts	UC.274.B
TX	78040	Laredo	USCourts	UC.274.C
TX	77901	Victoria	USCourts	UC.275.A
TX	75702	Tyler	USCourts	UC.284.A
TX	79901	El Paso	USCourts	UC.288.A
TX	78229	San Antonio	USCourts	UC.290.A
TX	78701	Austin	USCourts	UC.293.A
TX	78701	Austin	USCourts	UC.293.A
TX	79701	Midland	USCourts	UC.306.A
TX	79772	Pecos	USCourts	UC.307.A
TX	76701	Waco	USCourts	UC.308.A
TX	78840	Del Rio	USCourts	UC.309.A
TX	78040	Laredo	USCourts	UC.318.A
TX	75074	Plano	USCourts	UC.321.A
TX	78401	Corpus Christi	USCourts	UC.327.A
UT	84056	Hill AFB	USAF	AF.010.A
UT	84056	Hill AFB	USAF	AF.010.B
UT	84056	Hill AFB	USAF	AF.060.A
UT	84056	Hill AFB	USAF	AF.060.B
UT	84056	Hill AFB	USAF	AF.135.A
UT	84116	Salt Lake City	ANG	AG.085.A
UT	84116	Salt Lake City	ANG	AG.085.B
UT	84116	Salt Lake City	ANG	AG.085.C
UT	84116	Salt Lake City	ANG	AG.085.D
UT	84020	Draper	ANG	AG.145.A
UT	84511	Blanding	ARNG	AN.090.A
UT	84511	Blanding	ARNG	AN.090.B
UT	84084	West Jordan	ARNG	AN.091.A
UT	84084	West Jordan	ARNG	AN.091.B
UT	84020	Draper	USA	AY.069.A
UT	84056	Hill AFB	DLA	DA.035.A
UT	84111	Salt Lake City	DOJ	DJ.121.A
UT	84116	Salt Lake City	FAA	FA.029.A
UT	84116	Salt Lake City	FAA	FA.029.B
UT	84116	Salt Lake City	FAA	FA.123.A
UT	84532	Moab	NPS	NP.004.A

UT	84717	Bryce Canyon	NPS	NP.014.A
UT	84775	Torrey	NPS	NP.057.A
UT	84767	Springdale	NPS	NP.075.A
UT	84145	Salt Lake City	NPS	NP.139.A
UT	84511	Blanding	NPS	NP.175.A
UT	84720	Cedar City	NPS	NP.212.A
UT	84790	St George	NPS	NP.219.A
UT	84101	Salt Lake City	USCourts	UC.016.A
VA	23665	Langley AFB	USAF	AF.002.A
VA	23665	Langley AFB	USAF	AF.002.B
VA	23511	Norfolk	USAF	AF.008.A
VA	25311	Norfolk	USAF	AF.008.B
VA	23511	Norfolk	USAF	AF.008.C
VA	23665	Langley AFB	USAF	AF.064.A
VA	23604	Fort Eustis	USAF	AF.120.A
VA	23150	Sandston	ANG	AG.087.A
VA	23150	Sandston	ANG	AG.087.B
VA	23150	Sandston	ANG	AG.087.C
VA	23150	Sandston	ANG	AG.087.C
VA	23150	Sandston	ANG	AG.087.D
VA	23824	Blackstone	ANG	AG.147.A
VA	23458	Virginia Beach	ANG	AG.252.A
VA	23458	Virginia Beach	ANG	AG.252.B
VA	22204	Arlington	ARNG	AN.001.A
VA	22204	Arlington	ARNG	AN.001.B
VA	22204	Arlington	ARNG	AN.001.C
VA	22311	Alexandria	ARNG	AN.002.A
VA	22311	Alexandria	ARNG	AN.002.B
VA	22060	Fort Belvoir	ARNG	AN.020.A
VA	22060	Fort Belvoir	ARNG	AN.020.B
VA	23150	Sandston	ARNG	AN.092.A
VA	23150	Sandston	ARNG	AN.092.B
VA	23801	Fort Lee	USA	AY.011.B
VA	23801	Fort Lee	USA	AY.011.C
VA	23801	Fort Lee	USA	AY.011.D
VA	23801	Fort Lee	USA	AY.011.E
VA	23801	Fort Lee	USA	AY.011.F
VA	23801	Fort Lee	USA	AY.011.G
VA	23801	Fort Lee	USA	AY.011.H
VA	23801	Fort Lee	USA	AY.011.I
VA	23801	Fort Lee	USA	AY.011.J
VA	23801	Fort Lee	USA	AY.011.K
VA	23801	Fort Lee	USA	AY.011.L
VA	23801	Fort Lee	USA	AY.011.M
VA	23801	Fort Lee	USA	AY.011.N
VA	23801	Fort Lee	USA	AY.011.O
VA	23801	Fort Lee	USA	AY.011.P
VA	23801	Fort Lee	USA	AY.011.Q
VA	22602	Winchester	USA	AY.025.A
VA	23604	Fort Eustis	USA	AY.058.A
VA	23604	Fort Eustis	USA	AY.074.A
VA	23801	Fort Lee	USA	AY.099.A
VA	23801	Fort Lee	USA	AY.099.B
VA	23860	Hopewell	DOJ	BP.001.A
VA	23297	Richmond	DLA	DA.002.A
VA	23297	Richmond	DLA	DA.002.B
VA	23512	Norfolk	DLA	DA.012.A
VA	23237	Richmond	DLA	DA.032.A
VA	23297	Richmond	DLA	DA.032.B
VA	22060-6220	Fort Belvoir	DLA	DA.044.A
VA	24210	Abingdon	DOJ	DJ.122.A
VA	23510	Norfolk	DOJ	DJ.124.A
VA	23219	Richmond	DOJ	DJ.125.A
VA	24011	Roanoke	DOJ	DJ.126.A
VA	23606	Newport News	DOJ	DJ.165.A
VA	22314	Alexandria	DOJ	DJ.886.B
VA	22901	Charlottesville	DOJ	DJ.887.B

VA	22041	Baileys Crossroads	DOJ	EI.001.A
VA	20176	Leesburg	FAA	FA.007.A
VA	20176	Leesburg	FAA	FA.007.B
VA	20170	Herndon	FAA	FA.013.A
VA	20170	Herndon	FAA	FA.013.C
VA	23250	Richmond	FAA	FA.124.A
VA	20166	Dulles	FAA	FA.125.A
VA	20171	Herndon	FAA	FA.130.A
VA	22135	Quantico	FBI	FB.001.A
VA	22203	Arlington	USF&W	FW.003.A
VA	23336	Chincoteague Island	USF&W	FW.020.A
VA	22202	Arlington	DOJ	MS.001.A
VA	22405-2508	Fredericksburg	NPS	NP.052.A
VA	22172	Triangle	NPS	NP.053.A
VA	22835	Luray	NPS	NP.097.A
VA	23690	Yorktown	NPS	NP.106.A
VA	22101	McLean	NPS	NP.135.A
VA	24522	Appomattox	NPS	NP.157.A
VA	24179	Vinton	NPS	NP.160.A
VA	23219	Richmond	NPS	NP.178.A
VA	22443	Colonial Beach	NPS	NP.194.A
VA	23219	Richmond	USCourts	UC.069.A
VA	24011	Roanoke	USCourts	UC.070.A
VA	22341	Alexandria	USCourts	UC.123.A
VA	23510	Norfolk	USCourts	UC.124.A
VA	22314	Alexandria	USCourts	UC.125.A
VA	24012	Roanoke	USCourts	UC.262.A
VA	22901	Charlottesville	USCourts	UC.276.A
VA	24210	Abingdon	USCourts	UC.277.A
VA	23219	Richmond	USCourts	UC.801.B
VA	20191	Reston	USCourts	UC.UP1.RV.B
VI	00850	Kingshill	ANG	AG.251.A
VI	00850	Kingshill	ANG	AG.251.B
VI	00820	St Croix	DOJ	DJ.127.A
VI	00802	St Thomas	DOJ	DJ.888.B
VI	00830	St John	NPS	NP.184.A
VI	00802	St Thomas	USCourts	UC.160.A
VT	05403	South Burlington	ANG	AG.086.A
VT	05403	South Burlington	ANG	AG.086.B
VT	05403	South Burlington	ANG	AG.086.B
VT	05403	South Burlington	ANG	AG.086.C
VT	05403	South Burlington	ANG	AG.086.D
VT	05446	Colchester	ANG	AG.148.A
VT	05701	Rutland	DOJ	DJ.028.A
VT	05402	Burlington	DOJ	DJ.889.B
VT	05402	Burlington	USCourts	UC.057.A
VT	05701	Rutland	USCourts	UC.058.A
WA	99011	Fairchild AFB	USAF	AF.038.A
WA	99011	Fairchild AFB	USAF	AF.038.B
WA	99011	Fairchild AFB	USAF	AF.038.C
WA	98438	McChord AFB	USAF	AF.053.A
WA	98438	McChord AFB	USAF	AF.053.A
WA	98438	McChord AFB	USAF	AF.053.A
WA	98438	McChord AFB	USAF	AF.053.A
WA	98438	McChord AFB	USAF	AF.053.B
WA	99164	Pullman	USAF	AF.081.A
WA	98438	McChord AFB	USAF	AF.100.A
WA	98438	McChord AFB	USAF	AF.100.A
WA	98438	McChord AFB	USAF	AF.127.A
WA	99011	Fairchild AFB	USAF	AF.F95.B
WA	99011	Fairchild AFB	USAF	AF.F95.C
WA	99011	Fairchild AFB	ANG	AG.088.A
WA	99011	Fairchild AFB	ANG	AG.088.B
WA	99011	Fairchild AFB	ANG	AG.088.C
WA	99011	Fairchild AFB	ANG	AG.088.D
WA	98438	McChord AFB	ANG	AG.089.A
WA	98438	McChord AFB	ANG	AG.089.B

WA	98438	McChord AFB	ANG	AG.089.C
WA	98438	McChord AFB	ANG	AG.089.D
WA	98430	Tacoma	ANG	AG.149.A
WA	98430	Tacoma	ANG	AG.149.B
WA	98430	Tacoma	ANG	AG.149.C
WA	98430	Tacoma	ANG	AG.149.D
WA	99004	Cheney	ANG	AG.253.A
WA	99004	Cheney	ANG	AG.253.B
WA	98108	Seattle	ANG	AG.254.A
WA	98108	Seattle	ANG	AG.254.B
WA	98204	Everett	ANG	AG.255.A
WA	98204	Everett	ANG	AG.255.B
WA	99219	Spokane	ANG	AG.256.A
WA	99219	Spokane	ANG	AG.256.B
WA	98226	Bellingham	ANG	AG.257.A
WA	98226	Bellingham	ANG	AG.257.B
WA	99223	Spokane	ARNG	AN.800.B
WA	98433	Fort Lewis	USA	AY.073.A
WA	98314	Bremerton	DLA	DA.030.A
WA	99352	Richland	DOE	DE.001.A
WA	99352	Richland	DOE	DE.001.B
WA	98101	Seattle	DOJ	DJ.129.A
WA	98402	Tacoma	DOJ	DJ.130.1
WA	99201	Spokane	DOJ	DJ.891.B
WA	98907	Yakima	DOJ	DJ.892.B
WA	98055	Renton	FAA	FA.026.A
WA	98055	Renton	FAA	FA.026.B
WA	98092	Auburn	FAA	FA.027.A
WA	98092	Auburn	FAA	FA.027.B
WA	99212	Spokane	FAA	FA.126.A
WA	98188	SeaTac	FAA	FA.127.A
WA	98503	Lacey	USF&W	FW.010.A
WA	99116	Coulee Dam	NPS	NP.005.A
WA	98304	Longmire	NPS	NP.011.A
WA	98101	Seattle	NPS	NP.077.A
WA	98284	Sedro Woolley	NPS	NP.080.A
WA	98362	Port Angeles	NPS	NP.088.A
WA	99362	Walla Walla	NPS	NP.186.A
WA	98901	Yakima	USCourts	UC.106.A
WA	99201	Spokane	USCourts	UC.107.A
WA	98101	Seattle	USCourts	UC.108.A
WA	98101	Seattle	USCourts	UC.109.A
WA	98101	Seattle	USCourts	UC.109.B
WA	98402	Tacoma	USCourts	UC.110.A
WA	99352	Richland	USCourts	UC.234.A
WA	99352	Richland	USCourts	UC.234.B
WA	99201	Spokane	USCourts	UC.268.A
WA	98907	Yakima	USCourts	UC.269.A
WI	53027	Gen Mitchell IAP ARS	USAF	AF.091.A
WI	53027	Gen Mitchell IAP ARS	USAF	AF.091.B
WI	53027	Gen Mitchell IAP ARS	USAF	AF.091.C
WI	53704	Madison	ANG	AG.092.A
WI	53704	Madison	ANG	AG.092.B
WI	53704	Madison	ANG	AG.092.C
WI	53704	Madison	ANG	AG.092.D
WI	53207	Milwaukee	ANG	AG.093.A
WI	53207	Milwaukee	ANG	AG.093.A
WI	53207	Milwaukee	ANG	AG.093.B
WI	53207	Milwaukee	ANG	AG.093.C
WI	53207	Milwaukee	ANG	AG.093.D
WI	54618	Camp Douglas	ANG	AG.094.A
WI	54618	Camp Douglas	ANG	AG.094.B
WI	54618	Camp Douglas	ANG	AG.094.C
WI	54618	Camp Douglas	ANG	AG.094.D
WI	53704	Madison	ANG	AG.151.A
WI	53095	West Bend	ARNG	AN.093.A
WI	53095	West Bend	ARNG	AN.093.B

WI	54656	Fort McCoy	USA	AY.081.A
WI	53703	Madison	DOJ	DJ.131.A
WI	54305	Green Bay	DOJ	DJ.191.A
WI	53202	Milwaukee	DOJ	DJ.893.B
WI	53207	Milwaukee	FAA	FA.128.A
WI	54814	Bayfield	NPS	NP.054.A
WI	53711	Madison	NPS	NP.225.A
WI	53202	Milwaukee	USCourts	UC.135.A
WI	53703	Madison	USCourts	UC.137.A
WI	54701	Eau Claire	USCourts	UC.138.A
WV	25311	Charleston	ANG	AG.090.A
WV	25311	Charleston	ANG	AG.090.A
WV	25311	Charleston	ANG	AG.090.B
WV	25311	Charleston	ANG	AG.090.C
WV	25311	Charleston	ANG	AG.090.D
WV	25401	Martinsburg	ANG	AG.091.A
WV	25401	Martinsburg	ANG	AG.091.B
WV	25401	Martinsburg	ANG	AG.091.C
WV	25401	Martinsburg	ANG	AG.091.D
WV	26301	Clarksburg	DOJ	DJ.132.A
WV	26003	Wheeling	DOJ	DJ.133.A
WV	25801	Beckley	DOJ	DJ.163.A
WV	25301	Charleston	DOJ	DJ.894.B
WV	26241	Elkins	DOJ	DJ.895.B
WV	25701	Huntington	DOJ	DJ.896.B
WV	25401	Martinsburg	DOJ	DJ.899.B
WV	25311	Charleston	FAA	FA.129.A
WV	26306	Clarksburg	FBI	FB.006.A
WV	25443	Shepherdstown	USF&W	FW.001.A
WV	25443	Shepherdstown	USF&W	FW.001.A
WV	25443	Shepherdstown	USF&W	FW.999.A
WV	25425	Harpers Ferry	NPS	NP.059.A
WV	25846	Glen Jean	NPS	NP.087.A
WV	25301	Charleston	USCourts	UC.072.A
WV	25301	Charleston	USCourts	UC.072.B
WV	26003	Wheeling	USCourts	UC.162.A
WV	26003	Wheeling	USCourts	UC.162.B
WV	25801	Beckley	USCourts	UC.280.A
WV	25701	Huntington	USCourts	UC.281.A
WV	25401	Martinsburg	USCourts	UC.297.A
WV	26302	Clarksburg	USCourts	UC.298.A
WV	26241	Elkins	USCourts	UC.299.A
WV	26302	Clarksburg	USCourts	UC.352.A
WY	82005	FE Warren AFB	USAF	AF.039.A
WY	82005	FE Warren AFB	USAF	AF.039.B
WY	82009	Cheyenne	ANG	AG.095.A
WY	82009	Cheyenne	ANG	AG.095.B
WY	82009	Cheyenne	ANG	AG.095.C
WY	82009	Cheyenne	ANG	AG.095.D
WY	82003	Cheyenne	ANG	AG.152.A
WY	82520	Lander	DOJ	DJ.134.A
WY	82601	Casper	DOJ	DJ.182.A
WY	82190	Yellowstone National Pk	DOJ	DJ.801.B
WY	82009	Cheyenne	DOJ	DJ.898.B
WY	82212	Fort Laramie	NPS	NP.056.A
WY	82190	Yellowstone National Park	NPS	NP.062.A
WY	82190	Yellowstone National Park	NPS	NP.062.A
WY	82190	Yellowstone National Park	NPS	NP.062.A
WY	83012	Moose	NPS	NP.110.A
WY	82714	Devils Tower	NPS	NP.129.A
WY	82601	Casper	USCourts	UC.139.A
WY	82009	Cheyenne	USCourts	UC.140.A
(END OF ATTACHMENT J-11)				

ATTACHMENT J-12
Sample Task Order (STO) #3 - BLUE PERSONNEL TRACKING

1 Background

1.1 A U.S. Federal Agency (USFA) regularly sends personnel overseas in support of a variety of projects. Although much of the work is performed in the larger cities, a large proportion of the tasks require personnel to drive to sites in sparsely populated areas. The wireless communications infrastructure in the cities is reasonably reliable, but there are still numerous areas within the cities where reception is poor or the system is congested. Outside of the cities, wireless communication is frequently non-existent on the roads between towns or at mountainous destinations. Due to the large number of countries with which this USFA interacts, personnel are frequently deployed to regions classified as “high risk” areas – either due to local insurgents or to ongoing military conflicts.

1.2 Security personnel within this USFA have observed the success of the Army Blue Force Tracking system, and they have determined that use of a commercial satellite communications-based solution combined with an intuitive map-based application to support dissemination of position data and exchange of text messages provides great benefits, including:

- Ability for local, deployed teams and the central network manager to automatically determine the locations of ‘friendly’ teams within an area
- Ability for deployed teams to easily identify the positions of risk areas and communicate this to other teams operating locally and to a central network manager
- Ability for deployed teams to easily communicate through text messaging in a manner similar to chat applications

1.3 When traveling, personnel must minimize the amount of equipment that they place into checked or carry-on luggage. Once personnel reach their destination airport, they rent vehicles which can range from small to midsize automobiles, cargo vans or off-road vehicles. Minimizing the size, weight and power requirements of equipment needed to implement this capability is an important consideration, along with ease of temporary installations that allow for quick removal and reinstallations daily so equipment can be secured (e.g., in hotel rooms). Personnel are typically sent to an area in multiple groups of small deployed teams (2-4 people per team) plus additional protective security teams and carry laptops and cell phones with a variety of communication interfaces (e.g., Bluetooth, WiFi) that can be incorporated into a communications solution. The Contractor has the option of supplying all devices used in this capability, or incorporating the BPT capability into existing devices normally carried by personnel.

1.4 USFA is not part of the Department of Defense (DoD), so utilizing the Army Blue Force Tracking system is not an option. Additionally, the budget for this USFA does not permit deployment of a similar standalone system, so this USFA has determined that the most cost effective method to proceed is to leverage an existing commercial capability.

2 REQUIREMENTS

2.1 A requirement exists for the Contractor to provide a communications infrastructure to support the USFA as it operates worldwide, with teams redeploying within or between continents with minimal advance notice (latitudes: 65 degrees North to 65 degrees South; land areas only). This is to be accomplished through the end-to-end implementation and integration of mobile capabilities between deployed teams operating within a region and a central network management system. The central network management center shall be connected by the Contractor through the Internet.

2.2 The Period of Performance for BPT is 3 base years, with two 1 year options.

2.3 Project Planning: The Contractor shall develop a Service Plan in accordance with Section C. The Service Plan should include a description of the systems, a network diagram, procedures and performance metrics to put in place to assure successful and timely completion of the Task, procedures explaining how subcontractors will be managed (if applicable), description of how costs will be controlled, and plan to ensure timely submission of invoices. Additionally, include a description of the process(es) that the Contractor will use to interface with the appropriate Government Representative(s). The Service Plan shall include a project implementation schedule. The Service Plan shall address all assumptions, risks and resultant mitigation plans associated with the proposed solution.

2.4 The system shall support the deployment of USFA teams to multiple countries located on one or more continents on an ad-hoc basis with minimal advance notice.

2.5 USFA personnel will operate any equipment associated with this Task Order installed at the USFA facility. Performance shall take place at the Contractor's facilities (CONUS), USFA in Washington DC and multiple locations overseas (OCONUS). The Contractor shall be required to perform background checks for satellite operations staff (commercial, U.S. civil, or foreign). Additionally, the Contractor shall guarantee at least one operations staff member and one decision making authority (e.g., CEO, COO, CTO), who are appropriately cleared for access to the customer's operations and/or data, are available for incident response.

2.6 This effort shall include the following requirements. For each, provide a solution description:

2.6.1 Communications Infrastructure: Develop and implement the requisite communications infrastructure to support the USFA mission. Identify chosen components and explain rationale for selection including lifecycle cost considerations. Provide a detailed architecture and explain operation of all required interfaces. The Contractor shall provide link budgets, as applicable. The Contractor's solution shall address reliability, availability, and maintainability. The Contractor shall demonstrate the ability to comply with the Federal Information Security Management Act of 2002 as implemented by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations*" for a high impact information system, specifically addressing the following controls: CA-7, CP-7, SC-7. Regarding CA-7, the Agency specification for reporting is Monthly. Regarding CP-7, the Agency specification for recovery time objective is 24 hours. Regarding SC-7, the Agency specification for Control Enhancement (4e) is Performed Annually, and there is no Agency specification for Control Enhancement (8), so it is per contractor system determination. The Contractor shall demonstrate the ability to comply with the Committee on National Security Systems Policy (CNSSP) 12, to the maximum extent practicable. See attachment J-3 for additional details on Information Assurance. The communications infrastructure shall have an availability of at least 99.7%.

2.7 The phased deployment of communications installation shall be proposed according to the following schedule:

2.7.1 Phase I (IOC) - Initial Operating Capability (IOC) shall support the installation and deployment of a system connecting USFA deployed teams and Central Site facility. Capabilities for this phase shall include:

- Supply of Central Site terminal to main USFA facility in Washington DC. The Government shall install the Central Site terminal in the main USFA facility; the Contractor shall not be permitted entry.
- Supply of Remote Site terminals, antennas, and any other necessary user hardware or software to the main USFA facility in Washington, DC.
  - Remote Site terminals shall be mobile for vehicular use
  - Remote Site terminals shall include a "panic button" which shall cause the terminal's position icon to noticeably change its status indication on all terminals in the geographic vicinity plus at the central USFA facility.
  - Remote Site terminals shall report position at a minimum rate of once per three minutes to as often as once per minute to minimize location offsets during long trips.
  - Remote Site terminals shall include the ability to be shut down and disabled from the central site.

- Establishment of a central, Contractor-run, 24x7 network management capability
- Establishment of a central Contractor-run 24x7 help desk capability
- Establishment of the infrastructure and supply of terminals to the Government shall be complete 120 days after Task Order award. Testing and acceptance of each remote terminal shall be completed within 2 days after Government checkout has been performed at the USFA facility. Operation shall commence immediately after each terminal is tested and accepted.
- Remote Site Quantities:
  - Number of deployed teams supported: 600
  - Deployed Teams will typically be scattered across multiple continents.
  - Redeploy of teams within or between continents shall occur with minimal advance notice.

2.7.2 Phase 2 Option (FOC) - Full Capability (FOC) shall support steady state operations of the IOC system and provide the Government with the option to procure additional Central Site and Remote Site terminals. Capabilities for this phase shall include:

- Central Site Quantity Update: Up to 3 additional central sites. Central sites will be located within the site coverage areas.
- Remote Site Quantity Update: Up to 3,000 additional teams deployed across multiple continents.
- Contractor surge capability to support simultaneous use of all Central Site and Remote Site terminals.

2.8 Engineering Support: The Contractor shall clearly explain the recommendation for bandwidth, stating assumptions. The Contractor shall engineer the USFA communications architecture, including capacity planning and preparing and developing designs, plans, and reports. The Contractor shall implement configuration management, prepare engineering documents and reference manuals, and provide engineering and testing services for the USFA communications infrastructure. The Offeror is encouraged to use non-proprietary solutions when possible.

2.9 Sustainment: The Contractor shall implement and execute logistics, training, and O&M support. Deliveries will be sent to the central warehouse. A phased approach may be considered.

2.9.1 Integrated Logistics Support - The Contractor shall develop and implement a maintenance and supply concept necessary to ensure the order, receipt, delivery and accountability of materials necessary to support delivery of the project within the schedule and budget identified by the Government. Logistics support shall include all hardware/software elements and ancillary items necessary for maintaining an operational schedule. The Contractor shall use available commercial materials to the maximum extent possible.

2.9.2 Training - The Contractor shall explain the necessary installation and operation and maintenance training plans and courses. The Contractor shall present the training classes at the main USFA facility in Washington DC.

2.9.3 Installation - The Contractor shall develop necessary installation documentation for the Government to install terminals and operate terminals or any fixed or mobile asset.

2.9.4 Operations and Maintenance - The Contractor shall provide qualified technical support for the duration of the task's period of performance. Maintenance support shall include the replacement of defective components, upgrades to include COTS technology insertion, and any software updates, as required. Operations support includes 24/7 NOC support.

2.9.5 Usage - The system shall be available for use on a 24x7 basis, but usage may be sporadic on an ad-hoc basis for varying periods of time.

2.9.6 EMI/RFI Identification and Resolution - The Contractor shall implement and support EMI/RFI identification and resolution procedures. The Contractor shall explain how EMI/RFI identification and resolution will be communicated to the Government. The Government prefers the Contractor have access to a media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

2.9.7 Network Monitoring - The Contractor shall establish, and provide USFA access to, a common NetOps web portal with multiple secure account access to present the health of the entire BPT system in a consolidated view using data from multiple sources. The Contractor shall collect NetOps metrics on the Central Site, Gateway, Satellite, and Remote Terminal segments of the BPT system. The Contractor shall specify the NetOps metrics to be collected for each segment, frequency of data delivery, retrieval methods, data units, and data format.

2.9.8 Priced Line Items - At a minimum, pricing is required for the following line items. The Contractor shall note if certain line items are not separately priced**.** All prices shall be fixed price.

2.9.9 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost

2.9.10 Network operations center (NOC) operations cost

2.9.11 IOC Central Site terminal cost

2.9.12 FOC additional Central Site terminals cost per unit

2.9.13 Remote Site terminals cost per unit

2.9.14 Engineering Support cost per month

2.9.15 Sustainment support cost per month

2.9.16 Travel can be charged as ODC and is not required as part of the STO pricing.

(END OF ATTACHMENT J-12)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
			Access Control	
ECAN-1 ECPA-1 PRAS-1 DCAR-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	
IAAC-1	AC-2	ACCOUNT MANAGEMENT	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
			transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*].	
DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	AC-3	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	
EBBD-1 EBBD-2	AC-4	INFORMATION FLOW ENFORCEMENT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))
ECLP-1	AC-5	SEPARATION OF DUTIES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))
ECLP-1	AC-6	LEAST PRIVILEGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II))

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECLO-1	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECWM-1	AC-8	SYSTEM USE NOTIFICATION	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	
	AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
ECLO-1	AC-10	CONCURRENT SESSION CONTROL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References			Threshold Compliance	
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PESL-1	AC-11	SESSION LOCK	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	AC-12	SESSION TERMINATION	Withdrawn: Incorporated into SC-10	Optional: (May be applicable for DoD MAC I or MAC II)
ECAT-1 ECAT-2 E3.3.9	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	Withdrawn: Incorporated into AC-2 and AU-6.	Optional: (May be applicable for DoD MAC I or MAC II)
---	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.	
ECML-1	AC-15	AUTOMATED MARKING	Withdrawn: Incorporated into MP-3.	Optional: (May be applicable for DoD MAC I or MAC II)
	AC-16	SECURITY ATTRIBUTES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
EBRP-1 EBRU-1	AC-17	REMOTE ACCESS	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.	
ECCT-1 ECWN-1	AC-18	WIRELESS ACCESS	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
ECWN-1	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
---	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.	
	AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	
			Awareness and Training	
PRTN-1 DCAR-1	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PRTN-1	AT-2	SECURITY AWARENESS	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	
PRTN-1	AT-3	SECURITY TRAINING	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	
---	AT-4	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].	
	AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
Audit and Accountability				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECAT-1 ECTB-1 DCAR-1	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	
ECAR-3	AU-2	AUDITABLE EVENTS	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECAR-1 ECAR-2 ECAR-3 ECLC-1	AU-3	CONTENT OF AUDIT RECORDS	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	
---	AU-4	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	
---	AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	
ECAT-1 E3.3.9	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECRG-1	AU-7	AUDIT REDUCTION AND REPORT GENERATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECAR-1	AU-8	TIME STAMPS	The information system uses internal system clocks to generate time stamps for audit records.	
ECTP-1	AU-9	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
	AU-10	NON-REPUDIATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECRR-1	AU-11	AUDIT RECORD RETENTION	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	
	AU-12	AUDIT GENERATION	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	
	AU-13	MONITORING FOR INFORMATION DISCLOSURE	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	AU-14	SESSION AUDIT	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
Security Assessment and Authorization				
DCAR-1 DCII-1	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCII-1 ECMT-1 PEPS-1 E3.3.10	CA-2	SECURITY ASSESSMENTS	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. .	
DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	CA-3	INFORMATION SYSTEM CONNECTIONS	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCAR-1 5.7.5	CA-4	SECURITY CERTIFICATION	Withdrawn: Incorporated into CA-2.	Optional: (May be applicable for DoD MAC I or MAC II)
5.7.5	CA-5	PLAN OF ACTION AND MILESTONES	The organization: a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	
5.7.5	CA-6	SECURITY AUTHORIZATION	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCCB-1 DCPR-1 E3.3.9	CA-7	CONTINUOUS MONITORING	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	
Configuration Management				
DCCB-1 DCPR-1 DCAR-1 E3.3.8	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	
DCHW-1 DCSW-1	CM-2	BASELINE CONFIGURATION	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
DCPR-1	CM-3	CONFIGURATION CHANGE CONTROL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCPR-1 E3.3.8	CM-4	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	
DCPR-1 ECSD-2	CM-5	ACCESS RESTRICTIONS FOR CHANGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCSS-1 ECSC-1 E3.3.8	CM-6	CONFIGURATION SETTINGS	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
DCPP-1 ECIM-1 ECVI-1 E3.3.8	CM-7	LEAST FUNCTIONALITY	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials.	
	CM-9	CONFIGURATION MANAGEMENT PLAN	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
Contingency Planning				
COBR-1 DCAR-1	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	

ATTACHMENT J-2

INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References			Threshold Compliance	
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
CODP-1 COEF-1	CP-2	CONTINGENCY PLAN	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PRTN-1	CP-3	CONTINGENCY TRAINING	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].	
COED-1	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions.	
DCAR-1	CP-5	CONTINGENCY PLAN UPDATE	Withdrawn: Incorporated into CP-2.	May be applicable for DoD MAC I or MAC II)
CODB-2	CP-6	ALTERNATE STORAGE SITE	Not Applicable	May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
COAS-1 COEB-1 COSP-1 COSP-2	CP-7	ALTERNATE PROCESSING SITE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	CP-8	TELECOMMUNICA-TIONS SERVICES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References			Threshold Compliance	
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
CODB-1 CODB-2 COSW-1	CP-9	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location.	
COTR-1 ECND-1	CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	
Identification and Authentication				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
IAIA-1 DCAR-1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.	
IAIA-1	IA-2	IDENTIFICATION AND AUTHENTICATION (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancement: (1) The information system uses multifactor authentication for network access to privileged accounts.	
---	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
IAGA-1 IAIA-1	IA-4	IDENTIFIER MANAGEMENT	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
IAKM-1 IATS-1	IA-5	AUTHENTICATOR MANAGEMENT	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancement: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization*	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
---	IA-6	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
---	IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	
	IA-8	IDENTIFICATION AND AUTHENTICATION (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
Incident Response				
VIIR-1 DCAR-1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	
VIIR-1	IR-2	INCIDENT RESPONSE TRAINING	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
VIIR-1	IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
VIIR-1 E3.3.9	IR-4	INCIDENT HANDLING	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	
VIIR-1	IR-5	INCIDENT MONITORING	The organization tracks and documents information system security incidents.	
VIIR-1 E3.3.9	IR-6	INCIDENT REPORTING	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities.	
---	IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	IR-8	INCIDENT RESPONSE PLAN	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
			Maintenance	
PRMP-1 DCAR-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	
---	MA-2	CONTROLLED MAINTENANCE	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	
---	MA-3	MAINTENANCE TOOLS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
EBRP-1	MA-4	NON-LOCAL MAINTENANCE	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.	
PRMP-1	MA-5	MAINTENANCE PERSONNEL	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	
COMS-1 COSP-1	MA-6	TIMELY MAINTENANCE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
Media Protection				

ATTACHMENT J-2

INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PESP-1 DCAR-1	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	
PEDI-1 PEPF-1	MP-2	MEDIA ACCESS	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].	
ECML-1	MP-3	MEDIA MARKING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PESS-1	MP-4	MEDIA STORAGE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	MP-5	MEDIA TRANSPORT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PECS-1 PEDD-1	MP-6	MEDIA SANITIZATION	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	
PEDD-1	MP-7	MEDIA DESTRUCTION AND DISPOSAL	Withdrawn from SP 800-53, Rev. 3	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
			Physical and Environmental Protection	
PETN-1 DCAR-1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	
PECF-1	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PEPF-1	PE-3	PHYSICAL ACCESS CONTROL	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	
	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PEDI-1 PEPF-1	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PEPF-2	PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and c. Coordinates results of reviews and investigations with the organization's incident response capability.	
PEVC-1	PE-7	VISITOR CONTROL	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	
PEPF-2 PEVC-1	PE-8	ACCESS RECORDS	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records [*Assignment: organization-defined frequency*].	
---	PE-9	POWER EQUIPMENT AND POWER CABLING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
PEMS-1	PE-10	EMERGENCY SHUTOFF	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
COPS-1 COPS-2 COPS-3	PE-11	EMERGENCY POWER	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PEEL-1	PE-12	EMERGENCY LIGHTING	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
PEFD-1 PEFS-1	PE-13	FIRE PROTECTION	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
PEHC-1 PETC-1	PE-14	TEMPERATURE AND HUMIDITY CONTROLS	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	
---	PE-15	WATER DAMAGE PROTECTION	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
---	PE-16	DELIVERY AND REMOVAL	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	
EBRU-1	PE-17	ALTERNATE WORK SITE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	PE-19	INFORMATION LEAKAGE	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
			Planning	
DCAR-1 E3.4.6	PL-1	SECURITY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCSD-1	PL-2	SYSTEM SECURITY PLAN	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
5.7.5	PL-3	SYSTEM SECURITY PLAN UPDATE	Withdrawn: Incorporated into PL-2.	Optional: (May be applicable for DoD MAC I or MAC II)
5.7.5 PRRB-1	PL-4	RULES OF BEHAVIOR	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	
---	PL-5	PRIVACY IMPACT ASSESSMENT	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	
	PL-6	SECURITY-RELATED ACTIVITY PLANNING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
Personnel Security				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PRRB-1 DCAR-1	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	
---	PS-2	POSITION CATEGORIZATION	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	
PRAS-1	PS-3	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
5.12.7	PS-4	PERSONNEL TERMINATION	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	
5.12.7	PS-5	PERSONNEL TRANSFER	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	
PRRB-1	PS-6	ACCESS AGREEMENTS	The organization: a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	
5.7.10	PS-7	THIRD-PARTY PERSONNEL SECURITY	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References			**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PRRB-1	PS-8	PERSONNEL SANCTIONS	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
Risk Assessment				
DCAR-1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	
E3.4.2	RA-2	SECURITY CATEGORIZATION	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCDS-1 DCII-1 E3.3.10	RA-3	RISK ASSESSMENT	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	
DCAR-1 DCII-1	RA-4	RISK ASSESSMENT UPDATE	Withdrawn: Incorporated into RA-3.	Optional: (May be applicable for DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECMT-1 VIVM-1	RA-5	VULNERABILITY SCANNING	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	
System and Services Acquisition				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCAR-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	
DCPB-1 E3.3.4	SA-2	ALLOCATION OF RESOURCES	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
5.8.1	SA-3	LIFE CYCLE SUPPORT	The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	
DCAS-1 DCDS-1 DCIT-1 DCMC-1	SA-4	ACQUISITIONS	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCCS-1 DCHW-1 DCID-1 DCSD-1 DCSW-1 ECND-1 DCFA-1	SA-5	INFORMATION SYSTEM DOCUMENTATION	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCPD-1	SA-6	SOFTWARE USAGE RESTRICTIONS	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
---	SA-7	USER INSTALLED SOFTWARE	The organization enforces explicit rules governing the installation of software by users.	
DCBP-1 DCCS-1 E3.4.4	SA-8	SECURITY DESIGN PRINCIPLES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCDS-1 DCID-1 DCIT-1 DCPP-1	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
---	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
E3.4.4	SA-11	DEVELOPER SECURITY TESTING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-12	SUPPLY CHAIN PROTECTION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-13	TRUSTWORTHI-NESS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SA-14	CRITICAL INFORMATION SYSTEM COMPONENTS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
System and Communications Protection				
DCAR-1	SC-1	SYSTEM AND COMMUNICA-TIONS PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCPA-1	SC-2	APPLICATION PARTITIONING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCSP-1	SC-3	SECURITY FUNCTION ISOLATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECRC-1	SC-4	INFORMATION IN SHARED RESOURCES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SC-5	DENIAL OF SERVICE PROTECTION	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	
---	SC-6	RESOURCE PRIORITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
COEB-1 EBBD-1 ECIM-1 ECVI-1	SC-7	BOUNDARY PROTECTION	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
ECTM-1	SC-8	TRANSMISSION INTEGRITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECCT-1	SC-9	TRANSMISSION CONFIDENTIALITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SC-10	NETWORK DISCONNECT	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-11	TRUSTED PATH	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
IAKM-1	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	
IAKM-1 IATS-1	SC-13	USE OF CRYPTOGRAPHY	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	
EBPW-1	SC-14	PUBLIC ACCESS PROTECTIONS	The information system protects the integrity and availability of publicly available information and applications.	
ECVI-1	SC-15	COLLABORATIVE COMPUTING DEVICES	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
IAKM-1	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
DCMC-1	SC-18	MOBILE CODE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECVI-1	SC-19	VOICE OVER INTERNET PROTOCOL	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (Authoritative Source)	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (Recursive or Caching Resolver)	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-23	SESSION AUTHENTICITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-24	FAIL IN KNOWN STATE	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-25	THIN NODES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-26	HONEYPOTS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-27	OPERATING SYSTEM-INDEPENDENT APPLICATIONS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-28	PROTECTION OF INFORMATION AT REST	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	SC-29	HETEROGENEITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-30	VIRTUALIZATION TECHNIQUES	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-31	COVERT CHANNEL ANALYSIS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-32	INFORMATION SYSTEM PARTITIONING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
	SC-33	TRANSMISSION PREPARATION INTEGRITY	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
	SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
System and Information integrity				
DCAR-1	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
DCSQ-1 DCCT-1 E.3.3.5.7	SI-2	FLAW REMEDIATION	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
ECVP-1 VIVM-1	SI-3	MALICIOUS CODE PROTECTION	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	
EBBD-1 EBVC-1 ECID-1	SI-4	INFORMATION SYSTEM MONITORING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
VIVIM-1	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	
DCSS-1	SI-6	SECURITY FUNCTIONALITY VERIFICATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
ECSD-2	SI-7	SOFTWARE AND INFORMATION INTEGRITY	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-8	SPAM PROTECTION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-9	INFORMATION INPUT RESTRICTIONS	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-10	INFORMATION INPUT VALIDATION	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)
---	SI-11	ERROR HANDLING	Not Applicable	Optional: (May be applicable for NIST Moderate or High Impact, or DoD MAC I or MAC II)

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
PESP-1	SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	
	SI-13	PREDICTABLE FAILURE PREVENTION	Not Applicable	Optional: (May be applicable for DoD MAC I or MAC II)
Program Management				

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	PM-1	INFORMATION SECURITY PROGRAM PLAN	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	
	PM-2	SENIOR INFORMATION SECURITY OFFICER	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	

ATTACHMENT J-2

INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		CONTROL NAME	Threshold Compliance	
DoDI 8500.2	NIST 800-53		Low-Impact Information System (FIPS 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)	Explain Your Current Compliance OR Actions to Become Compliant
	PM-3	INFORMATION SECURITY RESOURCES	The organization: a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	
	PM-4	PLAN OF ACTION AND MILESTONES PROCESS	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	
	PM-5	INFORMATION SYSTEM INVENTORY	The organization develops and maintains an inventory of its information systems.	
	PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	The organization develops, monitors, and reports on the results of information security measures of performance.	
	PM-7	ENTERPRISE ARCHITECTURE	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.	
	PM-8	CRITICAL INFRASTRUCTURE PLAN	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	

ATTACHMENT J-2
INFORMATION ASSURANCE MINIMUM SECURITY CONTROLS CHECKLIST

References		**CONTROL NAME**	**Threshold Compliance**	
DoDI 8500.2	**NIST 800-53**		**Low-Impact Information System (FIPS 200 / NIST SP 800-53)** **MAC III (DoDI 8500.2)** **(generally commercial best practices)**	**Explain Your Current Compliance OR Actions to Become Compliant**
	PM-9	RISK MANAGEMENT STRATEGY	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	
	PM-10	SECURITY AUTHORIZATION PROCESS	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	
	PM-11	MISSION/ BUSINESS PROCESS DEFINITION	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	

(END OF ATTACHMENT J-2)

ATTACHMENT J-3

Security Controls for Information Systems
Definitions from NIST Special Publication 800-53

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
FIPS Pub 200 Definition for High/Moderate/Low Impact Information System:			FIPS Publication 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept must be used to determine the overall impact level of the information system. Thus, a **low-impact system** is an information system in which all three of the security objectives are low. A **moderate-impact system** is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a **high-impact system** is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.		
DoDI 8500.2 Mission Assurance Category (MAC) Definitions:			Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures.	Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance Category II systems require additional safeguards beyond best practices to ensure assurance.	Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. **Mission Assurance Category III systems require protective measures, techniques, or procedures generally**

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
					commensurate with commercial best practices.
			Access Control		
ECAN-1 ECPA-1 PRAS-1 DCAR-1	AC-1	ACCESS CONTROL POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
IAAC-1	AC-2	ACCOUNT MANAGEMENT	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts; f. Specifically authorizing and	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating, modifying, disabling, and removing accounts;	The organization manages information system accounts, including: a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary); b. Establishing conditions for group membership; c. Identifying authorized users of the information system and specifying access privileges; d. Requiring appropriate approvals for requests to establish accounts; e. Establishing, activating,

References			Task Order Requirement		
DoDI 8500.2	NIST 800-53	CONTROL NAME	High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. (3) The information system	f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to support the management of information system accounts. (2) The information system automatically terminates temporary	modifying, disabling, and removing accounts; f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes; h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users; i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and j. Reviewing accounts [*Assignment: organization-defined frequency*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			automatically disables inactive accounts after [*Assignment: organization-defined time period*]. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	and emergency accounts after [*Assignment: organization-defined time period for each type of account*]. (3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*]. (4) The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	AC-3	ACCESS ENFORCEMENT	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.
EBBD-1 EBBD-2	AC-4	INFORMATION FLOW ENFORCEMENT	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy	The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	Not Applicable
ECLP-1	AC-5	SEPARATION OF DUTIES	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	The organization: a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	b. Documents separation of duties; and c. Implements separation of duties through assigned information system access authorizations.	
ECLP-1	AC-6	LEAST PRIVILEGE	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*]. (2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. Control Enhancements: (1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*]. (2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
ECLO-1	AC-7	UNSUCCESSFUL LOGIN ATTEMPTS	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	The information system: a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.
ECWM-1	AC-8	SYSTEM USE NOTIFICATION	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use	The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded,

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.
	AC-9	PREVIOUS LOGON (ACCESS) NOTIFICATION	Not Applicable	Not Applicable	Not Applicable
ECLO-1	AC-10	CONCURRENT SESSION CONTROL	The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PESL-1	AC-11	SESSION LOCK	The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	The information system: a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.	Not Applicable
---	AC-12	SESSION TERMINATION	Withdrawn: Incorporated into SC-10.	Withdrawn: Incorporated into SC-10.	Withdrawn: Incorporated into SC-10
ECAT-1 ECAT-2 E3.3.9	AC-13	SUPERVISION AND REVIEW — ACCESS CONTROL	Withdrawn: Incorporated into AC-2 and AU-6.	Withdrawn: Incorporated into AC-2 and AU-6.	Withdrawn: Incorporated into AC-2 and AU-6.
---	AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Control Enhancement: (1) The organization permits actions to be performed without identification and	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. Control Enhancement: (1) The organization permits actions to be performed without identification	The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			authentication only to the extent necessary to accomplish mission/business objectives.	and authentication only to the extent necessary to accomplish mission/business objectives.	
ECML-1	AC-15	AUTOMATED MARKING	Withdrawn: Incorporated into MP-3.	Withdrawn: Incorporated into MP-3.	Withdrawn: Incorporated into MP-3.
	AC-16	SECURITY ATTRIBUTES	Not Applicable	Not Applicable	Not Applicable
EBRP-1 EBRU-1	AC-17	REMOTE ACCESS	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses cryptography to protect the confidentiality and	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. (2) The organization uses	The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			integrity of remote access sessions. (3) The information system routes all remote accesses through a limited number of managed access control points. (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited. (8) The organization disables networking protocols within the information system deemed to be nonsecure except for explicitly identified components in support of specific operational requirements.	cryptography to protect the confidentiality and integrity of remote access sessions. (3) The information system routes all remote accesses through a limited number of managed access control points. (4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. (5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited. (8) The organization disables networking protocols within the information system deemed to be	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
				nonsecure except for explicitly identified components in support of specific operational requirements.	
ECCT-1 ECWN-1	AC-18	WIRELESS ACCESS	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Control Enhancements: (1) The information system protects wireless access to the system using authentication and encryption. (2) The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered. (4) The organization does not allow users to independently configure wireless networking capabilities. (5) The organization confines wireless	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system. Control Enhancement: (1) The information system protects wireless access to the system using authentication and encryption.	The organization: a. Establishes usage restrictions and implementation guidance for wireless access; b. Monitors for unauthorized wireless access to the information system; c. Authorizes wireless access to the information system prior to connection; and d. Enforces requirements for wireless connections to the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			communications to organization-controlled boundaries.		
ECWN-1	AC-19	ACCESS CONTROL FOR MOBILE DEVICES	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning	The organization: a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices; b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; c. Monitors for unauthorized connections of mobile devices to organizational information systems; d. Enforces requirements for the connection of mobile devices to organizational information systems; e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			accordance with organizational policies and procedures. Control Enhancements: (1) The organization restricts the use of writable, removable media in organizational information systems. (2) The organization prohibits the use of personally owned, removable media in organizational information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures. Control Enhancements: (1) The organization restricts the use of writable, removable media in organizational information systems. (2) The organization prohibits the use of personally owned, removable media in organizational information systems. (3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.	devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.
---	AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems. Control Enhancements:	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.	The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to: a. Access the information system from the external information systems; and b. Process, store, and/or transmit organization-controlled information using the external information systems.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	Control Enhancements: (1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. (2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
	AC-21	USER-BASED COLLABORATION AND INFORMATION SHARING	Not Applicable	Not Applicable	Not Applicable
	AC-22	PUBLICLY ACCESSIBLE CONTENT	The organization: a. Designates individuals authorized to post information onto an organizational information system that is publicly	The organization: a. Designates individuals authorized to post information onto an organizational information system that	The organization: a. Designates individuals authorized to post information onto an organizational information system

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.	that is publicly accessible; b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.
Awareness and Training					
PRTN-1 DCAR-1	AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.	b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.
PRTN-1	AT-2	SECURITY AWARENESS	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.	The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.
PRTN-1	AT-3	SECURITY TRAINING	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.	The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.
---	AT-4	SECURITY TRAINING RECORDS	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].	The organization: a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and b. Retains individual training records for [*Assignment: organization-defined time period*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
	AT-5	CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	Not Applicable	Not Applicable	Not Applicable
Audit and Accountability					
ECAT-1 ECTB-1 DCAR-1	AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.
ECAR-3	AU-2	AUDITABLE EVENTS	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational entities requiring audit-related	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational	The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*]; b. Coordinates the security audit function with other organizational

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*]. Control Enhancements: (3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*]. (4) The organization includes execution of privileged functions in the list of events to be audited by the information system.	entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*]. Control Enhancements: (3) The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*]. (4) The organization includes execution of privileged functions in the list of events to be audited by the information system.	entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].
ECAR-1 ECAR-2	AU-3	CONTENT OF AUDIT RECORDS	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred,	The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
ECAR-3 ECLC-1			and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Control Enhancements: (1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject. (2) The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].	when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. Control Enhancement: (1) The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.	occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
---	AU-4	AUDIT STORAGE CAPACITY	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.
---	AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].	The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Control Enhancements: (1) The information system provides a warning when allocated audit record storage volume reaches [*Assignme*nt: organi*zation-defined percentage*] of maximum audit record storage capacity. (2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].		
ECAT-1 E3.3.9	AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. Control Enhancement: (1) The information system integrates	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.	The organization: a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.		
ECRG-1	AU-7	AUDIT REDUCTION AND REPORT GENERATION	The information system provides an audit reduction and report generation capability. Control Enhancement: (1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	The information system provides an audit reduction and report generation capability. Control Enhancement: (1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.	Not Applicable
ECAR-1	AU-8	TIME STAMPS	The information system uses internal system clocks to generate time stamps for audit records. Control Enhancement: (1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	The information system uses internal system clocks to generate time stamps for audit records. Control Enhancement: (1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].	The information system uses internal system clocks to generate time stamps for audit records.
ECTP-1	AU-9	PROTECTION OF AUDIT INFORMATION	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
	AU-10	NON-REPUDIATION	The information system protects against an individual falsely denying having performed a particular action.	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
ECRR-1	AU-11	AUDIT RECORD RETENTION	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
	AU-12	AUDIT GENERATION	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. Control Enhancement: (1) The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of*	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			individual records in the audit trail].		
	AU-13	MONITORING FOR INFORMATION DISCLOSURE	Not Applicable	Not Applicable	Not Applicable
	AU-14	SESSION AUDIT	Not Applicable	Not Applicable	Not Applicable
Security Assessment and Authorization					
DCAR-1 DCII-1	CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.
DCII-1 ECMT-1 PEPS-1 E3.3.10	CA-2	SECURITY ASSESSMENTS	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used	The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Control Enhancements: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. (2) The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced;*	to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Control Enhancement: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.	used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. .

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			unannounced], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security testing*]].		
DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	CA-3	INFORMATION SYSTEM CONNECTIONS	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	The organization: a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.
DCAR-1 5.7.5	CA-4	SECURITY CERTIFICATION	Withdrawn: Incorporated into CA-2.	Withdrawn: Incorporated into CA-2.	Withdrawn: Incorporated into CA-2.
5.7.5	CA-5	PLAN OF ACTION AND MILESTONES	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate	The organization: a. Develops a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.	and to reduce or eliminate known vulnerabilities in the system; and b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.
5.7.5	CA-6	SECURITY AUTHORIZATION	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].	The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [*Assignment: organization-defined frequency*].
DCCB-1 DCPR-1 E3.3.9	CA-7	CONTINUOUS MONITORING	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the	The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a. A configuration management process for the information system and its constituent components; b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].	assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].
Configuration Management					
DCCB-1 DCPR-1 DCAR-1 E3.3.8	CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.
DCHW-1 DCSW-1	CM-2	BASELINE CONFIGURATION	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and updates the baseline configuration of	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system. Control Enhancements: (1) The organization reviews and	The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and (c) As an integral part of information system component installations and upgrades. (2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. (3) The organization retains older versions of baseline configurations as deemed necessary to support rollback. (5) The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. (6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	updates the baseline configuration of the information system: (a) [*Assignment: organization-defined frequency*]; (b) When required due to [*Assignment organization-defined circumstances*]; and (c) As an integral part of information system component installations and upgrades. (3) The organization retains older versions of baseline configurations as deemed necessary to support rollback. (4) The organization: (a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and (b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.	
DCPR-1	CM-3	CONFIGURATION CHANGE	The organization: a. Determines the types of changes to	The organization: a. Determines the types of changes to	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
		CONTROL	the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]]. Control Enhancements: (1) The organization employs automated mechanisms to: (a) Document proposed changes to the information system; (b) Notify designated approval authorities;	the information system that are configuration controlled; b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses; c. Documents approved configuration-controlled changes to the system; d. Retains and reviews records of configuration-controlled changes to the system; e. Audits activities associated with configuration-controlled changes to the system; and f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]]. Control Enhancement: (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(c) Highlight approvals that have not been received; (d) Inhibit change until designated approvals are received; and (e) Document completed changes to the information system. (2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.		
DCPR-1 E3.3.8	CM-4	SECURITY IMPACT ANALYSIS	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation. Control Enhancement: (1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.
DCPR-1 ECSD-2	CM-5	ACCESS RESTRICTIONS FOR CHANGE	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system. Control Enhancements: (1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. (2) The organization conducts audits of	The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information system changes [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred. (3) The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.		
DCSS-1 ECSC-1 E3.3.8	CM-6	CONFIGURATION SETTINGS	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			Control Enhancements: (1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings. (2) The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*]. (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	Control Enhancement: (3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	
DCPP-1 ECIM-1 ECVI-1 E3.3.8	CM-7	LEAST FUNCTIONALITY	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*]. Control Enhancements: (1) The organization reviews the information system [*Assignment:*	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*]. Control Enhancement: (1) The organization reviews the information system [*Assignment:*	The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services. (2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].	*organization-defined frequency*] to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
	CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials. Control Enhancements: (1) The organization updates the inventory of information system components as an integral part of	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials. Control Enhancements: (1) The organization updates the inventory of information system	The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and e. Is available for review and audit by designated organizational officials.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			component installations, removals, and information system updates. (2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. (3) The organization: (a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials. (4) The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components. (5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	components as an integral part of component installations, removals, and information system updates. (5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
	CM-9	CONFIGURATION MANAGEMENT	The organization develops, documents, and implements a configuration	The organization develops, documents, and implements a	Not Applicable

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
		PLAN	management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	configuration management plan for the information system that: a. Addresses roles, responsibilities, and configuration management processes and procedures; b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	
Contingency Planning					
COBR-1 DCAR-1	CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
				controls.	controls.
CODP-1 COEF-1	CP-2	CONTINGENCY PLAN	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling	The organization: a. Develops a contingency plan for the information system that: - Identifies essential missions and business functions and associated contingency requirements; - Provides recovery objectives, restoration priorities, and metrics; - Addresses contingency roles, responsibilities, assigned individuals with contact information; - Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; - Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]; c. Coordinates contingency planning activities with incident handling

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]. Control Enhancements: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans. (2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations. (3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.	activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*]. Control Enhancement: (1) The organization coordinates contingency plan development with organizational elements responsible for related plans.	activities; d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*]; e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
PRTN-1	CP-3	CONTINGENCY TRAINING	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].	The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].
COED-1	CP-4	CONTINGENCY PLAN TESTING AND EXERCISES	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancements: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans. (2) The organization tests/exercises the	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions. Control Enhancement: (1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related	The organization: a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and b. Reviews the contingency plan test/exercise results and initiates corrective actions.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. (4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	plans.	
DCAR-1	CP-5	CONTINGENCY PLAN UPDATE	Withdrawn: Incorporated into CP-2.	Withdrawn: Incorporated into CP-2.	Withdrawn: Incorporated into CP-2.
CODB-2	CP-6	ALTERNATE STORAGE SITE	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. (2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives. (3) The organization identifies potential accessibility problems to the alternate	The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information. Control Enhancements: (1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards. (3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
COAS-1 COEB-1 COSP-1 COSP-2	CP-7	ALTERNATE PROCESSING SITE	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	The organization: a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Control Enhancements: (1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards. (2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions. (5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	and outlines explicit mitigation actions. (3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. (5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	
---	CP-8	TELECOMMUNICATIONS SERVICES	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and (b) Requests Telecommunications	The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable. Control Enhancements: (1) The organization: (a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements; and	Not Applicable

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services. (3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards. (4) The organization requires primary and alternate telecommunications service providers to have contingency plans.	(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. (2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	
CODB-1 CODB-2 COSW-1	CP-9	INFORMATION SYSTEM BACKUP	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point*	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and*	The organization: a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and*

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			objectives]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location. Control Enhancements: (1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity. (2) The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing. (3) The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not colocated with the operational system.	*recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location. Control Enhancement: (1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.	*recovery point objectives*]; c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and d. Protects the confidentiality and integrity of backup information at the storage location.
COTR-1 ECND-1	CP-10	INFORMATION SYSTEM RECOVERY AND	The organization provides for the recovery and reconstitution of the information system to a known state	The organization provides for the recovery and reconstitution of the information system to a known state	The organization provides for the recovery and reconstitution of the information system to a known state

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		RECONSTITUTION	after a disruption, compromise, or failure. Control Enhancements: (2) The information system implements transaction recovery for systems that are transaction-based. (3) The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution. (4) The organization provides the capability to reimage information system components] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	after a disruption, compromise, or failure. Control Enhancements: (2) The information system implements transaction recovery for systems that are transaction-based. (3) The organization provides compensating security controls for organization-defined circumstances that can inhibit recovery and reconstitution. .	after a disruption, compromise, or failure.
Identification and Authentication					
IAIA-1 DCAR-1	IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			identification and authentication policy and associated identification and authentication controls.	identification and authentication policy and associated identification and authentication controls.	the identification and authentication policy and associated identification and authentication controls.
IAIA-1	IA-2	IDENTIFICATION AND AUTHENTICATION (Organizational Users)	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (4) The information system uses multifactor authentication for local access to non-privileged accounts. (8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts. (9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancements: (1) The information system uses multifactor authentication for network access to privileged accounts. (2) The information system uses multifactor authentication for network access to non-privileged accounts. (3) The information system uses multifactor authentication for local access to privileged accounts. (8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). Control Enhancement: (1) The information system uses multifactor authentication for network access to privileged accounts.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			non-privileged accounts.		
---	IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.	Not Applicable
IAGA-1 IAIA-1	IA-4	IDENTIFIER MANAGEMENT	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].	The organization manages information system identifiers for users and devices by: a. Receiving authorization from a designated organizational official to assign a user or device identifier; b. Selecting an identifier that uniquely identifies an individual or device; c. Assigning the user identifier to the intended party or the device identifier to the intended device; d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].
IAKM-1 IATS-1	IA-5	AUTHENTICATOR MANAGEMENT	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device	The organization manages information system authenticators for users and devices by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancements: (1) The information system, for	receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators. Control Enhancements:	device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators upon information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate); g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*]; h. Protecting authenticator content from unauthorized disclosure and modification; and i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. (3) The organization requires that the	(1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. (2) The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to	Control Enhancement: (1) The information system, for password-based authentication: (a) Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*]; (b) Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created; (c) Encrypts passwords in storage and in transmission; (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	the user account. (3) The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).	
---	IA-6	AUTHENTICATOR FEEDBACK	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
---	IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.	The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.
	IA-8	IDENTIFICATION AND AUTHENTICATION (Non-Organizational Users)	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).
Incident Response					

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
VIIR-1 DCAR-1	IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
VIIR-1	IR-2	INCIDENT RESPONSE TRAINING	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations. (2) The organization employs automated mechanisms to provide a	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*].	The organization: a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and b. Provides refresher training [*Assignment: organization-defined frequency*].

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			more thorough and realistic training environment.		
VIIR-1	IR-3	INCIDENT RESPONSE TESTING AND EXERCISES	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results. Control Enhancement: (1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.	The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.	Not Applicable
VIIR-1 E3.3.9	IR-4	INCIDENT HANDLING	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly. Control Enhancement:	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(1) The organization employs automated mechanisms to support the incident handling process.	Control Enhancement: (1) The organization employs automated mechanisms to support the incident handling process.	
VIIR-1	IR-5	INCIDENT MONITORING	The organization tracks and documents information system security incidents. Control Enhancement: (1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	The organization tracks and documents information system security incidents.	The organization tracks and documents information system security incidents.
VIIR-1 E3.3.9	IR-6	INCIDENT REPORTING	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities. Control Enhancement: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities. Control Enhancement: (1) The organization employs automated mechanisms to assist in the reporting of security incidents.	The organization: a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and b. Reports security incident information to designated authorities.
---	IR-7	INCIDENT RESPONSE ASSISTANCE	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and	The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and	The organization provides an incident response support resource, integral to the organizational incident response capability, that

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			assistance to users of the information system for the handling and reporting of security incidents. Control Enhancement: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	assistance to users of the information system for the handling and reporting of security incidents. Control Enhancement: (1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.	offers advice and assistance to users of the information system for the handling and reporting of security incidents.
	IR-8	INCIDENT RESPONSE PLAN	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an	The organization: a. Develops an incident response plan that: - Provides the organization with a roadmap for implementing its incident response capability; - Describes the structure and organization of the incident response capability; - Provides a high-level approach for how the incident response capability fits into the overall organization; - Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; - Defines reportable incidents; - Provides metrics for measuring the incident response capability within the organization. - Defines the resources and management support needed to effectively maintain and mature an

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			- Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].	incident response capability; and - Is reviewed and approved by designated officials within the organization; b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*]; c. Reviews the incident response plan [*Assignment: organization-defined frequency*]; d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].
Maintenance					
PRMP-1 DCAR-1	MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented information system maintenance policy that

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.	addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. .
---	MA-2	CONTROLLED MAINTENANCE	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning properly	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning	The organization: (a) schedules, performs, documents and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (b) controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (c) requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (d) sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			following maintenance or repair actions. (1) Control Enhancements: The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable). (2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.	properly following maintenance or repair actions. (1) Control Enhancements: The organization maintains maintenance records for the information system that include: (a) Date and time of maintenance; (b) Name of the individual performing the maintenance; (c) Name of escort, if necessary; (d) A description of the maintenance performed; and (e) A list of equipment removed or replaced (including identification numbers, if applicable).	maintenance or repairs; and (e) checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
---	MA-3	MAINTENANCE TOOLS	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Control Enhancements: (1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious	The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools. Control Enhancements: (1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			improper modifications. Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system. (2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system. (3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.	obvious improper modifications. Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system. (2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.	
EBRP-1	MA-4	NON-LOCAL MAINTENANCE	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;	The organization: a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities; b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; c. Employs strong identification and authentication techniques in the establishment of non-local

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. Control Enhancements: (1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. (2) The organization documents, in the security plan for the information (3) The organization: (a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or (b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants)	d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed. Control Enhancements: (1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions. (2) The organization documents, in the security plan for the information	maintenance and diagnostic sessions; d. Maintains records for non-local maintenance and diagnostic activities; and e. Terminates all sessions and network connections when non-local maintenance is completed.

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			before reconnecting the component to the information system.		
PRMP-1	MA-5	MAINTENANCE PERSONNEL	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	The organization: a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.
COMS-1 COSP-1	MA-6	TIMELY MAINTENANCE	The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.	Not Applicable
Media Protection					

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
PESP-1 DCAR-1	MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.
PEDI-1 PEPF-1	MP-2	MEDIA ACCESS	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Control Enhancement: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures]. Control Enhancement: (1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.	The organization restricts access to [Assignment: organization-defined types of digital and non-digital media] to [Assignment: organization-defined list of authorized individuals] using [Assignment: organization-defined security measures].
ECML-1	MP-3	MEDIA MARKING	The organization: a. Marks, in accordance with	The organization: a. Marks, in accordance with	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].	
PESS-1	MP-4	MEDIA STORAGE	The organization: a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	The organization: a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*]; b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	Not Applicable
---	MP-5	MEDIA TRANSPORT	The organization: a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined*	The organization: a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-*	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			security measures]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (2) The organization documents activities associated with the transport of information system media. (3) The organization employs an identified custodian throughout the transport of information system media. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	*defined security measures*]; b. Maintains accountability for information system media during transport outside of controlled areas; and c. Restricts the activities associated with transport of such media to authorized personnel. Control Enhancements: (2) The organization documents activities associated with the transport of information system media. (4) The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	
PECS-1 PEDD-1	MP-6	MEDIA SANITIZATION	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. Control Enhancements: (1) The organization tracks, documents, and verifies media sanitization and disposal actions. (2) The organization tests sanitization	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*]. (3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].		
PEDD-1	MP-7	MEDIA DESTRUCTION AND DISPOSAL	Withdrawn from SP 800-53, Rev. 3	Withdrawn from SP 800-53, Rev. 3	Withdrawn from SP 800-53, Rev. 3
			Physical and Environmental Protection		
PETN-1 DCAR-1	PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PECF-1	PE-2	PHYSICAL ACCESS AUTHORIZATIONS	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.	The organization: a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); b. Issues authorization credentials; c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.
PEPF-1	PE-3	PHYSICAL ACCESS CONTROL	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; e. Secures keys, combinations, and	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;	The organization: a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); b. Verifies individual access authorizations before granting access to the facility; c. Controls entry to the facility containing the information system using physical access devices and/or guards; d. Controls access to areas officially designated as publicly accessible in accordance with the organization's

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated. Control Enhancements: (1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.	e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	assessment of risk; e. Secures keys, combinations, and other physical access devices; f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
	PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	The organization controls physical access to information system distribution and transmission lines within organizational facilities.	Not Applicable
PEDI-1 PEPF-1	PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	Not Applicable
PEPF-2	PE-6	MONITORING PHYSICAL ACCESS	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and	The organization: a. Monitors physical access to the information system to detect and respond to physical security incidents; b. Reviews physical access logs [*Assignment: organization-defined*

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			c. Coordinates results of reviews and investigations with the organization's incident response capability. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment. (2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.	c. Coordinates results of reviews and investigations with the organization's incident response capability. Control Enhancements: (1) The organization monitors real-time physical intrusion alarms and surveillance equipment.	*frequency*]; and c. Coordinates results of reviews and investigations with the organization's incident response capability.
PEVC-1	PE-7	VISITOR CONTROL	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancement: (1) The organization escorts visitors and monitors visitor activity, when required.	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible. Control Enhancement: (1) The organization escorts visitors and monitors visitor activity, when required.	The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.
PEPF-2 PEVC-1	PE-8	ACCESS RECORDS	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and b. Reviews visitor access records	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and	The organization: a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			[*Assignment: organization-defined frequency*]. Control Enhancements: (1) The organization employs automated mechanisms to facilitate the maintenance and review of access records. (2) The organization maintains a record of all physical access, both visitor and authorized individuals.	b. Reviews visitor access records [*Assignment: organization-defined frequency*].	b. Reviews visitor access records [*Assignment: organization-defined frequency*].
---	PE-9	POWER EQUIPMENT AND POWER CABLING	The organization protects power equipment and power cabling for the information system from damage and destruction.	The organization protects power equipment and power cabling for the information system from damage and destruction.	Not Applicable
PEMS-1	PE-10	EMERGENCY SHUTOFF	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	The organization: a. Provides the capability of shutting off power to the information system or individual system components in emergency situations; b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and c. Protects emergency power shutoff capability from unauthorized activation.	Not Applicable
COPS-1	PE-11	EMERGENCY	The organization provides a short-term uninterruptible power supply to facilitate	The organization provides a short-term uninterruptible power supply to	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
COPS-2 COPS-3		POWER	an orderly shutdown of the information system in the event of a primary power source loss. Control Enhancement: (1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
PEEL-1	PE-12	EMERGENCY LIGHTING	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
PEFD-1 PEFS-1	PE-13	FIRE PROTECTION	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancements: (1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source. Control Enhancements: (1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire. (2) The organization employs fire	The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders. (3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.	
PEHC-1 PETC-1	PE-14	TEMPERATURE AND HUMIDITY CONTROLS	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].	The organization: a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].
---	PE-15	WATER DAMAGE PROTECTION	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel. Control Enhancement: (1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
---	PE-16	DELIVERY AND REMOVAL	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.	The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.
EBRU-1	PE-17	ALTERNATE WORK SITE	The organization: a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	The organization: a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites; b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.	Not Applicable
	PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. Control Enhancements: (1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the	The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			physical and environmental hazards in its risk mitigation strategy.		
	PE-19	INFORMATION LEAKAGE	Not Applicable	Not Applicable	Not Applicable
			Planning		
DCAR-1 E3.4.6	PL-1	SECURITY PLANNING POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.
DCSD-1	PL-2	SYSTEM SECURITY PLAN	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of	The organization: a. Develops a security plan for the information system that: - Is consistent with the organization's enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	of the information system in terms of missions and business processes; - Provides the security category and impact level of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
					implementation or security control assessments.
5.7.5	PL-3	SYSTEM SECURITY PLAN UPDATE	Withdrawn: Incorporated into PL-2.	Withdrawn: Incorporated into PL-2.	Withdrawn: Incorporated into PL-2.
5.7.5 PRRB-1	PL-4	RULES OF BEHAVIOR	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	The organization: a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.
---	PL-5	PRIVACY IMPACT ASSESSMENT	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.	The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.
	PL-6	SECURITY-RELATED ACTIVITY PLANNING	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets,	Not Applicable

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
				and individuals.	
Personnel Security					
PRRB-1 DCAR-1	PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.
---	PS-2	POSITION CATEGORIZATION	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].	The organization: a. Assigns a risk designation to all positions; b. Establishes screening criteria for individuals filling those positions; and c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].
PRAS-1	PS-3	PERSONNEL SCREENING	The organization: a. Screens individuals prior to authorizing access to the information system; and	The organization: a. Screens individuals prior to authorizing access to the information system; and	The organization: a. Screens individuals prior to authorizing access to the information system; and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].	b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].
5.12.7	PS-4	PERSONNEL TERMINATION	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.	The organization, upon termination of individual employment: a. Terminates information system access; b. Conducts exit interviews; c. Retrieves all security-related organizational information system-related property; and d. Retains access to organizational information and information systems formerly controlled by terminated individual.
5.12.7	PS-5	PERSONNEL TRANSFER	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].	The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].
PRRB-1	PS-6	ACCESS AGREEMENTS	The organization: a. Ensures that individuals requiring	The organization: a. Ensures that individuals requiring	The organization: a. Ensures that individuals requiring

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].	access to organizational information and information systems sign appropriate access agreements prior to being granted access; and b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].
5.7.10	PS-7	THIRD-PARTY PERSONNEL SECURITY	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.	The organization: a. Establishes personnel security requirements including security roles and responsibilities for third-party providers; b. Documents personnel security requirements; and c. Monitors provider compliance.
PRRB-1	PS-8	PERSONNEL SANCTIONS	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
Risk Assessment					
DCAR-1	RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.	compliance; and b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
E3.4.2	RA-2	SECURITY CATEGORIZATION	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.
DCDS-1 DCII-1 E3.3.10	RA-3	RISK ASSESSMENT	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results in [*Selection: security plan; risk*	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment results	The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; b. Documents risk assessment

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			assessment report; [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]]; c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
DCAR-1 DCII-1	RA-4	RISK ASSESSMENT UPDATE	Withdrawn: Incorporated into RA-3.	Withdrawn: Incorporated into RA-3.	Withdrawn: Incorporated into RA-3.
ECMT-1 VIVM-1	RA-5	VULNERABILITY SCANNING	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote	The organization: a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that promote

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned. (2) The organization updates the list of	interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). Control Enhancements: (1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	interoperability among tools and automate parts of the vulnerability management process by using standards for: - Enumerating platforms, software flaws, and improper configurations; - Formatting and making transparent, checklists and test procedures; and - Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported. (3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked). (4) The organization attempts to discern what information about the information system is discoverable by adversaries. (5) The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning. (7) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.		
System and Services Acquisition					
DCAR-1	SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		PROCEDURES	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.	a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.
DCPB-1 E3.3.4	SA-2	ALLOCATION OF RESOURCES	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.	The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.
5.8.1	SA-3	LIFE CYCLE SUPPORT	The organization: a. Manages the information system using a system development life cycle methodology that includes information	The organization: a. Manages the information system using a system development life cycle methodology that includes information	The organization: a. Manages the information system using a system development life cycle methodology that includes

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.	information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.
DCAS-1 DCDS-1 DCIT-1 DCMC-1	SA-4	ACQUISITIONS	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Control Enhancements: (1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. Control Enhancements: (1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or	The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls. (4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.	
DCCS-1 DCHW-1 DCID-1 DCSD-1 DCSW-1 ECND-1 DCFA-1	SA-5	INFORMATION SYSTEM DOCUMENTATION	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized	The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			- User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. Control Enhancements: (1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. (2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing. (3) The organization obtains, protects	personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. Control Enhancements: (1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. (3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation	personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	
DCPD-1	SA-6	SOFTWARE USAGE RESTRICTIONS	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
---	SA-7	USER INSTALLED SOFTWARE	The organization enforces explicit rules governing the installation of software by users.	The organization enforces explicit rules governing the installation of software by users.	The organization enforces explicit rules governing the installation of software by users.
DCBP-1 DCCS-1	SA-8	SECURITY DESIGN PRINCIPLES	The organization applies information system security engineering principles in the specification, design,	The organization applies information system security engineering principles in the specification, design,	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
E3.4.4			development, implementation, and modification of the information system.	development, implementation, and modification of the information system.	
DCDS-1 DCID-1 DCIT-1 DCPP-1	SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.	The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers.
---	SA-10	DEVELOPER CONFIGURATION MANAGEMENT	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes;	The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes;	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	d. Document approved changes to the information system; and e. Track security flaws and flaw resolution.	
E3.4.4	SA-11	DEVELOPER SECURITY TESTING	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes.	Not Applicable
	SA-12	SUPPLY CHAIN PROTECTION	The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.	Not Applicable	Not Applicable
	SA-13	TRUSTWORTHI-NESS	The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].	Not Applicable	Not Applicable
	SA-14	CRITICAL INFORMATION	Not Applicable	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
		SYSTEM COMPONENTS			
System and Communications Protection					
DCAR-1	SC-1	SYSTEM AND COMMUNICA-TIONS PROTECTION POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.
DCPA-1	SC-2	APPLICATION PARTITIONING	The information system separates user functionality (including user interface services) from information system management functionality.	The information system separates user functionality (including user interface services) from information system management functionality.	Not Applicable
DCSP-1	SC-3	SECURITY FUNCTION ISOLATION	The information system isolates security functions from nonsecurity functions.	Not Applicable	Not Applicable
ECRC-1	SC-4	INFORMATION IN SHARED RESOURCES	The information system prevents unauthorized and unintended information transfer via shared system	The information system prevents unauthorized and unintended information transfer via shared	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			resources.	system resources.	
---	SC-5	DENIAL OF SERVICE PROTECTION	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].	The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].
---	SC-6	RESOURCE PRIORITY	Not Applicable	Not Applicable	Not Applicable
COEB-1 EBBD-1 ECIM-1 ECVI-1	SC-7	BOUNDARY PROTECTION	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. (2) The information system prevents public access into the organization's	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. Control Enhancements: (1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces. (2) The information system prevents public access into the organization's	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. (3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. (4) The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. (5) The information system at managed interfaces, denies network traffic by	internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. (3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. (4) The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. (5) The information system at	

References			Task Order Requirement		
DoDI 8500.2	**NIST 800-53**	**CONTROL NAME**	**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			default and allows network traffic by exception (i.e., deny all, permit by exception). (6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. (7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. (8) The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.	managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). (7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	
ECTM-1	SC-8	TRANSMISSION INTEGRITY	The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected	The information system protects the integrity of transmitted information. Control Enhancements: (1) The organization employs cryptographic mechanisms to recognize changes to information	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			by alternative physical measures.	during transmission unless otherwise protected by alternative physical measures.	
ECCT-1	SC-9	TRANSMISSION CONFIDENTIALITY	The information system protects the confidentiality of transmitted information. Control Enhancement: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	The information system protects the confidentiality of transmitted information. Control Enhancement: (1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.	Not Applicable
---	SC-10	NETWORK DISCONNECT	The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.	Not Applicable
	SC-11	TRUSTED PATH	Not Applicable	Not Applicable	Not Applicable
IAKM-1	SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	The organization establishes and manages cryptographic keys for required cryptography employed within the information system. Control Enhancement: (1) The organization maintains availability of information in the event of the loss of cryptographic keys by users.	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
IAKM-1 IATS-1	SC-13	USE OF CRYPTOGRAPHY	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
EBPW-1	SC-14	PUBLIC ACCESS PROTECTIONS	The information system protects the integrity and availability of publicly available information and applications.	The information system protects the integrity and availability of publicly available information and applications.	The information system protects the integrity and availability of publicly available information and applications.
ECVI-1	SC-15	COLLABORATIVE COMPUTING DEVICES	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.	The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and b. Provides an explicit indication of use to users physically present at the devices.
	SC-16	TRANSMISSION OF SECURITY ATTRIBUTES	Not Applicable	Not Applicable	Not Applicable
IAKM-1	SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
DCMC-1	SC-18	MOBILE CODE	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system.	Not Applicable
ECVI-1	SC-19	VOICE OVER INTERNET PROTOCOL	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and b. Authorizes, monitors, and controls the use of VoIP within the information system.	Not Applicable
	SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (Authoritative Source)	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child	The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. Control Enhancements: (1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			supports secure resolution services) enable verification of a chain of trust among parent and child domains.	supports secure resolution services) enable verification of a chain of trust among parent and child domains.	child supports secure resolution services) enable verification of a chain of trust among parent and child domains.
	SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (Recursive or Caching Resolver)	The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.	Not Applicable	Not Applicable
	SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.	Not Applicable
	SC-23	SESSION AUTHENTICITY	The information system provides mechanisms to protect the authenticity of communications sessions.	The information system provides mechanisms to protect the authenticity of communications sessions.	Not Applicable
	SC-24	FAIL IN KNOWN STATE	The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.	Not Applicable	Not Applicable
	SC-25	THIN NODES	Not Applicable	Not Applicable	Not Applicable

References		**CONTROL NAME**	**Task Order Requirement**		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
	SC-26	HONEYPOTS	Not Applicable	Not Applicable	Not Applicable
	SC-27	OPERATING SYSTEM-INDEPENDENT APPLICATIONS	Not Applicable	Not Applicable	Not Applicable
	SC-28	PROTECTION OF INFORMATION AT REST	The information system protects the confidentiality and integrity of information at rest.	The information system protects the confidentiality and integrity of information at rest.	Not Applicable
	SC-29	HETEROGENEITY	Not Applicable	Not Applicable	Not Applicable
	SC-30	VIRTUALIZATION TECHNIQUES	Not Applicable	Not Applicable	Not Applicable
	SC-31	COVERT CHANNEL ANALYSIS	Not Applicable	Not Applicable	Not Applicable
	SC-32	INFORMATION SYSTEM PARTITIONING	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.	Not Applicable
	SC-33	TRANSMISSION PREPARATION INTEGRITY	Not Applicable	Not Applicable	Not Applicable
	SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Not Applicable	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			System and Information Integrity		
DCAR-1	SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.	The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]: a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.
DCSQ-1 DCCT-1 E.3.3.5.7	SI-2	FLAW REMEDIATION	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. Control Enhancements: (1) The organization centrally manages the flaw remediation process and installs software updates automatically.	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process. Control Enhancement: (2) The organization employs automated mechanisms [*Assignment:*	The organization: a. Identifies, reports, and corrects information system flaws; b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and c. Incorporates flaw remediation into the organizational configuration management process.

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	*organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.	
ECVP-1 VIVM-1	SI-3	MALICIOUS CODE PROTECTION	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;	The organization: a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code: - Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or - Inserted through the exploitation of information system vulnerabilities; b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: - Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			- [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions). (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.	and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Control Enhancements: (1) The organization centrally manages malicious code protection mechanisms. (2) The information system automatically updates malicious code protection mechanisms (including signature definitions). (3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.	downloaded, opened, or executed in accordance with organizational security policy; and - [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.
EBBD-1 EBVC-1 ECID-1	SI-4	INFORMATION SYSTEM MONITORING	The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i)	The organization: a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks; b. Identifies unauthorized use of the information system; c. Deploys monitoring devices: (i)	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. Control Enhancements: (2) The organization employs automated tools to support near real-time analysis of events. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise*	strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. Control Enhancements: (2) The organization employs automated tools to support near real-time analysis of events. (4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. (5) The information system provides near real-time alerts when the following indications of compromise or	

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	**NIST 800-53**		**High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)**	**Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)**	**Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)**
			indicators]. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	potential compromise occur: [*Assignment: organization-defined list of compromise indicators*]. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	
VIVIM-1	SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. Control Enhancement: (1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	The organization: a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis; b. Generates internal security alerts, advisories, and directives as deemed necessary; c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.
DCSS-1	SI-6	SECURITY FUNCTIONALITY	The information system verifies the correct operation of security functions	Not Applicable	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
		VERIFICATION	[*Selection (one or more):* [*Assignment: organization-defined system transitional states*]*; upon command by user with appropriate privilege; periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.		
ECSD-2	SI-7	SOFTWARE AND INFORMATION INTEGRITY	The information system detects unauthorized changes to software and information. Control Enhancements: (1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system. (2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.	The information system detects unauthorized changes to software and information. Control Enhancement: (1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.	Not Applicable
---	SI-8	SPAM PROTECTION	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited	The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures. Control Enhancement: (1) The organization centrally manages spam protection mechanisms.	messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	
---	SI-9	INFORMATION INPUT RESTRICTIONS	The organization restricts the capability to input information to the information system to authorized personnel.	The organization restricts the capability to input information to the information system to authorized personnel.	Not Applicable
---	SI-10	INFORMATION INPUT VALIDATION	The information system checks the validity of information inputs.	The information system checks the validity of information inputs.	Not Applicable
---	SI-11	ERROR HANDLING	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel.	Not Applicable

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
PESP-1	SI-12	INFORMATION OUTPUT HANDLING AND RETENTION	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.	The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.
	SI-13	PREDICTABLE FAILURE PREVENTION	Not Applicable	Not Applicable	Not Applicable
Program Management					
	PM-1	INFORMATION SECURITY PROGRAM PLAN	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is	The organization: a. Develops and disseminates an organization-wide information security program plan that: - Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; - Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.	intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; - Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance; - Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.
	PM-2	SENIOR INFORMATION SECURITY OFFICER	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.	The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
	PM-3	INFORMATION SECURITY RESOURCES	The organization: a. Ensures that all capital planning and investment requests include the	The organization: a. Ensures that all capital planning and investment requests include the	The organization: a. Ensures that all capital planning and investment requests include the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.	resources needed to implement the information security program and documents all exceptions to this requirement; b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and c. Ensures that information security resources are available for expenditure as planned.
	PM-4	PLAN OF ACTION AND MILESTONES PROCESS	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.	The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.
	PM-5	INFORMATION SYSTEM INVENTORY	The organization develops and maintains an inventory of its information systems.	The organization develops and maintains an inventory of its information systems.	The organization develops and maintains an inventory of its information systems.
	PM-6	INFORMATION SECURITY MEASURES OF PERFORMANCE	The organization develops, monitors, and reports on the results of information security measures of performance.	The organization develops, monitors, and reports on the results of information security measures of performance.	The organization develops, monitors, and reports on the results of information security measures of performance.
	PM-7	ENTERPRISE ARCHITECTURE	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and	The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals,

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			Nation.	the Nation.	other organizations, and the Nation.
	PM-8	CRITICAL INFRASTRUCTURE PLAN	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.	The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
	PM-9	RISK MANAGEMENT STRATEGY	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.	The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and b. Implements that strategy consistently across the organization.
	PM-10	SECURITY AUTHORIZATION PROCESS	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.	The organization: a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c. Fully integrates the security authorization processes into an organization-wide risk management program.
	PM-11	MISSION/ BUSINESS PROCESS DEFINITION	The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to	The organization: a. Defines mission/business processes with consideration for information security and the resulting	The organization: a. Defines mission/business processes with consideration for information security and the

References		CONTROL NAME	Task Order Requirement		
DoDI 8500.2	NIST 800-53		High-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC I (DoDI 8500.2)	Moderate-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC II (DoDI 8500.2)	Low-Impact Information System (FIPS Pub 200 / NIST SP 800-53) MAC III (DoDI 8500.2) (generally commercial best practices)
			organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

(END OF ATTACHMENT J-3)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Sept 1, 2012 - Sept 30, 2012

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Oct 1, 2012 - Oct 31, 2012

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Nov 1, 2012 - Nov 30, 2012

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Dec 1, 2012 - Dec 31, 2012

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Jan 1, 2013 - Jan 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Feb 1, 2013 - Feb 28, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: March 1, 2013 - March 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: April 1, 2013 - April 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: May 1, 2013 - May 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: June 1, 2013 - June 30, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Business Volume (Sales) Report

Reporting Period: July 1, 2013 - July 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: Aug 1, 2013 - Aug 31, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

Attachment J-5
CS2 MONTHLY BUSINESS VOLUME (SALES) REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Business Volume (Sales) Report
Reporting Period: September 1, 2013 - September 30, 2013

	Date of Order	Agency Name/ Ordering Activity	Description of Services	Period of Performance	Task Order / Delivery Order Number	Total Value of Order Received
1						
2						
3						
4						
5						
6						
7						
8						
9						
					Total Sales this Month	$0.00
					Cumulative Sales to Date	$0.00

(END OF ATTACHMENT J-5)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Revenue Report

Reporting Period: Sept 1, 2012 - Sept 30, 2012

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Oct 1, 2012 - Oct 31, 2012

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Nov 1, 2012 - Nov 30, 2012

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Dec 1, 2012 - Dec 31, 2012

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Jan 1, 2013 - Jan 31, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Revenue Report

Reporting Period: Feb 1, 2013 - Feb 28, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Mar 1, 2013 - Mar 31, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Revenue Report

Reporting Period: Apr 1, 2013 - Apr 30, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Revenue Report

Reporting Period: May 1, 2013 - May 31, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Jun 1, 2013 - Jun 30, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Jul 1, 2013 - Jul 31, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx
CS2 Monthly Revenue Report
Reporting Period: Aug 1, 2013 - Aug 31, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-6
CS2 MONTHLY REVENUE REPORT FORMAT

Contractor Name

GSA Contract Number: GSxxxxxxxxxxxx

CS2 Monthly Revenue Report

Reporting Period: September 1, 2013 - September 30, 2013

	Date Received Payment	Agency Name/ Ordering Activity	Description of Services	Task Order/ Delivery Order Number	Total Value of Order	Amount Received	GSA Management Fee Collected (2%)	GSA Management Fee Remitted	Remaining Balance of Un-remitted GSA Management Fee
1									
2									
3									
4									
5									
6									
7									
8									
9									
				TOTALS	$0.00	$0.00	$0.00	$0.00	$0.00

EFT Number: **Amount:**

EFT Number: **Amount:**

(END OF ATTACHMENT J-6)

ATTACHMENT J-9
Sample Task Order (STO) #1 - MORALE, WELFARE, AND RECREATION SERVICES (MWR)

1 MWR BACKGROUND

1.1 Historically, deployed service members kept in touch with their family and friends with a letter or an occasional telephone call. With the rapid expansion and availability of the Internet, e-mail is taking the place of these more traditional communication methods. Now, deployed service members will be provided high-speed commercial Internet access supporting communications applications, including e-mail, voice calls and video teleconferencing, to better keep in touch with family and friends.

1.2 The United States Government (USG) intends to provide IP Voice, Video, and Data services via multiple Very Small Aperture Terminal (VSAT) satellite networks to Department of Defense (DoD) and Partner Nation Elements throughout the world. USG requires satellite IP services to support Morale, Welfare, and Recreation (MWR) and other non-Global Information Grid (GIG) operations in the Central Command (CENTCOM), African Command (AFRICOM), European Command (EUCOM), and Pacific Command (PACOM) Areas of Responsibility (AORs), as well as the British Indian Ocean Trust (BIOT) Territory. This Sample Task addresses the general parameters and requirements to provide the required satellite IP services. The system shall be flexible and adaptable to service personnel in the regions cited above, including hostile locations.

2 MWR REQUIREMENTS. A requirement exists to provide an MWR system to support DoD in-theater operations. Include solutions to requirements as part of the following documentation:

2.1 Project Planning: The Contractor shall develop a Service Plan in accordance with Section C. The Service Plan should include a description of the systems, a network diagram, procedures and performance metrics to put in place to assure successful and timely completion of the Task, procedures explaining how subcontractors will be managed (if applicable), a description of how costs will be controlled, and a plan to ensure timely submission of invoices. Additionally, include a description of the process(es) that the Contractor will use to interface with the appropriate Government Representative(s). The Service Plan shall include a project implementation schedule. The Service Plan shall address all assumptions, risks and resultant mitigation plans associated with the proposed solution.

2.2 MWR Infrastructure: The Contractor shall develop and implement the requisite communications infrastructure to support the MWR mission. The Contractor shall select a solution which provides an optimum lifecycle cost-benefit ratio. Identify chosen systems and explain rationale for selection, including lifecycle cost considerations, incorporating lessons learned when possible. Provide a detailed architecture and explain all required interfaces. The Contractor shall provide link budgets, as applicable. A network operations center (NOC) shall be employed to manage connectivity and network assets for the period of performance. The Contractor's solution shall address reliability, availability, maintainability, and security. The Contractor shall explain what network monitoring and status information will be provided to the Government on a recurring basis, how often it will be provided and in what format. The Contractor shall demonstrate the ability to comply with the Federal Information Security Management Act of 2002 as implemented by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "*Recommended Security Controls for Federal Information Systems and Organizations*" for a moderate impact information system, specifically addressing the following controls: CA-2, IA-2 and SI-3. Regarding CA-2, a security assessment plan is not required prior to contract award. The Agency specification for assessment of security controls in the information system is that they must be assessed annually. Regarding IA-2, there is no Agency specification for Control Enhancement (8), so it is per contractor system determination. Regarding SI-3, there is no Agency specification, so the values are per contractor system determination. The Contractor shall demonstrate the ability to comply with Committee on National Security Systems Policy (CNSSP) 12. See Section J, Attachment J-3 for additional details on Information Assurance.

2.3 Site Configuration and Locations: The MWR system consists of two types of Remote Deployable Units (RDUs). The RDUs shall be comprised of the equipment listed below plus transportable antenna, a temporary shelter with the workstation configurations listed below, 24-hour temporary power backup device plus other equipment the Contractor determines is required. All equipment shall be capable of being easily repacked and shipped by onsite Government personnel, and the overall MWR system shall be capable of supporting site redeployments, including areas outside the initial deployment regions. The contractor shall provide a portability plan for redeployment of sites to other regions in the event the government's requirements for MWR change.

2.3.1 <u>Large Remote Deployable Units (LRDUs)</u> - Contains 8 VoIP phones, 20 laptop computers w/ webcams. 200 LRDUs are required to be shipped to Iraq, 150 LRDU's to Afghanistan, 15 LRDUs to Poland, 10 LRDUs to Serbia, 12 LRDUs to Mali and 8 LRDUs to South Korea.

2.3.2 <u>Outpost Remote Deployable units (ORDUs)</u> - Contains 3 VoIP phones, 5 laptop computers w/ webcams. 30 ORDUs are required to be shipped to Iraq and 18 ORDU's are required to be shipped to Afghanistan and 10 ORDUs shall be shipped to Bangladesh.

2.4 Engineering Support: The Contractor shall provide the results of MWR system engineering studies to provide a clearly explained recommendation for bandwidth and per-site Committed Information Rate (CIR) for each RDU, stating assumptions. The Contractor shall propose the method for implementing Quality of Service (QoS) to ensure prioritization of traffic (VOIP, video and data) categories. The Contractor shall engineer the MWR communications architecture, including capacity planning and preparing and developing designs, plans, and reports. The Contractor shall implement configuration management, prepare engineering documents and reference manuals, and provide engineering, installation, configuration and testing services for the MWR communications infrastructure. Requirements are expected to grow up to 20% over 3 years, and Contractor engineering studies shall articulate how system expansion can be accommodated at minimum costs and support other potential emerging methods for obtaining cost efficiencies. The Contractor is encouraged to suggest alternative, innovative approaches to achieve desired capabilities. The Offeror is encouraged to use non-proprietary solutions when possible.

2.5 Satellite Access: The Contractor shall provide USG with recommendations for which satellite to use for commercial satellite spectrum. The Contractor shall provide a satellite network availability of at least 99.7%. The Contractor shall propose additional metrics to confirm service levels. The availability will be calculated based on the number of satellite network availability minutes during any calendar month divided by the number of total minutes during the same month. Periods of unavailability include unscheduled events such as network outages, rain fade, and network hardware/software failures. The 99.7% availability is for the entire network to the remote switch, excluding the VOIP phones and personal computers (local area network suite). The period of unavailability is measured across all sites.

2.6 Sustainment: The Contractor shall explain a plan to implement and execute logistics, fielding, training, and O&M support. A phased approach can be considered.

2.6.1 Integrated Logistics Support - Develop and implement a maintenance and supply concept necessary to ensure the order, receipt, delivery and accountability of materials necessary to support delivery of the project within the schedule and budget identified by the Government. Logistics support shall include all hardware/software elements and ancillary items necessary for maintaining an operational schedule.

2.6.2 Training - Explain the required operator and maintenance training plans and courses for the Government.

2.6.3 Operations and Maintenance - The Contractor shall provide qualified technical support for the duration of the task's period of performance. Maintenance support shall include the replacement of defective components, onsite technical support, upgrades to include COTS technology insertion, and any software updates, as recommended by the Contractor engineering support. Operations support includes 24/7 NOC support. The NOC shall support site commissioning by Government personnel with a 4-hour notification period maximum.

2.6.4 EMI/RFI Identification and Resolution - Implement and support EMI/RFI identification and resolution procedures. The Contractor shall explain how EMI/RFI identification and resolution will be communicated to the Government. The Government prefers the Contractor have access to media and voice communications capability capable of protecting "Sensitive, but Unclassified" data.

2.6.5 Network Monitoring - Establish, and provide the USG access to, a common Net Ops web portal to present the health of the entire solution in a consolidated view using data from multiple sources. The USG prefers the capability to receive alarms (e.g., interference, anomalies) in an automated way, vice a trouble ticket from an operations center.

2.6.5.1 NetOps metrics shall be collected, at a minimum, on the following network segments:

2.6.5.1.1 Gateway (e.g., Hub throughput, link latency, bit error rate, packet delay variation/jitter, service specific quality of service (QoS), packet loss, transmit power level, receive power level, signal-to-noise ratio (Eb/No), link status; Gateway Terminal high power amplifier (HPA) status, Low Noise Amplifier (LNA) status, converter status, up convert (U/C) attenuator);

2.6.5.1.2 Satellite (e.g., anomalies likely to disrupt service, interference data, spectrum data); and

2.6.5.1.3 Remote (e.g., Remote Terminal HPA status, LNA status, converter status, U/C attenuator; Remote Modem transmit power level, receive power level, Eb/No, link status, throughput, link latency, bit error rate, jitter, service specific QoS, packet loss).

2.6.5.2 The Contractor shall recommend the Net Ops metrics to be collected for each network segment and explain their rationale for including those metrics. The Contractor shall specify the frequency of delivery, retrieval method, and data units (e.g., kbps, dB) and format (e.g., XML, SNMP trap) of each Net Ops metric selected.

2.7 Delivery Schedule: The Government desires that the ORDUs arrive in-country and be commissioned by Contractor personnel within 90 days, and that the LRDUs arrive in-country and be commissioned by Contractor personnel within 180 days.

2.8 Period of Performance: The Period of Performance for MWR is 3 base years, with two 1 year options.

2.9 Priced Line Items: At a minimum, pricing is required for the following line items. The Contractor shall note if certain line items are not separately priced**.** All prices shall be fixed price.

2.9.1 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per month

2.9.2 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Africa per year

2.9.3 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per month

2.9.4 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Southwest Asia / Middle East per year

2.9.5 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per month

2.9.6 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Central Asia per year

2.9.7 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per month

2.9.8 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Pacific per year

2.9.9 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per month

2.9.10 Commercial satellite communications infrastructure (including satellite bandwidth and terrestrial connections) per unit cost – Europe per year

2.9.11 Network operations center (NOC) operations cost

2.9.12 Gateway Site terminal cost

2.9.13 Remote Site terminals cost per unit

2.9.14 Engineering Support cost per month

2.9.15 Sustainment support cost per month (excluding Onsite Technical Support)

2.9.16 Onsite Technical Support – Africa per day

2.9.17 Onsite Technical Support – Southwest Asia / Middle East per day

2.9.18 Onsite Technical Support – Central Asia per day

2.9.19 Onsite Technical Support – Pacific per day

2.9.20 Onsite Technical Support – Europe per day

2.9.21 Travel can be charged as Other Direct Costs (ODC) and is not required as part of the STO pricing.

(END OF ATTACHMENT J-9)

SECTION J
LIST OF DOCUMENTS, EXHIBITS, AND OTHER ATTACHMENTS

J.1 LIST OF ATTACHMENTS

J.1.1 ATTACHMENT J-1 – Acronyms and Abbreviations

J.1.2 ATTACHMENT J-2 – Information Assurance Minimum Security Controls Checklist

J.1.3 ATTACHMENT J-3 – Security Controls for Information Systems

J.1.4 ATTACHMENT J-4 – DELETED

J.1.5 ATTACHMENT J-5 – CS2 Monthly Business Volume (Sales) Report Format

J.1.6 ATTACHMENT J-6 – CS2 Monthly Revenue Report Format

J.1.7 ATTACHMENT J-7 – DELETED

J.1.8 ATTACHMENT J-8 – DELETED

J.1.9 ATTACHMENT J-9 – STO #1 - Morale, Welfare, and Recreation Services (MWR)

J.1.10 ATTACHMENT J-10 – STO #2 - Government Education and Training Network (GETN)

J.1.11 ATTACHMENT J-11 – Central Classroom Sites for STO #2: GETN STO

J.1.12 ATTACHMENT J-12 – STO #3 - Blue Personnel Tracking

(END OF SECTION J)