

Company Name:
Northrop Grumman

Contract Number:
HSHQDC-06-D-00022 (HSHQDC06D00022)

Order Number:
HSCETC-09-J-00002 (HSCETC09J00002)

Requisition/Reference Number:
SDD-08-DC05C (SDD08DC05C)

Latest Modification Processed:
P00001

Period of Performance:
1/4/2009 through 1/3/2013

Services Provided:
Task Order award for the Bed Space, Transportation and Detainee Location Tracking System (BST&T).

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 11/04/2008	2. CONTRACT NO. (If any) HSHQDC-06-D-00022	6. SHIP TO: a. NAME OF CONSIGNEE ICE Chief Information Officer
3. ORDER NO. HSCETC-09-J-00002	4. REQUISITION/REFERENCE NO. SDD-08-DC05C	

5. ISSUING OFFICE (Address correspondence to) ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW Washington DC 20536	b. STREET ADDRESS Immigration and Customs Enforcement 801 I Street, NW Suite 700
	c. CITY Washington
	d. STATE DC
	e. ZIP CODE 20536

7. TO: a. NAME OF CONTRACTOR NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC	f. SHIP VIA
b. COMPANY NAME	8. TYPE OF ORDER

c. STREET ADDRESS 7575 COLSHIRE DRIVE	<input type="checkbox"/> a. PURCHASE REFERENCE YOUR:	<input checked="" type="checkbox"/> b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.
d. CITY MCLEAN	e. STATE VA	f. ZIP CODE 221027508
9. ACCOUNTING AND APPROPRIATION DATA See Schedule		10. REQUISITIONING OFFICE Department of Homeland Security

11. BUSINESS CLASSIFICATION (Check appropriate box(es)).				12. F.O.B. POINT Destination	
<input type="checkbox"/> a. SMALL	<input checked="" type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> g. SERVICE-DISABLED VETERAN-OWNED		
<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. HUBZone	<input type="checkbox"/> f. EMERGING SMALL BUSINESS			

13. PLACE OF		14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) Multiple	16. DISCOUNT TERMS
a. INSPECTION Destination	b. ACCEPTANCE Destination			

17. SCHEDULE (See reverse for Rejections)						
ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 064681021 The following is the Task Order award for the Bed Space, Transportation and Detainee Location Tracking System, (BST&T), HSCETC-09-J-00002, under Northrop Grumman's EAGLE Contract HSHQDC-06-D-00022. Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO:				
a. NAME DHS, ICE			\$14,501,669.00	▲
b. STREET ADDRESS (or P.O. Box) Burlington Finance Center P.O. Box 1620 Attn: ICE-OCIO-SDD				17(i) GRAND TOTAL
c. CITY Williston	d. STATE VT	e. ZIP CODE 05495-1620	\$12,209,426.00	▲

22. UNITED STATES OF AMERICA BY (Signature)	23. NAME (Typed) Brooke Bernold TITLE: CONTRACTING/ORDERING OFFICER
--	---

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>The Task Order is a Cost-Plus-Fixed-Fee type contract.</p> <p>1. The period of performance for this Task Order will consist of a one year base and three potential option years. The period of performance is January 4, 2009 through January 3, 2013.</p> <p>2. Incremental funding in the amount of \$12,209,426.00 is hereby provided for this task order.</p> <p>3. The contract amount for the base year is \$14,501,669.00. The total contract amount, including the base year and three option periods, is \$44,348,547.00.</p> <p>4. The task order amounts for the base year and option periods are as follows: Period of Performance: 01/04/2009 to 01/03/2013</p>					
0001	<p>Detainee Location Tracking System: Labor Annual Cost: [REDACTED] b4 Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4		
0001A	<p>Detainee Location Tracking System: Hardware/Software Annual Cost: [REDACTED] b4 Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount: [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP Continued ...</p>	1	LO	[REDACTED] b4		

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

3 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	SYSTEMS DEVELOPMENT SERVICES					
	Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4					
0001B	Detainee Location Tracking System: Materials Annual Cost: \$ [REDACTED] b4 Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
	Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4					
0001C	Detainee Location Tracking System: Travel/Other Direct Costs (ODCs) Annual Cost [REDACTED] b4 Fixed Fee: \$ [REDACTED] b4 Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 Incrementally Funded Amount: \$ [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
	Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4					
0001D	Labor: Network Infrastructure Installation at 19 DRO dedicated facilities, Firm-Fixed-Price (Option Line Item) 02/04/2009 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
	Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
0001E	Equipment: Network Infrastructure Installation at 19-DRO dedicated facilities, Cost-Plus-Fixed-Fee (Option Line Item) 02/04/2009 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		b4	
0002	Central Reservation System: Labor Annual Cost: [REDACTED] Fixed Fee: [REDACTED] Cost-Plus-Fixed-Fee: \$ [REDACTED] Incrementally Funded Amount: \$ [REDACTED] Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: SEE ATTACHMENT A Funded: [REDACTED]	1	LO		b4	
0002A	Central Reservation System: Hardware/Software Annual Cost: [REDACTED] Fixed Fee: [REDACTED] Total Cost-Plus-Fixed-Fee: \$ [REDACTED] Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: SEE ATTACHMENT A Funded: \$ [REDACTED]	1	LO		b4	
0002B	Central Reservation System: Materials Annual Cost: [REDACTED] Fixed Fee: \$ [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: SEE ATTACHMENT A Continued ...	1	LO		b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

5 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008 CONTRACT NO. HSHQDC-06-D-00022

ORDER NO. HSCETC-09-J-00002

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Funded: \$ b4					
0002C	Central Reservation System: Travel/ODCs Annual Cost Fixed Fee: Total Cost-Plus-Fixed-Fee: Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: SEE ATTACHMENT A Funded:	1	LO		b4	
0003	Transportation Management System: Labor Cost-Plus-Fixed-Fee Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES		LO			
0003A	Transportation Management System: Hardware/Software Cost-Plus-Fixed-Fee Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES		LO			
0003B	Transportation Management System: Travel/ODCs Cost-Plus-Fixed-Fee Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES		LO			
1001	Option Year 1. Detainee Location Tracking System: Labor Annual Cost: Fixed Fee: Total Cost-Plus-Fixed-Fee: (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Continued ...	1	LO	b4		b4

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

6 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Funded: \$0.00					
1001A	Option Year 1. Detainee Location Tracking System: Hardware/Software Annual Cost: [REDACTED] b4 Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
1001B	Option Year 1. Detainee Location Tracking System: Materials Annual Cost: [REDACTED] b4 Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
1001C	Option Year 1. Detainee Location Tracking System: Travel/ODCs Annual Cost: [REDACTED] b4 Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO	[REDACTED] b4		
1001D	Option Year 1. Network Infrastructure Installation, Labor, Firm-Fixed-Price (Option Line Item) 01/04/2010 Product/Service Code: D302 Continued ...	1	LO	[REDACTED] b4		

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES					
	Accounting Info: Funded: b4					
1001E	Option Year 1. Network Infrastructure Installation, Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		b4	
	Accounting Info: Funded: b4					
1002	Option Year 1. Central Reservation System: Labor Annual Cost: b4 Fixed Fee: \$ b4 Total Cost-Plus-Fixed-Fee: \$ b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		b4	
	Accounting Info: Funded: b4					
1002A	Option Year 1. Central Reservation System: Hardware/Software Annual Cost: b4 Fixed Fee: b4 Total Cost-Plus-Fixed-Fee: b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		b4	
	Accounting Info: Funded: b4					
1002B	Option Year 1. Central Reservation System: Continued ...	1	LO		b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

8 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Materials Annual Cost [REDACTED] Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4					
1002C	Option Year 1. Central Reservation System: Travel/ODCs Annual Cost [REDACTED] b4 Fixed Fee: [REDACTED] Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO		[REDACTED] b4	
1003	Option Year 1. Transportation Management System: Labor Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO		[REDACTED] b4	
1003A	Option Year 1. Transportation Management System: Hardware/Software Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP Continued ...	1	LO		[REDACTED] b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

9

43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008 CONTRACT NO. HSHQDC-06-D-00022

ORDER NO. HSCETC-09-J-00002

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	SYSTEMS DEVELOPMENT SERVICES					
1003B	Accounting Info: Funded: [REDACTED] b4 Option Year 1. Transportation Management System: Travel/ODCs Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2010 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
2001	Accounting Info: Funded: [REDACTED] b4 Option Year 2. Detainee Location Tracking System: Labor Annual Cost [REDACTED] b4 Fixed Fee: \$ [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
2001A	Accounting Info: Funded: [REDACTED] b4 Option Year 2. Detainee Location Tracking System: Hardware/Software Annual Cost [REDACTED] b4 Fixed Fee: \$ [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[REDACTED] b4	
2001B	Accounting Info: Funded: [REDACTED] b4 Option Year 2. Detainee Location Tracking Continued ...	1	LO		[REDACTED] b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	System: Materials Annual Cost [REDACTED] Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4					
2001C	Option Year 2. Detainee Location Tracking System: Trave/ODCs Annual Cost [REDACTED] Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
2001D	Option Year 2. Network Infrastructure Installation: Labor Firm-Fixed-Price (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
2001E	Option Year 2. Network Infrastructure Installation: Equipment, Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Continued ...	1	LO	[REDACTED] b4		

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES
11 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
2002	Accounting Info: Funded: [b4] Option Year 2. Central Reservation System: Labor Annual Cost [b4] Fixed Fee: [b4] Total Cost-Plus-Fixed-Fee: \$ [b4] (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[b4]	
2002A	Accounting Info: Funded: [b4] Option Year 2. Central Reservation System: Hardware/Software Annual Cost [b4] Fixed Fee: [b4] Total Cost-Plus-Fixed-Fee: \$ [b4] (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[b4]	
2002B	Accounting Info: Funded: [b4] Option Year 2. Central Reservation System: Materials Annual Cost [b4] Fixed Fee: [b4] Total Cost-Plus-Fixed-Fee: \$ [b4] (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO		[b4]	
	Accounting Info: Funded: \$ [b4] Continued ...					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

12 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER

CONTRACT NO.

11/04/2008

HSHQDC-06-D-00022

ORDER NO.

HSCETC-09-J-00002

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
2002C	Option Year 2. Central Reservation System: Travel/ODCs Annual Cost: [REDACTED] Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4	[REDACTED] b4	
2003	Option Year 2. Transportation Management System: Labor Annual Cost: [REDACTED] Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: \$ [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4	[REDACTED] b4	
2003A	Option Year 2. Transportation Management System: Hardware/Software Annual Cost: [REDACTED] Fixed Fee: \$ [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4	[REDACTED] b4	
2003B	Option Year 2. Transportation Management System: Travel/ODCs. Annual Cost: [REDACTED] Fixed Fee: [REDACTED] b4 Continued ...	1	LO	[REDACTED] b4	[REDACTED] b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2011 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4					
3001	Option Year 3. Detainee Location Tracking System: Labor Annual Cost [REDACTED] b4 Fixed-Fee: [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
3001A	Option Year 3. Detainee Location Tracking System: Hardware/Software Annual Cost [REDACTED] b4 Fixed-Fee: [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO	[REDACTED] b4		
3001B	Option Year 3. Detainee Location Tracking System: Materials Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Continued ...	1	LO	[REDACTED] b4		

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
3001C	Accounting Info: Funded: [b4] Option Year 3. Detainee Location Tracking System: Travel/ODCs Annual Cost [b4] Fixed-Fee: [b4] Total Cost-Plus-Fixed-Fee: [b4] (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO	[b4]	[b4]	
3001D	Accounting Info: Funded: [b4] Option Year 3: Network Infrastructure Installation: Labor Firm-Fixed-Price (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO	[b4]	[b4]	
3001E	Accounting Info: Funded: [b4] Option Year 3. Network Infrastructure Installation: Equipment. Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES	1	LO	[b4]	[b4]	
3002	Accounting Info: Funded: [b4] Option Year 3. Central Reservation System: Labor Annual Cost [b4] Fixed Fee: [b4] Continued ...	1	LO	[b4]	[b4]	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

15 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 11/04/2008	CONTRACT NO. HSHQDC-06-D-00022	ORDER NO. HSCETC-09-J-00002
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4					
3002A	Option Year 3. Central Reservation System: Hardware/Software Annual Cost [REDACTED] Fixed-Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO		[REDACTED] b4	
3002B	Option Year 3. Central Reservation System: Materials Annual Cost [REDACTED] Fixed-Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Accounting Info: Funded: [REDACTED] b4	1	LO		[REDACTED] b4	
3002C	Option Year 3. Central Reservation System: Travel/ODCs Annual Cost [REDACTED] Fixed-Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Continued ...	1	LO		[REDACTED] b4	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

16 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER
11/04/2008

CONTRACT NO.
HSHQDC-06-D-00022

ORDER NO.
HSCETC-09-J-00002

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
3003	<p>Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: Funded: [REDACTED] b4</p> <p>Option Year 3. Transportation Management System: Labor Annual Cost [REDACTED] b4 Fixed-Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4	[REDACTED] b4	
3003A	<p>Option Year 3. Transportation Management System: Hardware/Software Cost-Plus-Fixed-Fee (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4	[REDACTED] b4	
3003B	<p>Option Year 3. Transportation Management System: Travel/ODCs Annual Cost [REDACTED] b4 Fixed-Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 (Option Line Item) 01/04/2012 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4	[REDACTED] b4	
Continued ...						

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

17 43

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER
11/04/2008

CONTRACT NO.
HSHQDC-06-D-00022

ORDER NO.
HSCETC-09-J-00002

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	The total amount of award: \$44,348,547.00. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

B. Supplies or Services/Prices	19
B-1 Items to be Acquired	19
B-2 Contract Pricing	20
C. Description/Specifications	22
D. Packaging and Marking	23
E. Inspection and Acceptance	24
FAR 52.246-5 E-1 Inspection of Services - Cost-Reimbursement. (APR 1984)	24
F. Deliveries or Performance	25
G. Contract Administration Data	26
G-1 TASK ORDER ADMINISTRATION	26
H. Special Contract Requirements	29
I. Contract Clauses	32
FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)	32
FAR 52.204-2 Security Requirements	32
FAR 52.217-7 Option for Increased Quantity- Separately Priced Line Item (MAR 1989)	33
FAR 52.217-8 Option to Extend Services (Nov 1999)	33
FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000)	33
FAR 52.223-14 Toxic Chemical Release Reporting (AUG 2003)	33
FAR 52.232-19 Availability of Funds for the Next Fiscal Year. (APR 1984)	35
FAR 52.232-22 Limitation of Funds (APR 1984)	35
HSAR 3052.204-70 Security requirements for unclassified information technology resources. (JUN 2006)	37
HSAR 3052.204-71 Contractor employee access. Alternate I (JUN 2006)	38
HSAR 3052.209-70 Prohibition on contracts with corporate expatriates. (JUN 2006)	40
HSAR 3052.211-70 Index for specifications. (DEC 2003)	42
HSAR 3052.219-70 Small business subcontracting plan reporting. (JUN 2006)	42
HSAR 3052.245-70 Government property reports. (JUN 2006)	42
J. List of Documents, Exhibits and Other Attachments	43

B. Supplies or Services/Prices

B-1 Items to be Acquired

The Contractor shall furnish all personnel, facilities, equipment, material, supplies, and services (except as may be expressly set forth in this contract as furnished by the Government) and otherwise do all things necessary to, or incident to, performing and providing the following items of work:

Listed in the Statement of Work, Attachment 1. See Table B-2 on page 3 for Contract Pricing and Contract Line Item (CLIN) structure.

B-2 Contract Pricing

(Table 1 -- CLIN Structure)

Line Item Number 1	Detainee Location Tracking System	Base Year (0001) 01/04/09-01/03/10	Option Year 1 (1001) 01/04/10-01/03/11	Option Year 2 (2001) 01/04/11-01/03/12	Option Year 3 (3001) 01/04/12-01/03/13
0001, 1001, 2001, 3001	Labor: Implementation, Configuration, Deployment, and Integration; Site Survey at 19 DRO-Dedicated Facilities, (Excluding cost of network infrastructure installation), Cost-Plus-Fixed-Fee (CPFF)				
0001A, 1001A, 2001A, 3001A	Hardware/Software, CPFF				
0001B, 1001B, 2001B, 3001B	Materials: Wireless Subscription Costs, Printing & Media Production, Incidentals (Excluding Cost of network infrastructure equipment), CPFF				
0001C, 1001C, 2001C, 3001C	Travel/ODCs, CPFF				
Optional CLIN*: 0001D, 1001D, 2001D, 3001D	Labor: Network Infrastructure Installation (SOW section 5.1.2), Firm-Fixed-Price				
Optional CLIN*: 0001E, 1001E, 2001E, 3001E	Equipment: Network Infrastructure Installation, CPFF	-	-	-	-

1. Annual Cost
2. Fixed Fee
3. Total Cost Plus Fixed Fee

*These tasks are optional, and will be exercised at the discretion of the Government.

Line Item Number 2	Central Reservation System	Base Year (0002) 01/04/09-01/03/10	Option Year 1 (1002) 01/04/10-01/03/11	Option Year 2 (2002) 01/04/11-01/03/12	Option Year 3 (3002) 01/04/12-01/03/13
0002, 1002, 2002, 3002	Labor: Implementation, Configuration, Deployment and Integration, CPFF				
0002A, 1002A, 2002A, 3002A	Hardware/Software, CPFF				
0002B, 1002B, 2002B, 3002B	Materials: Printing & Media Production, Incidentals, CPFF				

0002C, 1002C, 2002C, 3002C	Travel/ODCs, CPFF	1	b4
		2	
		3	

Line Item Number 3	Transportation Management System	Base Year (0003) 01/04/09-01/03/10	Option Year 1 (1003) 01/04/10-01/03/11	Option Year 2 (2003) 01/04/11-01/03/12	Option Year 3 (3003) 01/04/12-01/03/13
0003, 1003, 2003, 3003	Labor: Implementation, Configuration, Deployment, and Integration, Cost-Plus-Fixed-Fee	-	-	b4	
		-	-		
		-	-		
0003A, 1003A, 2003A, 3003A	Hardware/Software, Cost-Plus-Fixed-Fee	-	-	b4	
		-	-		
		-	-		
0003B, 1003B, 2003B, 3003B	Travel/ODCs, Cost-Plus-Fixed-Fee	-	-	b4	
		-	-		
		-	-		

Totals		Base Year 01/04/09-01/03/10	Option Year 1 01/04/10-01/03/11	Option Year 2 01/04/11-01/03/12	Option Year 3 01/04/12-01/03/13
		\$14,501,669		b4	

C. Description/Specifications

Please refer to the Statement of Work, Attachment 1

D. Packaging and Marking

Page Left Blank Intentionally

E. Inspection and Acceptance

FAR 52.246-5 E-1 Inspection of Services - Cost-Reimbursement. (APR 1984)

(a) *Definition.* Services, as used in this clause, includes services performed, workmanship, and material furnished or used in performing services.

(b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires.

(c) The Government has the right to inspect and test all services called for by the contract, to the extent practicable at all places and times during the term of the contract. The Government shall perform inspections and tests in a manner that will not unduly delay the work.

(d) If any of the services performed do not conform with contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, for no additional fee. When the defects in services cannot be corrected by reperformance, the Government may -

(1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and

(2) Reduce any fee payable under the contract to reflect the reduced value of the services performed.

(e) If the Contractor fails to promptly perform the services again or take the action necessary to ensure future performance in conformity with contract requirements, the Government may -

(1) By contract or otherwise, perform the services and reduce any fee payable by an amount that is equitable under the circumstances; or

(2) Terminate the contract for default.

(End of clause)

F. Deliveries or Performance

Please refer to the Statement of Work, Attachment 1 to the Task Order.

G. Contract Administration Data

G-1 TASK ORDER ADMINISTRATION

The following contact information is provided:

Task Order Contract Specialist (TO CS) (Post-Award/Administration)

Miranda Freethey, [REDACTED] b6 @dhs.gov

Task Order Contracting Officer (TO CO) (Post-Award/Administration)

Brooke Bernold, [REDACTED] b6 @dhs.gov

Program Manager (PM)

Denise Mackie-Smith, [REDACTED] b6 @dhs.gov

Task Order Contracting Officer Technical Representative (COTR)

Denise Mackie-Smith, [REDACTED] b6 @dhs.gov

Finance Office/Invoice Address

DHS ICE
Burlington Finance Center (BFC)
P.O. Box 1620
Williston, VT 05495-1620
Attn: ICE/OCIO/SDD invoice

Task Order Contracting Officer's Technical Representative

The Contracting Officer (CO) will appoint a Task Order Contracting Officer's Technical Representative (COTR) in writing for this task order in accordance with G.2.3 of the EAGLE contract. The COTR will receive, for the Government; all work called for by the task order and will represent the CO in the technical phases of the work. The COTR will provide no supervisory or instructional assistance to contractor personnel.

The COTR is not authorized to change any of the terms and conditions of the contract or the task order. Changes in the scope of work will be made only by the CO by properly executed modifications to the contract or the task order. Additional responsibilities of the COTR include:

Monitoring Performance

The COTR will ensure that the contractor complies with all of the requirements of the statement of work, specifications, or performance work statement, and when requested by the contractor, provide technical direction to the contractor's technical manager. This technical assistance must be within the scope of the contract (e.g., interpreting specifications, statement of work, performance work statement, etc.). When a difference of opinion between you and the contractor occurs, notify the Contracting Officer or the Contract Administrator/Specialist immediately for resolution.

Monitoring Costs

The COTR will review and evaluate the contractor's progress in relation to the expenditures. When the costs expended by the contractor are not commensurate with the contractor's progress, bring this to the attention of the Contracting Officer or contract administrator/specialist for immediate action.

The COTR will review the contractor's invoices/vouchers for reasonableness and applicability to the contract and

recommend to the Contracting Officer approval, conditional approval, or disapproval for payment.

Visits and Meetings With The Contractor

The COTR will make arrangements with the contractor for periodic visits to the contractor's facility to: (1) evaluate the contractor's performance; (2) evaluate changes in the technical performance affecting personnel, the schedule, deliverables, and price or costs; (3) inspect and monitor the use of Government property, if applicable; and (4) ensure that contractor employees being charged to the contract are actually performing the work under the contract. A trip report fully documenting all activities during the visit must be written and a copy provided to the Contracting Officer within three working days after the visit.

Inspection of Contract Items

When notified by the contractor or the Contracting Officer, the COTR will perform, in accordance with the terms of the contract, inspection, acceptance or rejection of the services or deliverables under the contract. Immediately notify the Contracting Officer of all rejections and the reason for the action. The COTR will review progress reports from the Contractor and advise the Contracting Officer of any contractor problems or action required to be taken by the Government.

G-2 Invoicing

(1) Contractors: Please use these procedures when you submit an invoice for all acquisitions from ICE/OAQ.

1. Invoices shall now be submitted via one of the following three methods:

a. By mail: DHS, ICE
Burlington Finance Center
P.O. Box 1620
Williston, VT 05495-1620
Attn: ICE OCIO-SDD invoice

b. By facsimile (fax) at: 802-288-7658 (include a cover sheet with point of contact & # of pages)

c. By e-mail at: Invoice.Consolidation@dhs.gov

Invoices submitted by other than these three methods will be returned. Contractor Taxpayer Identification Number (TIN) must be registered in the Central Contractor Registration (<http://www.ccr.gov>) prior to award and shall be notated on every invoice submitted to ICE/OAQ. The ICE program office identified in the delivery order/contract shall also be notated on every invoice. Please send an additional copy of the invoice to ICEOCIOITSRACQ@DHS.GOV.

2. In accordance with FAR 52.232-25 (a)(3), Prompt Payment, the information required with each invoice submission is as follows:

An invoice must include:

- (i) Name and address of the Contractor;
- (ii) Invoice date and number;
- (iii) Contract number, contract line item number and, if applicable, the order number;
- (iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
- (v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;

- (vi) Terms of any discount for prompt payment offered;
- (vii) Name and address of official to whom payment is to be sent;
- (viii) Name, title, and phone number of person to notify in event of defective invoice; and
- (ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract. (See paragraph 1 above.)
- (x) Electronic funds transfer (EFT) banking information.

(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer; Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer; Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

Invoices without the above information may be returned for resubmission.

Receiving Officer/COTR: Each Program Office is responsible for acceptance and receipt of goods and/or services. Upon receipt of goods/services, complete the applicable FFMS reports or DFC will not process the payment.

H. Special Contract Requirements

Security Requirements for Sensitive/Unclassified Contracts

GENERAL

The Department of Homeland Security (DHS) has determined that performance of the tasks as described in Task Order Number HSCETC-09-J-00002 requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

DHS shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the OPR-PSU. Contract employees assigned to the contract not needing access to sensitive DHS information or recurring access to DHS ' facilities will not be subject to security suitability screening.

BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Prospective Contractor employees with adequate security clearances issued by the Defense Industrial Security Clearance Office (DISCO) may not be required to submit complete security packages, as the clearance issued by DISCO may be accepted. Prospective Contractor employees without adequate security clearances issued by DISCO shall submit the following completed forms to the Personnel Security Unit through the COTR, no less than 5 days before the starting date of the contract or 5 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions" Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) **(2 copies)**
2. FD Form 258, "Fingerprint Card" **(2 copies)**
3. Foreign National Relatives or Associates Statement
4. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Optional Form 306 Declaration for Federal Employment (applies to contractors as well)

6. Authorization for Release of Medical Information

Required forms will be provided by DHS at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to, development of, or maintenance to any DHS IT system.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to Government facilities or information, the COTR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU may require reinvestigations when derogatory information is received and/or every 5 years.

DHS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COTR. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The OPR-PSU must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired DHS issued identification cards and building passes, or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COTR will return the identification cards and building passes to the responsible ID Unit.

EMPLOYMENT ELIGIBILITY

The Contractor must agree that each employee working on this contract will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or with this contract. The Contractor will ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this contract.

SECURITY MANAGEMENT

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The following computer security requirements apply to both Department of Homeland Security (DHS) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

INFORMATION TECHNOLOGY SECURITY CLEARANCE

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement*. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

All contractor employees using Department automated systems or processing Department sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

(End of Clause)

I. Contract Clauses

FAR 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 using the web site addresses listed below:

DIRECT LINK: <http://www.arnet.gov/far>
 <http://www.far.npr.gov>
 <http://www.deskbook.osd.mil>
 <http://www.dhs.gov/dhspublic>

In accordance with Federal Acquisition Regulation (FAR) 52.252-2 the following clauses are incorporated by reference:

52.203-6	Restrictions on Subcontractor Sales to the Government. (SEP 2006)
52.204-9	Personal Identity Verification of Contractor Personnel. (SEP 2007)
52.219-8	Utilization of Small Business Concerns. (MAY 2004)
52.219-9	Small Business Subcontracting Plan. (NOV 2007)
52.222-50	Combating Trafficking in Persons (AUG 2007)
52.225-13	Restrictions on Certain Foreign Purchases. (FEB 2006)
52.227-11	Patent Rights - Ownership by the Contractor (Dec 2007)
52.227-14	Rights in Data - General (DEC 2007)
52.233-4	Applicable Law for Breach of Contract Claim. (OCT 2004)
53.242-1	Notice of Intent to Disallow Costs
52.242-15	Stop-Work Order (AUG 1989)

The Contractor shall comply with the following Homeland Security Acquisition Regulation (HSAR) clauses incorporated by reference.

3052.215-70	Key Personnel or Facilities
3052.242-71	Dissemination of Contract Information
3052.242-72	Contracting Officer's Technical Representative

The following FAR clauses are hereby incorporated by attachment:

FAR 52.204-2 Security Requirements

This clause applies to the extent that this contract involves access to information classified information

The Contractor shall comply with—

(1) The Security Agreement (DD Form 441), including the *National Industrial Security Program Operating Manual* (DOD 5220.22-M); and

(2) Any revisions to that manual, notice of which has been furnished to the Contractor.

(b) If, subsequent to the date of this contract, the security classification or security requirements under this contract are changed by the Government and if the changes cause an increase or decrease in security costs or otherwise affect any other term or condition of this contract, the contract shall be subject to an equitable adjustment as if the changes were directed under the Changes clause of this contract.

(d) The Contractor agrees to insert terms that conform substantially to the language of this clause, including this paragraph (d) but excluding any reference to the Changes clause of this contract, in all subcontracts under this contract that involve access to classified information.

(End of Clause)

FAR 52.217-7 Option for Increased Quantity- Separately Priced Line Item (MAR 1989)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise the option by written notice to the Contractor within 60 calendar days before the contract expires. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

(End of Clause)

FAR 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 60 days before the task order expires.

(End of Clause)

FAR 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) thirty days before the task order expires; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the task order 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 four (4) years.

(End of Clause)

FAR 52.223-14 Toxic Chemical Release Reporting (AUG 2003)

(a) Unless otherwise exempt, the Contractor, as owner or operator of a facility used in the performance of this contract, shall file by July 1 for the prior calendar year an annual Toxic Chemical Release Inventory Form (Form R) as described in sections 313(a) and (g) of the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) (42 U.S.C. 11023(a) and (g)), and section 6607 of the Pollution Prevention Act of 1990 (PPA) (42 U.S.C. 13106). The Contractor shall file, for each facility subject to the Form R filing and reporting requirements, the annual Form R throughout the life of the contract.

(b) A Contractor-owned or -operated facility used in the performance of this contract is exempt from the requirement to file an annual Form R if—

(1) The facility does not manufacture, process, or otherwise use any toxic chemicals listed in 40 CFR 372.65;

(2) The facility does not have 10 or more full-time employees as specified in section 313(b)(1)(A) of EPCRA, 42 U.S.C. 11023(b)(1)(A);

(3) The facility does not meet the reporting thresholds of toxic chemicals established under section 313(f) of EPCRA, 42 U.S.C. 11023(f) (including the alternate thresholds at 40 CFR 372.27, provided an appropriate certification form has been filed with EPA);

(4) The facility does not fall within the following Standard Industrial Classification (SIC) codes or their corresponding North American Industry Classification System sectors:

(i) Major group code 10 (except 1011, 1081, and 1094.

(ii) Major group code 12 (except 1241).

(iii) Major group codes 20 through 39.

(iv) Industry code 4911, 4931, or 4939 (limited to facilities that combust coal and/or oil for the purpose of generating power for distribution in commerce).

(v) Industry code 4953 (limited to facilities regulated under the Resource Conservation and Recovery Act, Subtitle C (42 U.S.C. 6921, *et seq.*)), or 5169, or 5171, or 7389 (limited to facilities primarily engaged in solvent recovery services on a contract or fee basis); or

(5) The facility is not located in the United States or its outlying areas.

(c) If the Contractor has certified to an exemption in accordance with one or more of the criteria in paragraph (b) of this clause, and after award of the contract circumstances change so that any of its owned or operated facilities used in the performance of this contract is no longer exempt—

(1) The Contractor shall notify the Contracting Officer; and

(2) The Contractor, as owner or operator of a facility used in the performance of this contract that is no longer exempt, shall—

(i) Submit a Toxic Chemical Release Inventory Form (Form R) on or before July 1 for the prior calendar year during which the facility becomes eligible; and

(ii) Continue to file the annual Form R for the life of the contract for such facility.

(d) The Contracting Officer may terminate this contract or take other action as appropriate, if the Contractor fails to comply accurately and fully with the EPCRA and PPA toxic chemical release filing and reporting requirements.

(e) Except for acquisitions of commercial items as defined in FAR Part 2, the Contractor shall—

(1) For competitive subcontracts expected to exceed \$100,000 (including all options), include a solicitation provision substantially the same as the provision at FAR 52.223-13, Certification of Toxic Chemical Release Reporting; and

(2) Include in any resultant subcontract exceeding \$100,000 (including all options), the substance of this clause, except this paragraph (e).

(End of clause)

FAR 52.232-19 Availability of Funds for the Next Fiscal Year. (APR 1984)

Funds are not presently available for performance under this contract beyond 11/14/2009. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond 11/14/2009, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of Clause)

FAR 52.232-22 Limitation of Funds (APR 1984)

(a) The parties estimate that performance of this contract will not cost the Government more than

- (1) the estimated cost specified in the Schedule or,
- (2) if this is a cost-sharing contract, the Government's share of the estimated cost specified in the Schedule. The Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within the estimated cost, which, if this is a cost-sharing contract, includes both the Government's and the Contractor's share of the cost.

(b) The Schedule specifies the amount presently available for payment by the Government and allotted to this contract, the items covered, the Government's share of the cost if this is a cost-sharing contract, and the period of performance it is estimated the allotted amount will cover. The parties contemplate that the Government will allot additional funds incrementally to the contract up to the full estimated cost to the Government specified in the Schedule, exclusive of any fee. The Contractor agrees to perform, or have performed, work on the contract up to the point at which the total amount paid and payable by the Government under the contract approximates but does not exceed the total amount actually allotted by the Government to the contract.

(c) The Contractor shall notify the Contracting Officer in writing whenever it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of

- (1) the total amount so far allotted to the contract by the Government or,
- (2) if this is a cost-sharing contract, the amount then allotted to the contract by the Government plus the Contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the Schedule.

(d) Sixty days before the end of the period specified in the Schedule, the Contractor shall notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

(e) If, after notification, additional funds are not allotted by the end of the period specified in the Schedule or another agreed-upon date, upon the Contractor's written request the Contracting Officer will terminate this contract on that date in accordance with the provisions of the Termination clause of this contract. If the Contractor estimates that the funds available will allow it to continue to discharge its obligations beyond that date, it may specify a later date in its request, and the Contracting Officer may terminate this contract on that later date.

(f) Except as required by other provisions of this contract, specifically citing and stated to be an exception to this clause -

(1) The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount allotted by the Government to this contract; and

(2) The Contractor is not obligated to continue performance under this contract (including actions under the Termination clause of this contract) or otherwise incur costs in excess of --

(i) The amount then allotted to the contract by the Government or;

(ii) If this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, until the Contracting Officer notifies the Contractor in writing that the amount allotted by the Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to this contract.

(g) The estimated cost shall be increased to the extent that

(1) the amount allotted by the Government or,

(2) if this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, exceeds the estimated cost specified in the Schedule. If this is a cost-sharing contract, the increase shall be allocated in accordance with the formula specified in the Schedule.

(h) No notice, communication, or representation in any form other than that specified in subparagraph (f)(2) above, or from any person other than the Contracting Officer, shall affect the amount allotted by the Government to this contract. In the absence of the specified notice, the Government is not obligated to reimburse the Contractor for any costs in excess of the total amount allotted by the Government to this contract, whether incurred during the course of the contract or as a result of termination.

(i) When and to the extent that the amount allotted by the Government to the contract is increased, any costs the Contractor incurs before the increase that are in excess of --

(1) The amount previously allotted by the Government or;

(2) If this is a cost-sharing contract, the amount previously allotted by the Government to the contract plus the Contractor's corresponding share, shall be allowable to the same extent as if incurred afterward, unless the Contracting Officer issues a termination or other notice and directs that the increase is solely to cover termination or other specified expenses.

(j) Change orders shall not be considered an authorization to exceed the amount allotted by the Government specified in the Schedule, unless they contain a statement increasing the amount allotted.

(k) Nothing in this clause shall affect the right of the Government to terminate this contract. If this contract is terminated, the Government and the Contractor shall negotiate an equitable distribution of all property produced or purchased under the contract, based upon the share of costs incurred by each.

(l) If the Government does not allot sufficient funds to allow completion of the work, the Contractor is entitled to a percentage of the fee specified in the Schedule equaling the percentage of completion of the work contemplated by this contract.

(End of Clause)

FAR 52.233-3 Protest after Award, Alternate I (Jun 1985)

(a) Upon receipt of a notice of protest (as defined in FAR 33.101) or a determination that a protest is likely (see FAR 33.102(d)), the Contracting Officer may, by written order to the Contractor, direct the Contractor to stop performance of the work called for by this contract. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Upon receipt of the final decision in the protest, the Contracting Officer shall either --

(1) Cancel the stop-work order; or

(2) Terminate the work covered by the order as provided in the Termination clause of this contract.

(b) If a stop-work order issued under this clause is canceled either before or after a final decision in the protest, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule, the estimated cost, the fee, or a combination thereof, and in any other terms of the contract that may be affected, and the contract shall be modified, in writing, accordingly, if --

(1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and

(2) The Contractor asserts its right to an adjustment within 30 days after the end of the period of work stoppage; provided, that if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon a proposal at any time before final payment under this contract.

(c) If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

(d) If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

(e) The Government's rights to terminate this contract at any time are not affected by action taken under this clause.

(f) If, as the result of the Contractor's intentional or negligent misstatement, misrepresentation, or miscertification, a protest related to this contract is sustained, and the Government pays costs, as provided in FAR 33.102(b)(2) or 33.104(h)(1), the Government may require the Contractor to reimburse the Government the amount of such costs. In addition to any other remedy available, and pursuant to the requirements of Subpart 32.6, the Government may collect this debt by offsetting the amount against any payment due the Contractor under any contract between the Contractor and the Government.

(End of Clause)

The following HSAR clauses are hereby incorporated by attachment:

HSAR 3052.204-70 Security requirements for unclassified information technology resources. (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.204-71 Contractor employee access. Alternate I (JUN 2006)

(a) Sensitive Information, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information

Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, Policies and Procedures of Safeguarding and Control of SSI, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as For Official Use Only, which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated sensitive or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) Information Technology Resources include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the

COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U. S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this Individual as opposed to a U. S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

HSAR 3052.209-70 Prohibition on contracts with corporate expatriates. (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting 'more than 50 percent' for 'at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain Stock Disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(1) of Section 835 of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan Deemed In Certain Cases.* If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain Transfers Disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special Rule for Related Partnerships.* For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that (Check one):

It is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73;

It is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it has submitted a request for waiver pursuant to 3009.104-74, which has not been denied; or

It is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it plans to submit a request for waiver pursuant to 3009.104-74.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)

HSAR 3052.211-70 Index for specifications. (DEC 2003)

If an index or table of contents is furnished in connection with specifications, it is understood that such index or table of contents is for convenience only. Its accuracy and completeness is not guaranteed, and it is not to be considered as part of the specifications. In case of discrepancy between the index or table of contents and the specifications, the specifications shall govern.

(End of clause)

HSAR 3052.219-70 Small business subcontracting plan reporting. (JUN 2006)

(a) The Contractor shall enter the information for the Subcontracting Report for Individual Contracts (formally the Standard Form 294 (SF 294)) and the Summary Subcontract Report (formally the Standard Form 295 (SF-295)) into the Electronic Subcontracting Reporting System (eSRS) at <http://www.esrs.gov>.

(b) The Contractor shall include this clause in all subcontracts that include the clause at (FAR) 48 CFR 52.219-9.

(End of clause)

HSAR 3052.245-70 Government property reports. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.

(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700-5, Contractor Report of Government Property.

(End of clause)

J. List of Documents, Exhibits and Other Attachments

Attachment I— Statement of Work

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

**Statement of Work
U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



U.S. Immigration
and Customs
Enforcement

FINAL
Washington, DC

Procurement Sensitive. This document is confidential and intended solely for the use and information of the company to whom it is addressed.

CONTENTS

1.0	PROJECT TITLE.....	1
2.0	BACKGROUND	1
3.0	SCOPE OF WORK.....	2
4.0	APPLICABLE DOCUMENTS.....	2
5.0	TASKS	4
5.1	Develop Detainee Location Tracking System (DLT) (MANDATORY TASK).....	4
5.1.1	Site Survey.....	5
5.1.2	Install Hardware Infrastructure in “DRO-dedicated” Detention Facilities..	5
5.1.3	Internal Facility Location Tracking	7
5.1.4	Population Counts.....	8
5.1.5	Detainee Tracking Outside of “DRO-Dedicated” Detention Facilities	8
5.1.6	Detainee Identification and Tracking in Transportation Moves	8
5.1.7	Alerts and Retrieving Detainee Locations	9
5.1.8	Handheld Mobile Computing Devices.....	10
5.2	Develop a Central Reservation System (CRS) (MANDATORY TASK)	12
5.2.1	Detainee Discovery	12
5.2.2	Reservation Recommendation	12
5.2.3	Inventory Management	13
5.2.4	Reservation Details	13
5.2.5	Accounting.....	14
5.3	Develop a Transportation Management System (TMS) (OPTIONAL TASK).....	14
5.3.1	Local Transportation Planning.....	15
5.3.2	Transportation Asset Management	16
5.3.3	Information-based Execution.....	16
5.3.4	Strategic Planning	17
5.3.5	Performance Management	17
5.3.6	Resource Deployment.....	17
5.3.7	I-216 Manifest Standardization.....	18
5.4	Systems Integration (MANDATORY / OPTIONAL TASKS)	18
5.4.1	Data Groups	18
5.4.2	Integration with Internal Systems	19
5.4.3	Integration with External Systems	20
6.0	GENERAL REQUIREMENTS.....	23
6.1	Coordination with Contractor Program Support.....	23
6.2	Training.....	24
6.2.1	Training Material	24
6.2.2	Change Management	25
6.3	Solution Documentation	25
6.3.1	Requirements Documentation and Definition	25
6.3.2	System Lifecycle Management (SLM) Documentation	25
6.3.3	Certification and Accreditation Documentation	25

6.3.4	Interface Control Agreements.....	26
6.4	Data Requirements.....	26
6.4.1	NIEM Compliance and Definition.....	26
6.4.2	Integration with Enforcement Integrated Database (EID).....	26
6.5	Development Methodology.....	27
6.6	Reporting Requirements.....	27
6.6.1	Metrics Development.....	27
6.7	Key Performance Parameters.....	28
6.8	User Interface Requirements.....	29
6.9	COTS Requirements.....	29
6.10	Hardware Replacement.....	30
7.0	OPERATIONS AND MAINTENANCE.....	30
7.1	Solution Acceptance and Transition.....	30
7.2	Software Maintenance Support.....	31
7.3	Operational Support.....	31
7.4	Problem Analysis.....	32
7.4.1	Problem Trending Tracking.....	32
7.4.2	Performance Validation Support.....	32
7.4.3	COTS Integration Support.....	33
7.4.4	COTS Technical Refresh.....	33
7.4.5	COTS Installation Configuration.....	33
7.4.6	COTS Updates.....	33
7.4.7	Help Desk Requests.....	33
7.4.8	Configuration Management.....	34
8.0	DELIVERABLES.....	34
8.1	Task Project Plans and Schedules.....	34
8.1.1	Project Management Plan.....	35
8.1.2	Project Schedule.....	35
8.1.3	Risk Management Plan.....	35
8.1.4	Training Plan.....	35
8.1.5	Communication Plan.....	35
8.2	Progress Reports and Program Reviews.....	36
8.2.1	Progress Reports.....	36
8.2.2	Program Reviews.....	36
8.2.3	Weekly Status Report.....	36
8.2.4	Monthly Status Report.....	36
8.3	Presentations, Demonstrations, and Project Support Materials.....	36
8.4	Acceptance Criteria.....	37
8.5	Product Acceptance.....	38
8.6	Non-Disclosure Statements.....	38
9.0	GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION.....	39
10.0	PLACE OF PERFORMANCE.....	39
11.0	PERIOD OF PERFORMANCE.....	39
12.0	ACCESSIBILITY REQUIREMENTS.....	39

13.0	OTHER DIRECT COSTS (ODCS)	41
14.0	OVERTIME	41
14.0	KEY PERSONNEL	41
17.1	Project Manager	42
17.2	Functional Lead	43
17.3	Architecture/Technical Lead.....	43
16.0	TRANSITION	43
17.0	PERIODIC REVIEWS	44
APPENDIX A: LIST OF ACRONYMS		46
APPENDIX B: GLOSSARY		53

1.0 PROJECT TITLE

Bed Space, Transportation, and Detainee Location Tracking Automation (BST&T).

2.0 BACKGROUND

Detention and Removal Operations (DRO) is responsible for promoting public safety and national security by ensuring the safe and efficient departure from the United States of all removable aliens through the fair enforcement of the nation's immigration laws. As such, DRO's core mission is the identification, apprehension, detention, and removal of inadmissible and deportable aliens from the United States. The resources and expertise of DRO are utilized to identify and apprehend illegal aliens, fugitive aliens, and criminal aliens. DRO manages them while in custody as they progress through the immigration proceedings as well as enforce removal orders. DRO is committed to enforcing the nation's immigration laws in a fair, effective, and professional manner.

DRO's daily detention population consists of approximately 29,000 foreign nationals charged with violations of immigration law. In 2007, DRO removed over 276,000 people (including voluntary removals) from the United States. DRO is comprised of over 6,700 employees, including nearly 6,000 sworn law enforcement officers assigned to 24 field offices and manages an operating budget of nearly \$2 billion.

Foreign nationals detained under DRO supervision are located at a DRO-dedicated facility, or at a detention center that is not owned by the Government, but is chartered to support DRO. These facilities are considered "DRO-dedicated facilities" which include more than nineteen (19) facilities to date. Other detainees are housed in "non DRO-dedicated facilities" which are not owned by the Government and do not primarily serve DRO. Examples of these types of facilities include state prisons and county jails where DRO detainees make up a small proportion of the total facility population. There are more than 500 of these facilities leveraged across the continental U.S. (CONUS), and five (5) locations outside the continental U.S. (OCONUS), including Alaska, Hawaii, Guam, Puerto Rico, and the Virgin Islands.

DRO transports foreign nationals into custody, between detention facilities, to/from court and medical appointments, as well as removals to support repatriation. DRO performs approximately 1.3 million moves per year. There are over 3,000 ground vehicles and 6 airplanes (operating 6 flights daily) managed across the country. Commercial air is also used to transport aliens from one detention facility to another, connect to a DRO dedicated flight and/or to fulfill final removal orders back to their home country. DRO's centralized ticketing operation uses a system like SABRE to search for appropriate flights.

DRO is experiencing increases in apprehension rates and detention of illegal aliens. To support this, DRO is increasing detention capacity and improving transportation asset usage. To maximize operational efficiency and further the mission of DRO, a systems modernization effort has been undertaken to support bed space management, transportation management and detainee location tracking.

After a thorough analysis of the various industry solutions and technology, DRO has determined the need to add applications to their systems environment. Currently there is not a consistent nationwide supporting tool for supporting bed space management, transportation management or detainee location tracking.

The program is part of a multi-phase project, to be performed over four (4) years, which will replace or add new mission critical capabilities. Within this program, DRO and OCIO will evaluate and design a modern integrated systems solution that will interface with existing DRO legacy applications.

3.0 SCOPE OF WORK

Under the EAGLE Ordering Guide, this SOW falls under **Functional Category 4 – Software Development**.

This Statement of Work (SOW) document outlines the current high-level functional and technical requirements of Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE) Office, Detention and Removal Operations (DRO), and Office of the Chief Information Officer (OCIO) for the purchase, configuration, customization, installation, testing, training and support of software to address a centralized bed space reservation system, transportation management system and detainee location tracking system. These applications will serve Detention and Removal Operations (DRO) in several nation-wide locations.

The program is part of a multi-phase project, to be performed over four (4) years, which will add new mission critical DRO capabilities and integrate to existing DRO legacy systems. Within this program DRO and OCIO will evaluate and design a modern integrated systems solution that will interface with existing DRO legacy applications.

The objective of this project is to select and implement an integrated application environment encompassing several systems that will support the functionality, efficiency, and ease of use required by DRO. To enable these systemic improvements, DRO intends to implement the following:

- Detainee Location Tracking System (DLT) (MANDATORY TASK)
- Central Reservation System (CRS) (MANDATORY TASK)
- Transportation Management System (TMS) (OPTIONAL TASK)
- Systems Integration (MANDATORY / OPTIONAL TASKS)

4.0 APPLICABLE DOCUMENTS

For IT documentation and software products the following section applies.

The Contractor shall comply with all technology standards and architecture policies, processes, and procedures defined in ICE OCIO Architecture Division publications. These publications include, but are not limited to, the following:

- ICE System Lifecycle Management (SLM) Handbook
- ICE Enterprise Systems Assurance Plan
- ICE Architecture Test and Evaluation Plan
- ICE Web Standards and Guidelines
- ICE Technical Reference Model and Standards Profile

The Contractor shall not deviate from the Technology Standards without express approval granted by the Government via the formal Technology Change Process. If a deviation from the

Technology Standards is desired, the Government Project Manager (PM) must submit a formal request to the Architecture Division for adjudication. The Contractor shall not proceed with the deviation unless the Architecture Division approves the formal request and grants a waiver to deviate from the Technology Standards. If the Architecture Division approves the technology change request, the Contractor shall comply with all stipulations specified within the approval notification

The Contractor shall not deviate from the SLM Process (including any tailored SLM work pattern) without express approval granted by the Government via the formal Request for Deviation (RFD) Process. If a deviation from the SLM Process is desired, the PM must submit a formal RFD to the Architecture Division for adjudication. The Contractor shall not proceed with the deviation unless the Architecture Division approves the formal request and grants a waiver to deviate from the SLM Process. If the Architecture Division approves the RFD, the Contractor shall comply with all stipulations specified within the approval notification.

DHS Homeland Security Enterprise Architecture Compliance (HLS EA)

All solutions and services shall meet DHS Enterprise Architecture (EA) policies, standards, and procedures as it relates to this SOW and associated Task Orders (TO). Specifically, the contractor shall comply with the following HLS EA requirements:

All developed solutions and requirements shall be compliant with the HLS EA.

All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.

All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review and insertion into the DHS Data Reference Model.

5.0 TASKS

Specific user requirements can be referenced in ATTACHMENT B. The Contractor shall delivery the following functionality during the period of performance:

Contract Year	Milestones
BASE YEAR	DLT (pilot) <ul style="list-style-type: none"> • Deploy internal tracking system to four (4) facilities • Deploy mobile units to five (5) AORs CRS (pilot) <ul style="list-style-type: none"> • Requirements • Design & Development • Pilot at five (5) AORs (initial release)
OPTION YEAR 1	DLT (complete deployment) <ul style="list-style-type: none"> • All remaining AORs CRS (initial release) <ul style="list-style-type: none"> • Detainee Discovery • Inventory Management • Reservation Details • Accounting
OPTION YEAR 2	CRS (complete deployment) <ul style="list-style-type: none"> • Reservations Recommendation TMS (pilot) <ul style="list-style-type: none"> • Local Transportation Planning in all AORs • JPATS Integration
OPTION YEAR 3	Complete deployment of all remaining functionality

5.1 Develop Detainee Location Tracking System (DLT) (MANDATORY TASK)

The Contractor shall implement a Detainee Location Tracking (DLT) system for tracking the physical location of detainees as they pass through key checkpoints within and as they enter and exit facilities. Additionally, the tools utilized to collect location data shall:

- Verify the identity of detainees as they move from one facility or transportation node to another
- Perform daily headcounts of detainees within the facilities and reconcile detainee location to their assigned housing unit

Benefits of this system shall include increased visibility to detainee population data, assurance that the detainee is correctly identified (through their biometrics) prior to a transportation move,

development of tools that shall facilitate management to detention standards and more efficient and accurate logging of detainee locations.

The Contractor shall develop the system using custom developed software, Commercial Off-The-Shelf (COTS) products, or a combination of both.

There are four (4) major areas of functionality identified for this system:

1. **Detainee identification and tracking during transportation movements:** Verify a detainee's identification, and collect a detainee's location as they enter or exit detention centers and transportation nodes, such as commercial airports, and Ports of Entry (POE).
2. **Internal facility location tracking:** Track a detainee's location as they enter and exit at key areas within a subset of detention centers. Nineteen (19) large facilities are targeted for implementation.
3. **Population counts:** Identify the location of detainees within a detention center, and reconcile detainees to their assigned housing units.
4. **Reporting, alerts, and retrieving detainee locations:** Provide the capability to query and identify the checkpoints that a detainee or groups of detainees have passed through. Alert DRO staff of events based on detainee movement or location (variances in transportation manifests, holding cells at capacity, etc.). Deliver operational, management, and administrative reports based on detainees, facilities, and certain detention standards.

5.1.1 Site Surveys

The Contractor shall perform site surveys at nineteen (19) "DRO-Dedicated" facilities in order to assess the work to be performed in section 5.1.2.

5.1.2 Install Hardware Infrastructure in "DRO-dedicated" Detention Facilities (OPTIONAL)

The vendor shall be responsible for installing the physical infrastructure to support the DLT system at nineteen (19) "DRO-dedicated" detention centers. The scope shall include identification of all wired and wireless network components (cabling, switches, routers, etc.) and electrical infrastructure (additional outlets, circuits, etc.) required to support implementation. Network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

The infrastructure services shall include:

- Network design
- Cabling installation
- Equipment staging and installation
- Installation testing and commissioning services
- Coordination with local building maintenance organizations
- Obtaining building permits and complying with local ordinances
- Development of bill-of-materials

- Procurement of equipment

The Contractor shall coordinate with the internal OCIO IT infrastructure group and ICE facility IT contractors to define the division of responsibilities, including:

- Backup and recovery
- Equipment imaging and hosting
- Equipment standards
- Workstation and standard commodity procurement
- Installation and network provisioning

The Contractor shall be responsible for staging, configuration, deployment, and installation, as appropriate, of any mobile devices and associated accessories (e.g., charging/communication cradles) required to support the DLT system.

The Contractor shall install infrastructure at detention facilities that are Government owned Service Processing Centers (SPCs) and detention facilities that are owned by another entity, but are dedicated to housing DRO detainees. One implication of a “DRO-dedicated facility” is that DRO can install local infrastructure and systems to support DLT. The Contractor shall develop a solution that limits the amount of wide area traffic on the DHS OneNet wide area network, and is capable of operating locally in the event of a wide area network outage.

Service Processing Centers (SPCs) are Government owned facilities where suspected illegal aliens are brought to and a determination is made to detain the alien and to ultimately house the detainee. Detainees may spend less than 72 hours at a SPC, and often will not be housed overnight. Currently, there are nineteen (19) “DRO-dedicated” facilities¹ identified that house between 500-2300 detainees each (assume average of 1,000), and an anticipated twenty (20) Radio-Frequency Identification (RFID) transponder reading locations installed per facility. The Contractor shall install detainee location tracking infrastructure at the following facilities:

Facility Name	Location	Type
Krome North SPC	Miami, FL	Service Processing Center
Port Isabel SPC	Los Fresnos, TX	Service Processing Center
El Paso SPC	El Paso, TX	Service Processing Center
Florence SPC	Florence, AZ	Service Processing Center
El Centro SPC	El Centro, CA	Service Processing Center
Buffalo SPC	Batavia, NY	Service Processing Center
South Texas Detention Complex	Pearsall, TX	Contract Detention Facility
Correctional Corporation of America	San Diego, CA	Contract Detention Facility
Northwest Detention Center	Tacoma, WA	Contract Detention Facility
Houston Contract Detention Facility	Houston, TX	Contract Detention Facility

¹ Facility information correct as of March 28, 2008

Facility Name	Location	Type
Wackenhut Corrections Corp.	Pompano Beach, FL	Contract Detention Facility
Denver Contract Detention Facility	Aurora, CO	Contract Detention Facility
Elizabeth Contract Detention Facility	Elizabeth, NJ	Contract Detention Facility
Mira Loma Detention Center	Lancaster, CA	Contract Detention Facility
Willacy County Detention Center	Raymondville, TX	IGSA Facility
Eloy Federal Contract Facility	Eloy, AZ	IGSA Facility
Stewart Detention Center	Lumpkin, GA	IGSA Facility
York County Jail	York, PA	IGSA Facility
Laredo Contract Detention Facility	Laredo, TX	IGSA Facility

5.1.3 Internal Facility Location Tracking

The level of tracking shall be more inclusive at DRO-dedicated facilities. At “non DRO-dedicated” facilities, detainees shall be tracked the first time they enter and the last time they leave the facility. At DRO-dedicated facilities, detainees shall be automatically tracked when they enter and exit key areas (within 10 feet) of the facility including:

- Individual housing units and pods (2-10 per facility)
- Cafeterias
- Staging areas
- Law libraries
- Visitor areas
- Court rooms
- Segregated Housing Units (SHU)
- On-site medical clinics
- Recreation areas
- Unique, facility specific areas

Hardware components utilized for detainee tracking shall be tamper resistant, or at a minimum tamper "evident."

The functionality expected to be delivered shall include the ability to:

- Manage Wristband transponders, including assignment/reassignment
- Validate wristbands against detainee biometrics
- Link location data to detainee profile
- Track wristband replacements
- Track bad reads of encoded data on transmitters
- Track detainees at internal facility locations

5.1.4 Population Counts

The system shall support automatic headcounts at DRO-dedicated facilities. These headcounts shall be performed based on a comparison of the detainee's location data to their assigned pod or housing unit. Detainees may be in another area temporarily, for instance, at the law library or medical facility and their locations would be known through DLT and used to complete the reconciliation. Prior to implementation, this functionality shall require capturing detainee assignment to a pod or housing unit in a standardized automated system. Additionally, not all headcounts may be supported via the DLT since some facilities perform counts while detainees are sleeping.

The functionality expected to be delivered shall include the ability to:

- Perform real-time headcount reconciliations

5.1.5 Detainee Tracking Outside of "DRO-Dedicated" Detention Facilities

These facilities are not Government owned, but have a contract with DRO to house detainees on behalf of the Government. DRO detainees comprise only a portion of the inmate population, and DRO will not be installing local infrastructure or systems to support DLT at these facilities but will rely on handheld mobile computing devices to record initial drop-off and final pick-up of detainees. Examples of these facilities include state prisons and county jails. Some facilities have constraints regarding clothing, wristbands or other items that would identify detainees as being separate from the general population.

- **Transportation nodes:** Detainees are moved between facilities or removed to their country of nationality through various transportation nodes mobile tracking devices shall be used. These include:
 - **JPATS Hubs and terminals:** These are airport facilities administered by the Department of Justice U.S. Marshals Service to transport detainees.
 - **Commercial airports:** Detainees may be moved via commercial air transportation domestically or to their home country. Detainees may or may not be escorted on the flight by DRO officers, but DRO officers will transport the detainee to or from the commercial airport.
- **Border Ports of Entry:** These are official ports of entry along the ground borders with Mexico and Canada, administered by Customs and Border Protection, where mobile tracking devices shall be used to capture removal of deportable aliens.

5.1.6 Detainee Identification and Tracking in Transportation Moves

A detainee's entry and exit must be captured at all types of facilities and Ports of Entry. Specifically, this includes:

- The first time a detainee enters a detention center
- The last time a detainee leaves a detention center
- "Temp-outs" at DRO-dedicated facilities
- All entry and exit at other checkpoints

Handheld mobile computing devices shall be utilized to collect fingerprint scans and transmit detainee location data at these checkpoints. These devices must be able to display photographs and provide pen or key-based data entry. Detainee identification must be confirmed through biometrics in a timely manner (e.g., during vehicle loading and not impacting departure time).

Additionally, a “removal” checkpoint shall be captured. This removal checkpoint shall document:

- The date/time a detainee passes through a ground border POE
- The date/time a detainee is removed via an air transport segment (JPATS or commercial). Removal can be defined in two ways:
 - “Wheels up” of the plane when it leaves the final U.S. airport
 - Crossing the U.S./international border

It is expected that both “wheels up” and international air border crossings may be captured in a flight traffic mapping system, FlyteComm™, which is currently an in-house application used at DRO and transmitted to DLT by the TMS.

5.1.7 Alerts and Retrieving Detainee Locations

The system shall provide a user interface to allow DRO staff to track the current location of detainees and trace the movement of detainees through the DRO network.

The system shall also provide alerts to notify DRO staff of events that require their attention, for example, reaching maximum detainee capacity in a staging area.

The reporting functionality provided by the DLT solution shall improve the visibility of the detainee population for facilities, field offices and headquarters. The DLT system shall filter or aggregate raw location data into meaningful business transactions that can be utilized by other applications or reporting solutions.

Electronic records shall support more accurate and efficient retrieval of this information. The reporting shall enable DRO to:

- Access detainee length of detention at an Intergovernmental Service Agreement (IGSA) to confirm billing
- Identify how frequently certain areas of a facility are being used
- View other management, analysis and trending data

The Contractor shall develop the system to include the following functionality:

- Enroll detainees into tracking system
- Provide audit trails that document the passage of detainees through designated checkpoints
- Perform a match between the data encoded in the wristband with the detainee's biometric information
- Provide capability to locate a detainee
- Provide search functions by Alien number, Fingerprint Identification Number (FIN) and name

- Provide search capability by multiple detainees
- Display all checkpoints associated with a detainee
- Identify the transport vehicle a detainee is on
- Display all detainees located in a particular housing unit or pod
- Provide administrative reports to monitor system performance and operation
- Track all failed authentication attempts
- Filter and aggregate raw tracking data
- Generate alerts and notify staff of detainee movement and location
- Provide alerts when a detainee misses a scheduled departure or arrival
- Provide alert if a detainee transponder's signal is not received after a preconfigured amount of time
- Provide alert if detainee is missing from head count
- Provide the capability to create custom alerts

5.1.8 Handheld Mobile Computing Devices

The Contractor shall provide rugged mobile handheld Mobile Computing Devices (MCDs) to support data collection for the DLT system and perform basic data entry and enable searching and provide two (2) print tracking compatible with the US-VISIT Automated Biometric Identification System (IDENT) database. The Contractor shall coordinate the management and tracking of equipment assets with the ICE Sunflower System for inventory management.

5.1.8.1 Mobile Computing Device

The Contractor shall provide MCDs, estimated number shall be 500 (with an additional 10% spare pool for replacements), with the following characteristics:

- Handheld form factor
- Display color images, with a minimum of 65,000 colors and a minimum pixel screen resolution of 320 x 240
- Process on-line forms through either a web interface or lightweight Java application
- QWERTY keyboard
- Cellular data or wide area network connectivity (through existing ICE cellular network)
- Remote deactivation, in the event the device is either lost or stolen
- Docking for power recharge and data synchronization/upload
- Minimum IP54 environmental sealing
- Alert notification for persons of interest (via IAFIS)
- Provide alternate means of tracking if the system or network is unavailable
- Replaceable from supplier within 30 calendar days

5.1.8.2 Portable Biometric Accessory

The Contractor shall provide portable biometric devices, estimated number shall be 500 (with an additional 10% spare pool for replacements), with the following characteristics:

- Handheld form factor
- Attachable or built-in to MCD
- Fingerprint scanner provided as an accessory or peripheral (NIST compliant)
- Compatibility with US-VISIT/IDENT database
- Replaceable from supplier within 30 calendar days

5.1.8.3 RFID Wristband

The Contractor shall provide RFID wristband devices, estimated number shall be 20,000 (with an additional 10% spare pool for replacements), that shall interface with transponders located in detention facilities. The wristband shall have the following characteristics:

- Tamper resistant or evident
- No data retention of detainee biometric/biographical data
- Active mode, with alert when deactivated or tampered
- Include Hypo-allergenic materials
- Water resistant/waterproof
- Configurable transmission interval
- Alarm/notification when battery low
- Replaceable from supplier within 30 calendar days

5.1.8.4 Handheld Mobile Computing Device System Integration

The MCD shall be flexible to support the development of custom software for the purpose of integrating with ICE systems. The following capabilities shall be supported by processing in the field:

- Biometric verification of a subject on a subsequent encounter
- Issuance (for interfacing and capturing of key information for later case management processing) of charging documents and/or detainers
- Assignment of RFID wristband
- Real-time connectivity with Enforcement Integrated Database (EID)
- Data synchronization of subject information with EID/Enforcement Alien Removal Module (EARM)
- Photograph and biographical display of subject information EID/EARM
- Display case summary information, including alerts
- Integration of subject tracking verification with CRS and TMS

- Ability to close case on subsequent departure from final transportation node or border port of entry
- Alternate means of tracking, in the event biometrics cannot be used due to permanent disability and /or temporary injury

5.2 Develop a Central Reservation System (CRS) (MANDATORY TASK)

The CRS shall be custom developed software, Commercial Off- The-Shelf (COTS) products, or a combination of both. The CRS shall enable DRO to create, modify, assign, and manage bed space inventory. The applications shall also include automated tools driven by business processes to recommend bed space assignment options for a detainee based on biographical attributes and current DRO institutional knowledge.

DRO's functionality needs parallel the usage of COTS applications leveraged in the hospitality and prison management industry. Detainee profile data shall be leveraged for determining optimal bed space assignment for a detainee and for tracking the history of a detainee's stay. The ability to reserve a specific bed in advance of detainee arrival to a facility shall be necessary as occupancy is high in many facilities. Pre-assignment or fulfillment of bed space for a specific detainee is key functionality to ensure detainee locations can be tracked. Inventory management functionality shall provide a total picture of bed space status and availability as well as support group block inventory functionality. Operational reporting, specifically bed space usage and rate management are key metrics for DRO. DRO is not driven by profit maximization, but by reducing costs incurred in the assignment of detainees to the optimal bed space, supporting immigration proceedings and optimizing removals.

The CRS solution shall implement an integrated application environment encompassing several systems to support the functionality, efficiency and ease-of-use required by DRO. The technologies necessary to achieve these objectives shall include:

- Central Reservation System (CRS)
- Business Rules Management

5.2.1 Detainee Discovery

Detainee Discovery entails the collection of detainees' biographical attributes that drive bed type needs such as gender and criminal status. This functionality is expected to be provided via integration with existing DRO applications.

The functionality expected to be delivered shall include the ability to:

- Display detainee attributes (e.g., nationality, criminality, gender, medical status) when the record is retrieved
- Identify and alert user of potential duplicate profiles
- Maintain a history of updates to detainee profiles
- View detainee profile comments online

5.2.2 Reservation Recommendation

Reservation Recommendation is the administration, set-up and assignment of detention facilities and bed type priorities and rankings based upon detainee and facility attributes. This shall enable

the identification, scoring and prioritization of bed space recommendations. Bed space recommendations shall be validated against the detainee profile, business rules and bed space availability.

Reservation Recommendation automates the current local institutional knowledge and quickly and efficiently places detainees in facilities best equipped to process detainee removal. This ensures each facility can optimally play to comparative strengths by housing the detainees for which they are best suited.

The functionality expected to be delivered shall include:

- User definable rule and attribute weighting configuration and set up
- Recommendation request pre-processing
- Recommendation processing results display
- Group/special enforcement operation availability recommendations
- Sequencing reservation recommendations

5.2.3 Inventory Management

Inventory Management involves the administration, set-up, assignment and management of physical inventory (beds), available or occupied, within each region/Area of Responsibility (AOR). This shall include the inventory for several types of facilities including: SPCs, Contract Detention Facilities (CDFs), and IGSA facilities.

The functionality expected to be delivered shall include:

- Configuration and set-up of bed inventory
- Views of available and occupied inventory
- Availability request processing
- Booking of beds (changing status from available to occupied)
- Group/special enforcement operation inventory
- Out-of-order/Off-the-market
- Waitlist to support fulfilling inventory as it comes available
- Inventory Search Criteria

5.2.4 Reservation Details

Reservation Details allows creation, modification, cancellation and reinstatement of reservations for beds in facilities across the nation. This includes, but is not limited to, queries, wait-listing and inventory blocks for special enforcement operations. This shall also include the initiation and completion of fulfilling a reservation for one (1) or more beds (book-in/book-out).

The functionality expected to be delivered shall include:

- Alerts
- Reservation Detail

- Reservation Header
- Book Reservations
- Modify Reservation
- Cancel Reservation
- Waitlist Reservation
- Reservation Search Criteria

5.2.5 Accounting

Accounting is the administration, set-up and management of costs and utilization tracking of beds by facility. Limited general ledger and job costing functionality shall be required; however the emphasis shall be on utilization and tracking of cost rather than profit and loss.

The functionality expected to be delivered shall include:

- Folio Management
- Supplier Information
- Utilization and tracking of cost
- General ledger
- Job costing functionality

5.3 Develop a Transportation Management System (TMS) (OPTIONAL TASK)

The TMS shall be custom developed software, Commercial Off- The-Shelf (COTS) products, or a combination of both. The TMS shall support planning for detainees transported by multiple modes and, in some cases, shall adhere to pre-determined schedules. The solution shall include recent enhancements in COTS solutions enabling serialization of individuals (commercially as ‘packages’) as a part of a trip plan and tracing by individual. The solution shall create trips via multiple legs and modes using both DRO and contract transportation providers. The solution shall enable various facility types which represent pickup locations, consolidation points, hubs and staging areas. These shall all be distinguished with global and regional characteristics including, but not limited to hours of service, and length of stay duration categories.

The solution shall be effective in direct planning and execution of DRO assets as well as communication to and collection of information from 3rd party Contractors providing similar services.

- **Air transportation:** DRO uses commercial flights, charter flights, and U.S. Marshals Justice Prisoner and Alien Transport flights for movement of aliens. U.S. Marshals Justice Prisoner and Alien Transport flights are coordinated for DRO by the Flight Operations Unit (FOU). FOU and Central Ticketing (CENTIX) provide shared services to DRO for air transportation. JPATS airplanes are leased from the Department of Justice (DOJ) and CENTIX provides commercial air ticketing support. Most repatriation trips require escorts from U.S. Marshals and/or Immigration Enforcement Agents. DRO field locations request transport support independently from FOU and CENTIX. Visibility to all requests shall highlight consolidation opportunities from a geographic

and time perspective. This shall allow DRO to combine trips reducing the number of escorts required for international and/or cross-country air travel. The high-level functional requirements of the system shall include:

- Internal transfers: the movement of aliens from one detention facility to another in order to segment detainee populations for faster processing, or to free-up bed space in heavily constrained locations
- Final removal: the repatriation of aliens to their country of origin which generally requires air travel with the exception of ground removals to contingent borders
- **Ground transportation:** The solution shall support the DRO-operated fleet of approximately 3,000 ground vehicles including buses, vans and cars. In addition, the solution shall support third party Contractors operating similar equipment for DRO. Functionality shall include typical ground transport moves including:
 - Intake: Pickups from various locations and apprehending agencies from an arrest site (point of apprehension) to the processing facility. Intake may include the execution of an ICE detainer from other Federal, State, Local prisons/jails.
 - Book-In: Transport to the detention facility from the processing center. Coordination is handled by DRO even if the detainee is then picked up by other sources, such as the IGSA where the detainee will be housed.
 - Temp-outs: Trips for medical, court or consulate visits
 - Transfers: Movement from one detention facility to another may occur by ground.
 - Removals: Ground transportation is likely employed for repatriation when the detainee's home country is Mexico or Canada and he/she is located within driving distance to the border. Otherwise, air transportation is employed.

5.3.1 Local Transportation Planning

Based on known and estimated demand, the solution shall enable detainee transportation pre-planning, including the mode selection, assignment of vehicles, drivers and escorts and the logical consolidation of trips. Advance planning shall enable workload balancing and reduce the ad hoc environment of daily transportation management.

The solution shall enable the automation of the many rules governing the assignment of escorts above and beyond compatibility. Escorts are assigned based on compatibility, including gender, language skills, and other factors.

The functionality expected to be delivered shall include:

- Refine master routes, equipment types and restrictions
- Schedule movements using various transportation modes
- Reservations (tendering)
- Enable national oversight of schedules, routes, assets, and passenger manifests
- Enable regional and local scheduling of transportation moves
- Assign transportation mode to routes

- Assign transportation assets and drivers
- Track passenger characteristics
- Segment passenger assignment for transportation
- Restrict assignment of passengers to transportation
- Schedule passengers on non-DRO owned assets
- Assign escorts for commercial flights
- Account for traffic and congestion delays
- Create manifests
- Identify availability of alternative routes
- Notify receiving facility of inbound vehicles
- Enable receiving facility to review manifests in advance

5.3.2 Transportation Asset Management

The goal of transportation asset management is to efficiently allocate transportation resources to pre-defined work, prescribed courses of action and provide a buffer to accommodate expected levels of ad-hoc work. Transportation assets shall commonly share the definition of a “container” that can be applied to either ground or flight transportation.

The functionality expected to be delivered shall include the ability to:

- Maintain historical data on transportation resource information, both owned and contracted
- Track the availability of transportation resources for local, regional, and national allocation
- Manage capability characteristics of transportation resources (e.g., number of seats, segregated compartments, integrated processing, etc.)
- Maintain cost information for tracking bus and aircraft leases

5.3.3 Information-based Execution

Continuous asset visibility, real-time communication between all entities involved in a detainee move and the ability to distinguish out-of-the-ordinary events (event management) all provide current data that allows the transportation coordinator to identify a problem before it happens. The goal of information-based execution is proactive management to mitigate disruptions to transportation plans.

The functionality expected to be delivered shall include the ability to:

- Modify and update manifests
- Track and manage schedule or route changes
- Track unexpected pick-ups and drop-offs
- Communicate unexpected pick-ups and drop-offs

- Supply emergency provider information
- Generate alerts in the event a vehicle is overdue
- Generate alerts in the event a vehicle is early/other
- Modify routes in real-time
- Display a master list of all moves
- Display historic detainee trip information
- Create proof of delivery record
- Identify detainee status within the transportation network
- Coordinate transportation operations performed by third parties
- Capture ground and flight transportation costs
- Apply transportation costs to various assets
- Calculate transportation costs
- Capture vehicle utilization
- Capture load factors
- Support ad hoc dispatch capability

5.3.4 Strategic Planning

The solution shall enable the development of plans to accommodate transportation requirements over multiple regions. These activities may be in response to hypothetical questions associated with proposed detention policy, expected changes in detainee volume, defining transportation for major operations, and understanding how best to use national transportation infrastructure and resources. This type of analysis serves as a platform to develop and test transportation policies that align transportation goals with organizational goals.

The functionality expected to be delivered shall include the ability to:

- Enable optimization of transportation network
- Establish routine master transportation routes
- Enable major incident coordination (e.g. hurricane)

5.3.5 Performance Management

Productivity is a key driver for DRO. Transportation information captured in the TMS shall be used to track productivity and identify trends, including asset utilization by region, in order to better understand how specific resources are used regionally and nationally. The reporting solution shall include the measurement of cost per passenger per mile through the full lifecycle cost of bed space/volume movements.

5.3.6 Resource Deployment

Performance management is the precursor to resource deployment. With a toolset and process in place to track key performance indicators, DRO will be positioned to take advantage of

optimization and decision support functionality to, first, identify regional resource needs, and then, determine how to fulfill those needs proactively. This may include re-positioning equipment or escorts, acquiring new equipment or hiring new escorts, or initiating 3rd party contracts.

This functionality shall determine the capacity requirements, given the strategic plan and forecasted or historic demand.

The functionality expected to be delivered shall include the ability to:

- Display characteristics of driver/escort
- Identify regional resource needs
- Determine how to fulfill those needs proactively

Application access shall include local and remote management and third party informational access with varying permission (Third Party Providers, Contractor facilities, etc.)

5.3.7 I-216 Manifest Standardization

DRO uses a standard form to describe and communicate moves throughout the organization. The I-216 manifest is the document of record for movement for law enforcement agencies to coordinate the movement of subjects between organizations. The Contractor shall coordinate the data standards that need to be defined to support the nation-wide adoption of a manifest as regards to transportation. The following activities shall be required:

- Facilitation of data standards for the definition subject manifest information between Contractors, IGSA, and other law enforcement agencies including the Office of the Border Patrol, the Office of Field Operations, the Office of Investigations, and the U.S. Marshals Service JPATS
- Publication of manifest definition with the National Information Exchange Model (NIEM) data model

5.4 Systems Integration (MANDATORY / OPTIONAL TASKS)

In order to eliminate duplicate data entry and provide consolidated views of information for DRO to make the most informed operational decisions, the Contractor shall have a disciplined methodology for systems integration for the BST&T solution. The following systems

5.4.1 Data Groups

The data groups are an abstract conceptual representation of the major business data elements that have been identified for the BST&T solution. The Contractor shall take into consideration the data groupings that are specified in the following table:

Data Group	DLT (M)	CRS (M)	TMS (O)
Detainee Tracking (e.g., Unique ID, Time Stamp / Location)	✓	✓	✓

Data Group	DLT (M)	CRS (M)	TMS (O)
Detainee Characteristics (e.g., Criminal, Juvenile, Special Needs, Medical)		✓	✓
Detainee Biographic / Biometric information (e.g., Person Record)	✓	✓	✓
Reservation Detail (e.g., Reservation number, Detainee name, Arrival date, Departure date, Facility)		✓	
Transportation Asset Characteristics (e.g., Number of Seats, Bus / Plane, Special Ventilation System)			✓
Transportation Manifest (e.g., Person Record, Transfer To / From Location, Custody Agency)			✓
Transportation Logistics (e.g., Routes, Schedules, Escorts)			✓
Transportation Contract Information (e.g., ICE / Contractor / IGSA Owned, Rates, Mileage, Maintenance, Period of Performance)			✓
Facility Contract Information (e.g., ICE / Contractor / IGSA Owned, Rates, Service Offerings, Period of Performance)		✓	
Facility Characteristics (e.g., Number of Beds, Detainee Characteristics Supported)		✓	✓
Facility Allocation (e.g., Bed Space Availability)		✓	

Figure 1 - (M) = Mandatory Integration, (O) = Optional Integration

5.4.2 Integration with Internal Systems

The Contractor shall adapt the BST&T solution to DRO’s requirements by encapsulating functionality in mediator applications which are assumed to be largely made up of custom developed code. The mediator applications shall decouple the CRS, TMS, and DLT systems from the legacy systems to provide insulation for the enterprise architecture. The mediator applications shall also provide the ability to abstract the message structure to both facilitate message transformation and routing as well as facilitate mapping a COTS-specific message to a NIEM-specific message. This architectural pattern mitigates any need to modify the COTS application code.

To preserve the integrity of the COTS solution for maintenance and upgrade purposes the Contractor shall:

- Not modify COTS data structures or source code
- Build messaging services that are supported by NIEM standards
- Leverage existing SOA infrastructure
- Use a business rules management COTS solution for cataloging and managing the system logic

5.4.3 Integration with External Systems

The following table provides an inventory of legacy systems with which CRS, TMS, and DLT shall be required to integrate. It is expected that the Contractor shall validate this list of applications post-award and develop integration with the appropriate applications. The Contractor shall develop interfaces using the NIEM standard, and is expected to create and publish new standards to the governance body for widespread adoption by external agencies.

The following table represents the current systems that shall require integration with the BST&T solution:

External System	Description	COTS Solution		
		DLT (M)	CRS (M)	TMS (O)
Automated Biometric Identification System (IDENT)	<ul style="list-style-type: none"> IDENT is a two-fingerprint identification system to allow ICE offices to identify criminal aliens and repeat offenders of U.S. Immigration law. IDENT captures biometric, photographic, and biographical data. IDENT's basic function is to accept a pair of fingerprints, extract information from the prints, search the system's databases for prior encounters, create a new record when there is no prior encounter, and identify the current immigration status of those people already in the database or report that a new record is being created. IDENT shall integrate with DLT to provide unique detainee verification at select checkpoints. This integration point works in tandem with IAFIS (see IAFIS below). 	✓		
Detainee Location Tracking (DLT)	<ul style="list-style-type: none"> DLT is the new detainee tracking solution as proposed in this document. DLT shall integrate with CRS and TMS to exchange information which will trigger automatic processing under select scenarios (e.g., auto-book out, auto-book in, detainee status updates) 		✓	✓
Central Reservation System (CRS)	<ul style="list-style-type: none"> CRS is the new bed space management solution as proposed in this document. CRS shall be the system of record for bed space inventory. CRS shall integrate with DLT and TMS to exchange information which will trigger automatic processing under select scenarios (e.g., auto-book out, auto-book in, detainee status updates) 	✓		✓

External System	Description	COTS Solution		
		DLT (M)	CRS (M)	TMS (O)
Transportation Management System (TMS)	<ul style="list-style-type: none"> TMS is the new transportation management solution as proposed in this document. TMS shall integrate with DLT and CRS to exchange information which will trigger automatic processing under select scenarios (e.g., auto-book out, auto-book in, detainee status updates) 	✓	✓	
Enforcement Integrated Database (EID)	<ul style="list-style-type: none"> EID is the central database repository for case management concerning detainee in custody supporting book-in through removals. It is the system of record for detainee case management and maintains the person record. EID shall provide detainee profile information (e.g., name, sex, nationality) to CRS, TMS, and DLT. 	✓	✓	✓
ENFORCE/E3	<ul style="list-style-type: none"> ENFORCE/E3² is the primary system used by arresting authorities for booking aliens that are Present Without Authorization (PWA). ENFORCE/E3 shall provide initial intake information to CRS for reservation recommendation and bed space allocation. 		✓	
ICE Integrated Decision Support (IIDS)	<ul style="list-style-type: none"> IIDS is the ICE data warehouse for operational business intelligence reporting. The IIDS system provides operational dashboards, standard reports, and ad-hoc reporting capabilities using a web browser interface and uses the Hyperion BI solution. IIDS shall integrate with CRS, TMS, and DLT to provide operational business intelligence. 	✓	✓	✓
E-Government Internet Portal (eGov)	<ul style="list-style-type: none"> eGov is an internet portal environment which provides controlled access to information over the internet usually to non-US Government organizations (e.g., foreign consulates) in order to conduct transactions with the U.S. Federal Government. eGov shall host TMS and CRS portal solutions to allow select facilities not on the ICE intranet to have access to provide and receive information concerning bed space and transportation management. 		✓	✓

² As of March 28, 2008, E3 is a planned web-based system being developed by U.S. Customs and Border Protection, and is intended to replace the functionality contained within ENFORCE.

External System	Description	COTS Solution		
		DLT (M)	CRS (M)	TMS (O)
Automated Prisoner Scheduling System (APSS)	<ul style="list-style-type: none"> APSS is an application and is used by the United States Marshal Service (USMS) to schedule and manage Justice Prisoner & Alien Transportation System (JPATS) flights to transport detainees between facilities in the U.S. or to remove (i.e., deport) from the country. APSS shall integrate with TMS to give visibility to the JPATS flight features and functions. 			✓
CENTIX/Omega™	<ul style="list-style-type: none"> CENTIX is DRO's central ticketing group for booking detainees on commercial flights. CENTIX uses the commercial Omega system in order to make the reservations on commercial carriers. CENTIX/Omega shall integrate with TMS to give visibility to the commercial air flight features and functions. 			✓
FlyteComm™	<ul style="list-style-type: none"> FlyteComm™ is a commercial service used by DRO which provides aircraft and related air travel information. FlyteComm™ shall provide aircraft location information to TMS. 			✓
Large IGSA and CDF Facilities	<ul style="list-style-type: none"> For those large dedicated Intergovernmental Service Agreement (IGSA) Facilities and Contract Detention Facilities (CDF) which may have their own CRS or TMS system. TMS and CRS shall integrate with these legacy systems to provide coordinated sharing of information. 		✓	✓

External System	Description	COTS Solution		
		DLT (M)	CRS (M)	TMS (O)
Federal, State, and Local Jails/Prisons	<ul style="list-style-type: none"> Jails and prisons that are currently housing illegal aliens shall have release dates coordinated with completed travel documents to avoid costs associated with case processing in a DRO facility. TMS shall integrate using a NIEM compliant communication protocol and a global justice information broker 		✓	✓
Qualcomm (QTRACS, GPS Vehicle Tracking)	<ul style="list-style-type: none"> Qualcomm³ is a commercial service used by DRO which provides ground vehicle location and tracking information. Qualcomm shall provide ground location information to TMS. 			✓
Vehicle Management Information System (VMIS)	<ul style="list-style-type: none"> VMIS is a commercial service of Federal Prison Industry used by DRO which provides management of ground transportation vehicles. VMIS shall integrate with TMS to provide status updates of ground vehicles (e.g., in service, not in service) and is the system of record for vehicles and domicile locations 			✓

Figure 2 - (M) = Mandatory Integration, (O) = Optional Integration

6.0 GENERAL REQUIREMENTS

This section describes the type of tasks that are representative of the work to be completed by the Contractor.

6.1 Coordination with Contractor Program Support

The Contractor shall coordinate with multiple OCIO and DRO program support contractors. Relevant functional documentation and material shall be provided if requested without the explicit consent of the Government. The Contractor shall expect to interact with the following program support contractors:

- Architecture (includes Independent Testing)
- System Engineering
- Network Engineering
- Help Desk Operations
- IT Field Operations

³ DRO anticipates replacing the Qualcomm service with Fleet Management Solutions (FMS). Integration requirements will be similar.

- Program Management Office
- Requirements Analysts
- Security

6.2 Training

The Contractor shall provide training for approximately 1,000 DRO personnel and contractors (including technical staff, DRO trainers, detention contractors, contractor bus drivers, and charter flight crew). Training is subject to an approved training plan and shall include the following representative tasks:

- Training for up to fifteen (15) participants per class at the 24 DRO AORs, ICE Headquarters, and FLETC
- ICE Virtual University course development
- Training material development
- Train-the-Trainer (for DRO personnel)
- Training application environment (requiring daily refresh, if needed)
- Sufficient equipment for on-going training at the 24 AORs, ICE Headquarters, and FLETC
- Coordination of training participants

6.2.1 Training Material

The Contractor shall develop the BST&T solution training material. The Contractor shall support the distribution of material in a production environment, in coordination with the Government Printing Office (as needed), to include printing, packaging, shipping, and media. The following artifacts are representative of the type of material the Contractor shall develop:

- Help Desk Scripts: provides step-by-step troubleshooting of solution for TIER 1 and TIER 2 support staff
- Quick Reference Guides: provides visual guides for step-by-step overview of the most common tasks in a condensed format
- Train-the-Trainer: development of curriculum material
- Training Videos: informs end-users of new capabilities
- Briefings: supports training curriculum and management training reports
- User Manuals: detailed end-user documentation of system functionality
- Marketing Collateral: provides awareness of solution through branding on posters, pens, coffee mugs, mouse pads, etc.
- Surveys: soliciting feedback from training sessions to measure success of the content and delivery

6.2.2 Change Management

The Contractor shall take into consideration the efforts necessary to adopt a major operational change, and the various internal and external stakeholders that have a vested interest in the implementation of the solution. The Contractor shall recommend an approach to accomplish a smooth transition to the new solution.

6.3 Solution Documentation

The Contract shall develop project documentation in support of the BST&T solution which shall include the following artifacts:

6.3.1 Requirements Documentation and Definition

The Contractor shall develop detailed system requirements using a combination of narrative, wire-frames, user-interface mock-ups, feature/function lists, data dictionary, system process flows, user cases, network/system diagrams, architecture diagrams, and entity relationship diagrams. The Contractor shall assimilate, compile, and validate documentation artifacts from existing sources, including those in SOW ATTACHMENT B, ATTACHMENT C, ATTACHMENT E, and ATTACHMENT F. The documentation shall be developed in a way to accommodate an Agile development methodology.

Following an analysis of the existing documentation, the Contractor shall validate the requirements and facilitate a series of Joint Application Development (JAD) workshops with participation from stakeholders including OCIO Project Managers, DRO Program Analysts, DRO Subject Matter Experts (SMEs), and additional third party contractor staff to include requirements analysts and program management staff.

6.3.2 System Lifecycle Management (SLM) Documentation

The Contractor shall deliver copies of specific SLM documentation to the Electronic Library Management System (ELMS) in accordance with established manual guidelines. The Contractor shall deliver draft versions, revised versions, and final versions of required system documents.

Deliverables shall be deemed acceptable if the document adequately covers all required topics, is professionally prepared in terms of format, clarity and readability, and is delivered in hard and electronic copy on time to the designated delivery location.

6.3.3 Certification and Accreditation Documentation

The Contractor shall develop the Certification and Accreditation (C&A) documentation as required by DHS Sensitive Systems Policy Directive 4300A and DHS National Systems Policy Directive 4300B.

The Contractor shall meet the DHS Trusted Agent Federal Information Security Management Act (FISMA) standards for security documentation. These artifacts include a System Security Plan and a Privacy Impact Assessment, and other supporting documentation to support Certification and Accreditation and Privacy compliance with DHS.

6.3.4 Interface Control Agreements

The Contractor shall develop Interface Control Agreements (ICAs) that will specify the technical specifications for integrating between the BST&T solution and external systems. The activities associated with this task shall include:

- Coordinating and facilitating meetings with external agencies
- Developing definition of technical specifications for field attributes with external agencies
- Developing agreement of communication protocols with external agencies
- Complying with DHS/ICE security requirements
- Documenting Standard Operating Procedures (SOPs), Service Level Agreements (SLAs), installation/connection guides, and supporting detailed design documents

6.4 Data Requirements

The system shall use a Service Oriented Architecture (SOA) for data exchanges with external agency systems using ICE internal IBM® WebSphere-based J2EE Dynamic Web Application Runtime Pattern. The services shall be compatible with the DHS Enterprise Server Bus and use the NIEM standard for data definition. The solution shall take into consideration disparate networks and data centers from the DHS and DOJ.

6.4.1 NIEM Compliance and Definition

The Contractor shall use the NIEM data model for integration with internal and external systems. If the NIEM data model does not support the BST&T requirements, the Contractor shall support ICE by making the appropriate petitions to the governance body for inclusion of the proposed data definition for future releases of the data model. The Contractor shall support the following activities:

- Analysis of the NIEM data model for support of BST&T requirements
- Providing ICE representation at NIEM governance working groups and meetings
- Supporting NIEM documentation and definition of new requirements
- Training, coordination, and awareness of BST&T NIEM standards to external agencies, including other Federal, State, and Local organizations and Contract Detention facilities

6.4.2 Integration with Enforcement Integrated Database (EID)

The Contractor shall interface data connection points with law enforcement Information Exchange brokers (e.g., NLETS) for integrated information with other Federal, State, and Local law enforcement entities. The Contractor shall use the NIEM as the standard definition for exchanging data.

The Enforcement Integrated Database (EID) is shared by federal law enforcement agencies and is governed by a formal Change Control Board (CCB). The Contractor shall coordinate the addition and modification of database tables, fields, source code data, and connections with Information Exchange brokers with the governance body and support contractors.

6.5 Development Methodology

The Contractor shall develop the BST&T automation system using the Agile development methodology in a manner that is compliant with the ICE SLM. Releases shall be presented to key stakeholders throughout the development process and feedback shall be incorporated in subsequent releases. The Contractor shall prototype/pilot the solution prior to a production release, where the success of the solution shall be measured by an acceptable criterion that is subsequently approved by the OCIO Project Manager. In order to minimize impact to operations, a pilot/prototype release shall be limited to 10% participation of the end-user community and infrastructure, including officers, facilities, transportation. The Contractor shall leverage COTS products wherever deemed appropriate, the use of which requires prior approval by the ICE OCIO Technical Architecture Branch. The Government reserves the right to conduct code reviews at routine checkpoints by an independent party. The Contractor shall review and validate the deployment approach described in ATTACHMENT E.

6.6 Reporting Requirements

Reporting permits the creation and administration of reports including, but not limited to, ad hoc, operational, productivity and reservation history. Operational data provided to the DRO data warehouse shall also enable historical analysis, metric and trend reporting.

To maximize the effectiveness of the COTS applications a series of reports shall be developed. It is expected that the proposed COTS applications and the ICE Integrated Decision Support (IIDS) shall provide the data for the operational and management reports. The Contractor shall identify with DRO, local and national resources, as well as OCIO an inventory of required reports. The Contractor shall also prioritize and develop these operational and historical reports with DRO. The Contractor shall develop the following types of reports, according to ICE standards:

- **Operational reports:** Are available real-time and assist DRO in making informed decisions with tactical data. These are accessible through the BST&T solution via the ICE Data Mart (minimum 20 minute data refresh). Response times shall be consistent with web applications and not exceed five (5) seconds in length.
- **Management reports:** Are available with delayed data, from either the ICE data warehouse (minimum 24 hour data refresh). The management reports are designed to provide analytical functions to ICE management for improving the efficiency of the operation. They are currently a function of the ICE IIDS Hyperion system, which can support large aggregate reports with complex data relationships. Response times shall be consistent with the Hyperion technical specifications.

6.6.1 Metrics Development

The Contractor shall develop performance and costing metrics for measuring the key activities associated with BST&T. The metrics shall be validated with the operation and updated as solution components are released in prototype/pilot and production. The Contractor shall aggregate the metrics to provide clear and concise management reports focused on process improvements and cost avoidance.

6.7 Key Performance Parameters

The following table describes the Key Performance Parameters (KPPs) that each solution shall be required to meet. The Contractor shall take into consideration the KPPs prior to the solution design and development.

Metric	Unit of Measure	Threshold
Overall System Availability	% up-time	>99.97
	Schedule	24/7/365
	Scheduled downtime	<= 2 hours per month
Overall System Capacity	# of concurrent users supported	1,000
	# of total users supported	3,000
	# of aliens in custody supported	40,000
Overall Systems Support	Support availability	24/7/365
	Emergency/Critical issue support	24/7/365 with 1 hour response time
Overall System Performance Specs	User action response time	<= 5 seconds
	Alert delivery time	< 3 minutes from event occurrence
	False Alert rate	< 1%
DLT	RFID Response time	< 200ms (w/in 10ft)
	RFID: Detainee Identification Accuracy	>= 99.97% on read of detainee per key area
	Mobile Device biometric subject verification time	< 5 seconds ⁴
	Mobile Device passenger data upload time	< 60 seconds ⁵
	Mobile Device biometric first-read success rate ⁶	> 95%
	Mobile Device biometric subject verification false-positive rate	< 1%
	Mobile Device environmental sealing	Minimum of IP54
	Daily headcount reconciliation retrieval time	< 10 seconds
	Detainee location retrieval time	< 5 seconds

⁴ Does not assume three (3) second processing time by US-VISIT

⁵ Refers to bulk upload time for all passenger data upon confirmation of manifest

⁶ First-read refers to the first attempt to scan an individual fingerprint

Metric	Unit of Measure	Threshold
	Simultaneous tag locations supported	3,000 per two (2) second interval
	MCD Battery life	8hr (2hr actual air time) between charges
	RFID Wrist Band battery life	2 months @ 2 sec blink rate
CRS	Reservation Recommendation time	< 30 seconds
	Reservation submission time	< 5 seconds
	Detainee Attribute retrieval time	< 10 seconds
	Number of beds supported	40,000
TMS	# of ground vehicles supported	3,000
	# of individual items (unique detainees) tracked per vehicle	200
	Proof of Delivery generation time	< 10 seconds
	Schedule transportation utilizing only DRO assets	< 10 seconds
	Schedule transportation requiring combination of DRO and non-DRO assets	< 20 seconds

6.8 User Interface Requirements

The Contractor shall develop a system that meets the following user interface requirements:

- Accessible via a web browser through the EARM secure portal
- Product documentation, including quick reference guides, FAQs, and detailed step-by-step guides are available on-line
- Single sign-on through the EARM application portal using role-based security with support for third party access to select components and activity level enable/disable
- Consistent layout/look-and-feel of the EARM application
- Graceful error handling with readable reason codes, including information for submitting a help desk request
- Responds to user actions in five (5) seconds or less
- Support for multiple languages (at a minimum: English, Spanish)

6.9 COTS Requirements

The Contractor shall develop the BST&T solution using commercially available software packages that meet the following criteria:

- Is currently commercially available with an enterprise license option on a per-processor basis (not per user)
- Is not at an end-of-lifecycle release or mandatory upgrade path (either current or planned)
- Is not in a beta release, pre-production, or proof-of-concept
- Is installed at a minimum of three (3) clients with the equivalent performance criteria required by BST&T
- Is supported by an established technical help desk
- Source code and proprietary documentation is maintained by a third party escrow agent and shall be made available to the Government if the COTS vendor files for bankruptcy or fails to meet the terms of the software license agreement
- Does not require customization to the base source code to meet the BST&T desired functionality
- Does not require proprietary tools for extracting data and follows open standards (e.g., SOA / XML-based) for interoperability
- Is capable of interfacing with single sign-on products
- Is extensible/customizable using Application Program Interfaces (APIs) or Service Oriented Architecture (SOA)

6.10 Hardware Replacement

All hardware used in the BST&T solution shall be subject to a minimum of one (1) year OEM warranty. The Contractor shall offer replacement cost on a per unit basis for Operations and Maintenance (O&M) following the one (1) year warranty period.

7.0 OPERATIONS AND MAINTENANCE

The Contractor shall develop an Operations and Maintenance (O&M) plan. The plan shall address system change requests, standard operating procedures, system monitoring, periodic maintenance, installation procedures, and necessary staffing levels to adequately support the application following the production release.

7.1 Solution Acceptance and Transition

Following production release of a BST&T component, the Contractor shall provide a minimum of O&M support (not to exceed 90 days), after which the Contractor shall transition the tasks to a third party contractor. The Contractor shall adhere to the KPPs defined for the solution following the transition to a third party contractor. The Contractor shall obtain formal signed acceptance of the solution from the OCIO Project Manager prior to the transition to a third party contractor.

7.2 Software Maintenance Support

Software modifications to applications are based upon the submission and Government approval of a System Change Request (SCR). Modifications are classified as minor, moderate, or major, where:

Modification Type	Estimated Effort Required
Minor	1 – 40 Hours
Moderate	41 – 160 Hours
Major	161 – 500 Hours

Prior to commencing a system modification, the Contractor and the OCIO Project Manager shall agree on the degree of the modification as minor, moderate or major. Emergency maintenance shall be performed at the direction of the Government. The respective OCIO Project Manager must approve all SCRs in writing.

7.3 Operational Support

The Contractor shall fully maintain the BST&T software developed under this task up through the initial prototype / pilot and transition to a 3rd party Contractor 90 days after production launch. Typically maintenance activities involve software modifications that do not change the basic system's existing functionality. However, some maintenance activities shall be driven by requirements to adapt to a changing environment such as a new release of a database management system or programming language, or migrating to new technology platforms; e.g. Web environment. The development of new (or modification of) reports is also included in the maintenance task. The infrastructure application maintenance activities are those day-to-day processes or procedures that involve modifications necessary to sustain current operations and mandatory changes required as a result of legislative action. Minor modifications to the software may be a maintenance activity depending on complexity and system impact. These modifications may be bug fixes, minor adjustments, or necessary - must-do modifications brought about by external forces (e.g., COTS, OS patch, Security).

The Contractor shall perform all system administration activities associated with DRO application processes. These activities shall include regular monitoring of system resource utilization, disk storage utilization, identification of corrupt files or processes, system archiving, data archiving, installing operating system/software updates/versions and performing nightly application backups. Correcting flaws in software applications that escaped detection during development and testing of the system, or that have been introduced during previous maintenance activities. Improving software attributes such as performance, memory usage, and documentation

The Contractor shall participate, as needed, in system administration activities associated with application and database processes. As issues are reported, the Contractor shall assist in the resolution of problems and provide any technical support that shall be needed.

7.4 Problem Analysis

The Contractor shall provide Problem Analysis support for application components including:

- Problem Trending Tracking
- Performance Validation Support
- Subject Matter Expert (SME) Support
- COTS Integration Support
- Technical Refresh Support
- Technical Documentation Support
- Knowledge Transfer Support

7.4.1 Problem Trending Tracking

The Contractor shall collect as part of the day-to-day problem resolution efforts trending or repeating problems. The Contractor shall document, assign a risk value (High, Medium, or Low), and include in the monthly status report all known bugs, incompatibility issues, end-of-life products, custom code limitations and similar information that are issues within the infrastructure. If there are formal projects to resolve any of the tracked issues, the status of the resolution shall be tracked by the performing project.

7.4.2 Performance Validation Support

The Contractor shall support BST&T in monitoring infrastructure production performance and providing O&M support to ensure that system performance is optimized. The Contractor shall support BST&T to conduct and perform engineering and analysis activities and to develop recommendations and plans to handle peaks, i.e., (mass migration) for central reservation (bed space) periods, transportation management and detainee location tracking periods.

The Contractor shall work with the Government to perform Integration Coordination Services to include, but not limited to:

- Reviewing lessons learned following a peak reservation, transportation or tracking period
- Updating volumetric data based on revised estimates provided by Government
- Analyzing prior year peak empirical data
- Conducting performance related testing
- Hosting Performance Engineering BST&T meetings to develop engineering recommendations for handling estimated volumes
- Developing White Papers to support basis for engineering recommendations
- Building out various development, testing, and production environments
- Developing hardware/software migration road map for out-years
- Supporting external trading partner integration testing

7.4.3 COTS Integration Support

The Contractor shall support new COTS products that require integration with the BST&T Infrastructure.

This activity may include but is not limited to:

- Planning support (including scheduling, test plan development)
- Integration Testing
- Problem Resolution
- Recommendations on findings

7.4.4 COTS Technical Refresh

The Contractor shall provide assistance, as directed by the Government, in supporting technical refreshment activities. The tasking may support planning, scheduling, testing and implementing refreshment activities. The Contractor shall support the BST&T COTS applications with enhancements to the existing Infrastructure resulting from new project releases and/or required Infrastructure COTS upgrades for existing projects.

7.4.5 COTS Installation Configuration

Following the BST&T COTS installation of packages, the Contractor shall provide installation configuration SMEs to configure COTS packages in support of development, test and operations. Installations configurations shall conform to all applicable policies, procedures, settings and evaluations necessary to make the system operational.

7.4.6 COTS Updates

The Contractor shall support BST&T Operations in maintaining current or applicable versions of installed COTS packages in production. Potentially, different software releases may be required for different systems due to software compatibility issues either with other COTS packages, or with custom developed middleware. All applicable BST&T Operations processes concerning configuration/change management shall be followed. Where BST&T Operations does not have an applicable process, defined modernization processes shall either be followed, or changed appropriately, for BST&T Operations adoption.

7.4.7 Help Desk Requests

The Contractor shall provide all solution support during the pre-acceptance phase of work, which shall include the solution prototype/pilot. Following solution acceptance, and transition to a third party contractor for O&M, the Contractor shall provide TIER 3 support, as approved by the OCIO Project Manager, and shall support escalation to the COTS vendor if deemed necessary. The Contractor shall develop step-by-step Remedy® scripts for help desk troubleshooting purposes following the release of the prototype/pilot.

Post production deployment, all Help Desk calls are first directed to the ICE Service Desk referred to as TIER 1 at 1-888-347-7762. Functionality issues are referred to a TIER 2 DHS Help Desk, staffed by Government personnel familiar with the operation of the system. Unless specifically stated in this SOW, a Contractor Help Desk shall not be formally established. For emergency or critical issues, a 24/7/365 level of support must be available, whereas, the

Contractor shall be on-call and respond within one (1) hour. Such non-Monday -Friday (7AM - 8PM EST) requests for support shall be rare and can most likely be addressed via telephonic communications. The Contractor shall document user problem notifications and solutions in Remedy®.

7.4.8 Configuration Management

The Contractor shall conduct project-level configuration management for all development and maintenance work for the DRO applications. The Contractor shall handle all requests for changes to established baselines via the approved SCR process, including the chartering and conducting CCB meetings. The Contractor shall assign proper identification of all configuration items in accordance with agreed on conventions. This includes the proper labeling of all software releases, regardless of content. The Contractor shall submit an electronic version of all contract deliverables to the Electronic Library Management System (ELMS).

8.0 DELIVERABLES

All deliverables shall be delivered in hardcopy, electronic format and entered in the ICE ELMS. Software development deliverables, including customized source code development, COTS configurations, and SLM supporting documentation shall conform to the ICE SLM for configuration management and product acceptance procedures. Contractor shall develop documentation in the Microsoft Office Suite product approved by the Contracting Officer's Technical Representative (COTR). No other office automation product shall be used, unless approved by the Government.

8.1 Task Project Plans and Schedules

The Contractor shall develop a Project Management Plan and schedule, containing all resources, activities, and milestones necessary to accomplish work specified in the contract. The Contractor shall use the Project WBS below to develop its product-oriented Contractor Work Breakdown Structure (CWBS) and dictionary for approval by the government. The CWBS shall be prepared in accordance with the guidelines contained in MIL-HDBK-881A and be delivered with the Contractor's project management plan. Technical activities in the schedule shall be at a level of detail sufficient for the Contractor to manage the task. The Contractor shall develop a new Project Management Plan and schedule whenever a modification is made to the base contract and shall be submitted to the ICE COTR for review and approval. The Contractor shall provide the Project Management Plan and Schedule ten (10) days after contract award or modification. The PWBS primary elements shall include:

- Project Management
- DLT
- CRS
- TMS
- Systems Integration
- Training
- O&M Support

8.1.1 Project Management Plan

The Contractor shall develop a Project Plans for outlining the project execution and project control, including the approach, roles, responsibilities, cost, schedule, and scope. The document shall be used to facilitate key decision points, milestones, and communication among key stakeholders. The project plan shall be tailored to accommodate an Agile development methodology.

The Contractor shall establish, maintain, and use in the performance of this contract, an integrated performance management system. Central to this integrated system shall be a validated Earned Value Management System (EVMS) in accordance with FAR sections 34.201, 34.202, 52.234-3 and the EVMS Guidelines contained in ANSI/EIA-748B. *The Government will not formally validate/accept the Contractor's management system (no formal review). While no validation is required, the Government will observe compliance during the course of the contract through the EVMS surveillance process.* CPRs shall be prepared in accordance with the DHS version of DI-MGMT-81466A. CFSRs shall be prepared in accordance with directions contained in the DHS version of DI-MGMT-81468

8.1.2 Project Schedule

The Contractor shall develop and maintain an Integrated Master Schedule (IMS) in conformance with DI-MGMT-81650. The schedule shall contain the planned events and milestones, accomplishments, exit criteria, and activities from contract award to the completion of the contract. This IMS shall be delivered not later than ten days prior to the integrated baseline review (IBR). The project schedule shall be compatible with Microsoft Project. The phased delivery approach shall be validated in ATTACHMENT E.

The Contractor shall engage jointly with the Government's program manager in Integrated Baseline Reviews (IBRs) to evaluate the risks inherent in the contract's planned performance measurement baseline. The initial IBR shall be conducted not later than 60 days after contract award. Subsequent IBRs shall be conducted as needed following major changes to the baseline.

8.1.3 Risk Management Plan

The Contractor shall develop a Risk Management Plan for addressing risks associated with scope, cost, schedule, and the steps necessary for remediation.

8.1.4 Training Plan

The Contractor shall develop a Training Plan for describing the tasks associated with training the end-user community of the solution. The Training Plan shall take into consideration a geographically distributed workforce with various degrees of experience supporting the operation, and the complex distribution mechanisms for offering training.

8.1.5 Communication Plan

For meeting the widespread adoption goals of the project, the Contractor shall develop a Communication Plan. The Communication Plan shall take into consideration the efforts necessary to adopt a major operational change, and the various internal and external stakeholders that have a vested interest in the implementation of the solution.

8.2 Progress Reports and Program Reviews

To accurately track the completion of the solution, the Contractor shall submit to the Government the following status reports in a timely manner:

8.2.1 Progress Reports

The Contractor shall prepare a monthly progress report. Initial reports are due 30 days after task award and every 30 days thereafter until the last month of performance, the final delivery shall occur 10 days before the end of the of the final option period and shall summarize performance during the period of performance and provide the status of any planned transition activity. The monthly report shall contain the following:

- Description of work planned
- Description of work accomplished
- Analysis of the difference between planned and accomplished
- Work planned for the following month
- Open issues

8.2.2 Program Reviews

The Contractor shall participate in monthly Program Reviews with the OCIO Project Manager or designee to review selected projects. The purpose of this meeting is to ensure the state of production processing; and, that all application software efforts are coordinated, consistent, and not duplicative. The Contractor shall provide budgets; schedules and other program related issues should also be addressed when required. The program review is intended to be an informal executive summary of these events, and should require only minimal presentation time.

8.2.3 Weekly Status Report

The Contractor shall prepare a weekly status report for the OCIO Project Manager. Generally, these reports include the week's accomplishments, any deviations from planned activities; field related issues, other issues, and planned activities for the next period. The weekly reports shall be delivered in a meeting, by electronic (e-mail) or in hard copy. Additionally, the OCIO Project Manager shall request impromptu meetings to discuss status or issues.

8.2.4 Monthly Status Report

The Contractor shall prepare a monthly status report for the OCIO Project Managers for the BST&T solution that shall be considered high priority and visible. Generally, these reports include the month's accomplishments, any deviations from planned activities; field related issues, other issues, and planned activities for the next period. The Contractor shall submit reports electronically via e-mail.

8.3 Presentations, Demonstrations, and Project Support Materials

The Contractor shall prepare project presentations, conduct demonstrations, and prepare support materials such as designing system information guides or preparing project displays. It is estimated that a total of two instances of any one of these shall be required during a year. Each such instance shall encompass a single or multiple projects.

8.4 Acceptance Criteria

Deliverables shall be deemed acceptable if the document adequately covers all required topics, meets general quality measures; and, is professionally prepared in terms of format, clarity and readability; and is delivered in hard and electronic copy on time to the designated delivery location. General quality measures, as set forth below, shall be applied to each work product received from the Contractor under this SOW.

- **Accuracy:** Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- **Clarity:** Work Products shall be clear and concise. Any/All diagrams and graphics shall be easy to understand and be relevant to the supporting narrative.
- **Consistency to Requirements:** All work products must satisfy the requirements of this statement of work.
- **File Editing:** All text and diagrammatic files shall be editable by the Government.
- **Format:** Work Products shall be submitted in hard copy (where applicable) and in media mutually agreed upon prior to submission. Hard copy formats shall follow any specified Directives or Manuals.
- **Timeliness:** Work Products shall be submitted on or before the due date specified in this statement of work or submitted in accordance with a later scheduled date determined by the Government.

The documents shall be considered final upon receiving Government approval. All deliverables shall be delivered via e-mail and a letter of transmittal and to the COTR, ICE OCIO; Room 600; 801 I Street NW; Washington, DC; 20536 not later than 4:00 PM on the deliverable's due date.

Deliverables Summary & Matrix

Deliverable	Frequency	Copies	Recipients
Project Management Plan	Monthly Updates, by 5 th day (for previous month)	3	PM (1) copy/COTR (1) copy, ELMS (electronic)
Integrated Master Schedule	Weekly, by COB Friday (for current week)	3	PM (1) copy/COTR (1) copy, ELMS (electronic)
Risk Management Plan	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy, ELMS (electronic)
Training Plan	Monthly Updates, by 5 th day (for previous month)	3	PM (1) copy/COTR (1) copy, ELMS (electronic)
Communication Plan	Monthly Updates, by 5 th day (for previous month)	3	PM (1) copy/COTR (1) copy, ELMS (electronic)

Deliverable	Frequency	Copies	Recipients
Progress Reports	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Program Reviews	Weekly, by COB Friday (for current week)	2	PM (1) copy/COTR (1) copy
Weekly Status Reports	Weekly, by COB Friday (for current week)	2	PM (1) copy/COTR (1) copy
Monthly Status Reports	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Contract Performance Reports	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Contract Funds Status Report	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Financial Reporting	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Monthly Burn-Rate Report	Monthly Updates, by 5 th day (for previous month)	2	PM (1) copy/COTR (1) copy
Presentations, Demonstrations, Project Support Materials	As required	As Required	As Required

Unless otherwise specified, all documentation shall be in Microsoft Office 2003.

The Government will review documentation submitted by the Contractor and provide comments within 14 business days.

8.5 Product Acceptance

Information technology products delivered under this SOW shall be accepted when they meet all requirements, which includes validating objectives, processes and functionality, successful prototyping/piloting of solution, performance metrics, usability, technical accuracy or merit, compliance to ICE technical standards, and all coordination, review and approval forms required by the SLM Manual. Initial deliverables shall be considered draft versions and shall be reviewed and accepted or rejected by the Government within ten (10) working days.

8.6 Non-Disclosure Statements

Each Contractor employee who works on this contract shall have a signed “non-disclosure” agreement on file with the COTR.

9.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

Government Furnished Equipment (GFE) will not be provided. Documentation relevant to the SDD application systems will be available to the vendors upon award of the TO. Upon award (and obtaining required security clearance), the successful Contractor will be provided access to the Enterprise Library at 1101 Vermont Avenue, NW, Suite 220, Washington, DC, 20005.

10.0 PLACE OF PERFORMANCE

Work on this contract shall be performed primarily at Contractor's facilities. Frequent travel to DHS offices in the Washington, DC metropolitan area for meetings and briefings shall be required. The Contractor's operating facility shall be within the Washington, DC Metropolitan area for travel time to the DHS, ICE OCIO Office located 801 I Street NW, Washington DC. In some cases, work shall also be performed at various other locations.

To support implementation, the Contractor shall be required travel to the following based upon the request of the Government, to the following locations outside the metropolitan Washington, DC area including DRO Service Processing Centers, Contract Detention facilities, and IGSA facilities.

To support implementation, the Contractor shall be required to perform tasks at other locations, both within the continental United States and outside the continental United States, in support of activities within the scope of this contract.

11.0 PERIOD OF PERFORMANCE

The period of performance for this contract is one base year plus *3 one-year options* from the start of the contract to the end of the period of performance.

12.0 ACCESSIBILITY REQUIREMENTS

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable standards have been identified:

36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches

such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then “1194.21 Software” standards also apply to fulfill functional performance criteria.

36 CFR 1194.23 – Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available. This standard applies to any training videos provided under this work statement.

36 CFR 1194.31 – Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required “1194.31 Functional Performance Criteria”, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.2(b) – (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available and meet some but not all of the standards, the agency must procure the product that best meets the standards.

When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires approval from the DHS Office on Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

36 CFR 1194.3(b) – Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors

assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

13.0 OTHER DIRECT COSTS (ODCS)

The Government anticipates extensive travel to DRO field offices in support of this contract. The Contractor shall propose anticipated ODCs with appropriate justification and explanation in its technical and cost proposals. Once accepted those anticipated costs shall be included in the total estimated cost ceiling applied to the awarded contract.

All ODC expenditures shall be pre-approved by the Government in accordance with the following guidance:

- Travel shall be in compliance with Government per-diem rates
- The COTR will approve individual ODC requests totaling \$2,500 or less and all-domestic travel. This approval authority will include the purchase of personal computers (PCs), laptops, cell phones, pagers, handheld computers, cameras, and video equipment, in addition to computer systems/workstations, software and training which can only be approved by the COTR.
- The COTR will approve all international travel based on the recommendation of the OCIO Project Managers. OCIO Project Managers will review requirements, i.e. purpose of the trip, destination, number of travelers, and the duration of each trip.

The COTR will, with the recommendation of the OCIO Project Manager, approve all requests for payment of Contractor training cost. DHS, ICE will only pay for training costs associated with the training of Contractor personnel necessary to support DHS, ICE unique applications/requirements. ICE expects that all Contractor personnel will be properly trained and maintain proficiency in their field of expertise at no additional cost to the Government. Therefore the Government will not pay for training courses or seminar that Contractor personnel would normally attend to remain proficient or current in their fields of expertise. Costs associated with such training will be the sole responsibility of the Contractor.

14.0 OVERTIME

Neither the Contractor nor any teaming partners shall be authorized to invoice the Government for overtime.

15.0 KEY PERSONNEL

A number of billets within the Contractor's organization are expected to significantly affect Program success, and are accordingly designated as key. For this task, the Project Manager, the Functional Lead, and the Architecture/Technical Lead shall be designated as Key Personnel and shall be a full-time employee of the Contractor at the time of task award. Key personnel are expected to serve for the life of the Task, or until replacements with equivalent skills are nominated by the Contractor and accepted by DHS, ICE. In addition to these designations, the Government reserves the right to revise this designation during contract performance, including requiring the identification of additional Key Personnel.

During the first 180 days of contract performance, no key personnel substitutions shall be permitted, unless necessitated by compelling reasons including, but not limited to, an individual's illness, death, termination of employment, declining an offer of employment (for those

individuals proposed as contingent hires), or maternity leave. In any of these events, the Contractor shall promptly notify the CO and the COTR, and provide the information required herein.

Following this initial 180-day period, DHS, ICE will consider requests for changes in key personnel, if necessary. COTR and CO approval is required prior to any change in key personnel. Requests for key personnel changes shall be submitted at least (25) days in advance of a prospective substitution, and provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume of the proposed new personnel, and any other relevant information necessary to evaluate the impact of the prospective substitution on the Program requested by the COTR and CO. The qualifications of proposed substitute key personnel must meet or exceed the qualifications of personnel whom they are proposed to replace. The COTR and CO will generally accept or reject the resume within ten (10) working days.

The contract shall identify key personnel in the proposal regardless of the type of task. NOTE: Key personnel may not be added nor removed from the contract without express approval of the COTR. The following descriptions are key personnel required by the contract.

15.1 Project Manager

The Project Manager (PM) shall demonstrate progressively responsible experience as a PM or Deputy PM in the management of Federal Government systems analysis, implementation, resource allocation, planning, evaluation, and familiarity in the management of cost reimbursable type contracts. The PM shall have sufficient familiarity with modern management practices to apply.

- Candidate must have a PMI Project Management Professional (PMP) certification within 60 days after contract award
- Candidate must have documented managerial or supervisory experience sufficient to ensure positive direction of subordinates
- Candidate must have experience managing the balance between cost, schedule, cost, quality, and risk in system implementation projects
- Candidate must have experience in iterative software development delivery and has a thorough understanding of the Agile development methodology
- Candidate must have experience in effectively scheduling and communicating with clients
- Candidate must be able to demonstrate knowledge of systems integration techniques, web technology, system trade-off analysis, and program planning
- Candidate must have thorough knowledge of Federal Government planning, programming, budgeting and execution principles of Federal Government fiscal management
- Candidate must have thorough knowledge of staffing technical implementation projects and assigning resources as-needed during the software delivery lifecycle

15.2 Functional Lead

The Functional Lead shall be responsible for the development of business system software requirements. The Functional Lead shall have experience in creating software documentation, use cases, process diagrams, user interface wire frames, and supporting documentation such as release notes and end-user communication. The Functional Lead shall be responsible for fulfilling mission needs into system features and functions within a specific scope.

- Candidate must have formal design/development methodology experience in software delivery
- Candidate must have documented managerial or supervisory experience sufficient to ensure positive direction of subordinates
- Candidate must have excellent written and verbal communication and organizational skills
- Candidate must possess strong facilitation, negotiation, and conflict resolution skills
- Candidate must have experience developing systems in the Federal Government, and preferably has experience working with law enforcement or immigration systems
- Candidate preferably has experience working in supply chain and capacity planning

15.3 Architecture/Technical Lead

The Architecture/Technical lead shall be responsible for developing the underlying architecture for the system and oversee the delivery tasks for all technical staff. The Architecture/Technical lead shall be proficient in managing trade-offs and priorities of technology as it relates to budget, scope, and schedule.

- Candidate must have experience leading a team of programmers, architects, interface designers, and database engineers
- Candidate must have experience
- Candidate must have experience in iterative development delivery and has a thorough knowledge of Agile development methodology
- Candidate must have experience in lead system integration efforts and has a thorough familiarity with related application and development tools
- Candidate must have experience in database design and architecture
- Candidate must have experience in successfully managing and deploying web applications using Oracle databases and Java application servers
- Candidate must have experience in network design and systems architecture
- Candidate must have thorough knowledge of staffing technical implementation projects and assigning resources as-needed during throughout the lifecycle of the project

16.0 TRANSITION

The Contractor shall be responsible for the transition of all technical activities identified in this task. The Contractor shall complete the technical Transition Management Plan (TMP) within 90

days after contract award. The technical activities, which shall be included as part of the technical transition, consist of transition plans for the:

- Inventory and orderly transfer of all Government Furnished Equipment/Property (GFE/GFP), software and licenses
- Transfer of documentation currently in process at the time of TO award
- Transfer of all Software coding in process at the time of TO award
- Establishment of a facility for housing hardware/software, if any
- Coordinating the body of work with the current Contractor and turnover of tasking, staffing, etc.
- Review and coordination of changes from a project's TMP to include the closure of gaps within the software
- Work with the infrastructure ICE receiving organizations in the identification and initial resolution/mitigation of all Infrastructure gaps according to the TMP
- Incorporate readiness feedback from discussions with receiving organizations
- Discuss and analyze high level project infrastructure impacts with project and receiving organization managers to capture operational concerns

The Contractor's transition plan shall be approved by DHS, ICE and shall contain a milestone schedule of events and system turnovers. The TMP shall transition systems with no disruption in operational services. The Contractor shall provide the transition management plan 15 days after contract award. To ensure the necessary continuity of services and to maintain the current level of support, DHS, ICE will retain services of the incumbent Contractor for the transition period, if required.

At the completion of the period of performance of this contract, the Contractor shall fully support the transition of Systems Development requirements to the successor Offeror. Activities include supporting all of the activities listed above by making available personnel and documentation required to facilitate a successful transition.

Upon completion of the authorized period of performance for this contract including exercised options, the contracting officer shall issue a modification to authorize and fund the transition activity of the outgoing Contractor.

17.0 PERIODIC REVIEWS

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COTR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity,

availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

APPENDIX A: LIST OF ACRONYMS

This section provides a list and definition of the acronyms used in this document.

Acronym	Phrase
“A” File	Alien File
ADP	Average Daily Population
AFIS	Automated Fingerprint Identification System
AFOD	Assistant Field Office Director
AO	Asylum Officer
AOIC	Assistant Officer in Charge
AOR	Area of Responsibility
API	Application Programming Interface
APSO	Asylum Prescreening Operations
APSS	Automated Prisoner Scheduling System (U.S. Marshals Service)
ATD	Alternatives to Detention
ATMS	Alien Transportation Management System
ATU	Air Transportation Unit
AVL	Automated Vehicle Location
BOP	Bureau of Prisons
BPO	Border Patrol Office
CAD	Computer Aided Design
CAP	Criminal Alien Program
CBA	Cost-Benefit Analysis
CBP	Customs and Border Protection
CCA	Corrections Corporation of America
CDF	Contract Detention Facility
CDL	Commercial Driver’s License
CLASS	Consular Lookout and Support System
CONUS	Continental United States
COTR	Contracting Officers Technical Representative
COTS	Commercial Off- The-Shelf
CPD	Cellular Phone Device

Acronym	Phrase
CRS	Central Reservation System
CSF	Critical Success Factors
DACS	Deportable Alien Control System
DAD	Deputy Assistant Director
DBMS	Database Management System
DDMS	Detention Database Management System
DDO/DO	Detention and Deportation Officer/Deportation Officer
DETLOC	Detention Location
DETS	DACS Detention Summary
DFOD	Deputy Field Office Director
DHS	Department of Homeland Security
DIHS	Division of Immigration Health Services
DISCO	Defense Industrial Security Clearance Office
DLT	Detainee Location tracking
DMARC	Detention Management and Removal Coordinator
DOCC	Detention Operations Coordination Center
DOD	Department of Defense
DOJ	Department of Justice
DOS	U.S. Department of State
DRO	Office of Detention and Removal Operations
DROM	Detention and Removal Operations Modernization
DMTS	Detention Management Tracking System
EA	Enterprise Architecture
EABM	Enforcement Apprehension and Booking Module
EADM	Enforcement Alien Detention Module
EARM	Enforcement Alien Removal Module
EID	Enforcement Integrated Database
EIO	Executive Information Office
ENFORCE	Enforcement Case Tracking System
EOIR	Executive Office for Immigration Review
ER	Expedited Removal

Acronym	Phrase
EREM	Enforcement Removal Module (retired)
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
eTD	Electronic Travel Document
ETL	Extract, Transform and Load
FBI	Federal Bureau of Investigations
FFMS	Federal Financial Management System
FINS	Fingerprint Identification Number System
FO	Field Office
FOD	Field Office Director; or Field Office District
FRD	Functional Requirements Document
FTE	Full-Time Equivalent
FTP	File Transfer Protocol
FugOps	Fugitive Operations
FY	Fiscal Year
GAO	Government Accountability Office
GEMS	General Counsel Electronic Systems
GOTS	Government Off-the Shelf
GPS	Global Positioning System
GUI	Graphical User Interface
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HQ	Headquarters
IAFIS	Integrated Automated Fingerprint Identification System
ICE	U.S. Immigration and Customs Enforcement
ID	Identification
IDENT	Automated Biometric Identification System
IEA	Immigration Enforcement Agent
IGA	Intergovernmental Agreement

Acronym	Phrase
IGSA	Intergovernmental Service Agreement
IHG	InterContinental Hotels Group
IIDS	ICE Integrated Decision Support
IJ	Immigration Judge
INS	Immigration and Naturalization Service
IP	Ingress Protection
IRD	Integrated Requirements Document
IrDA	Infrared Data Association
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
JCAS	Justice Cost Accounting System
JDBC	Java Database Connectivity
JPATS	Justice Prisoner and Alien Transportation System
LAN	Local Area Network
LMS	Lodging Management System
LOD	Length of Detention
LOV	List of Values
MC	Mobile Computing
MoM	Message Oriented Middleware
MIL-STD	Military Standard
MOU	Memorandum of Understanding
NCIS	National Criminal Investigation Service
NFTS	National File Tracking System
NIEM	National Information Exchange Model
NIJ	National Institute of Justice
NTA	Notice To Appear
OCC	Operations Coordination Center
OCIO	Office of the Chief Information Officer
OCONUS	Outside Continental United States
ODBC	Open Database Connectivity
ODF	Otay Mesa Detention Facility

Acronym	Phrase
OFDT	Office of the Federal Detention Trustee
OFO	Office of Field Operations
OAG	Official Airline Guide
OI	Office of Investigations
OIC	Officer-in-Charge
OIG	Office of the Inspector General
OMB	Office of Management and Budget
OPLA	Office of Principal Legal Advisor
OPR-PSU	Office of Professional Responsibility, Personnel Security Unit
OR	Own Recognizance
ORG	Operation Reservation Guaranteed
ORR	Office of Refugee Resettlement
OTM	Other-than-Mexican
PC	Personal Computer
PDA	Personal Digital Assistant
PHS	Public Health Service
POC	Point of Contact
POCR	Post-Order Custody Review
POE	Point/Port of Entry
POD	Port of Departure
RAP	Record of Arrest and Prosecution
RAPS	Refugees, Asylum and Parole System
RFID	Radio Frequency Identification
RTLS	Real-Time Location System
SAIC	Science Applications International Corporation
SBI	Secure Border Initiative
SDDO	Supervisory Detention and Deportation Officer
SHU	Segregated Housing Unit
SIEA	Supervisor Immigration Enforcement Agent
SME	Subject Matter Expert
SMS	Subject Matter Specialist, Short Message Service

Acronym	Phrase
SOA	Service Oriented Architecture
SOP	Standard Operating Procedures
SOW	Statement of Work
SPAWAR	Space and Naval Warfare Systems Center
SPC	Service Processing Center
SSN	Social Security Number
SSO	Single Sign-On
STIP	Stipulated Removal
SYS	System
TAC	Third Party Agency Check
TAR	True Accept Rate
TD	Travel Document
TECS	Treasury Enforcement Communications System
TIF	Tuberculosis Isolation Facility
TMS	Transportation Management System
TRACES	Tri-Service Automated Cost Engineering System
TSA	Transportation Security Administration
TSWG	Technology Solutions Working Group
UI	User Interface
UML	Unified Modeling Language
URL	Uniform Resource Locator
USCIS	United States Citizenship and Immigration Services
USMS	United States Marshals Service
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
VD	Voluntary Departure
VoIP	Voice Over Internet Protocol
VR	Voluntary Return
VTC	Video Conferencing
WAN	Wide Area Network
WAP	Wireless Access Protocol
XML	eXtensible Markup Language

Acronym	Phrase
XQS	Oracle XML Query Service

APPENDIX B: GLOSSARY

This section provides a list and definition of the terms and abbreviations used in this document.

Term	Definition
287(g)	Section 287(g) of the Immigration and Nationality Act - The Illegal Immigration Reform and Immigrant Responsibility Act, effective September 30, 1996, added Section 287(g), performance of immigration officer functions by State officers and employees, to the Immigration and Nationality Act (INA). This authorizes the secretary of the U.S. Department of Homeland Security (DHS) to enter into agreements with State and Local law enforcement agencies permitting designated officers to perform immigration law enforcement functions pursuant to a Memorandum of Agreement (MOA) provided that the Local law enforcement officers receive appropriate training and function under the supervision of sworn U.S. Immigration and Customs Enforcement (ICE) officers.
G-324A	Form included as part of the Facility Inspection Sheet that ICE developed for each facility on an annual basis. The Facility Inspection Sheet assigns a rating for each facility based on ICE-DRO standards. Form G-324A contains basic facility characteristic information as well as population figures for the previous 12 months.
I-77	The I-77 is a claim ticket for a detainee's luggage and personal belongings. The ticket contains a description of contents which the detainee surrenders once they have been processed into a detention facility.
I-203	The 203 is a form that documents DRO's decision to detain or release an alien. The form is included in a detainee's "A" file and travels with the detainee while they are in DRO custody.
I-216	The 216 is a form that serves as a record for the transfer of a detainee from one location to another. The form documents the name, nationality and criminal status of an alien, as well as other possible information, and travels with the alien while they are being transferred.
"A" File	An "A" File is a hard-copy folder(s) containing all relevant data concerning a specific alien, including all standard forms (e.g., Notice to Appear). USCIS is responsible for the custody of all closed "A" Files. For repeat offenders, the same "A" File is used with additional information added. For aliens apprehended for the first time, a new "A" File number is provided by USCIS. "A" File numbers are recorded in the Central Index System (CIS). "A" Files are bar-coded. As the "A" File moves within a particular facility, it is to be scanned and its location recorded in CIS. An "A" File accompanies the alien

Term	Definition
	as the alien is transferred between detention facilities. If an apprehended alien is a repeat offender, a temporary “A” File is created while the “official” “A” File is secured from the USCIS repository.
“A” Number	Alien registration number. A unique identifier associated with each alien.
Ad hoc Report	A report that is not pre-designed but is constructed from a user’s inputs, options, selections of fields, ranges, sorting and grouping, filtering, and arithmetic calculations of groupings.
Admission	Lawful entry of an alien into the United States after inspection and authorization by an immigration officer.
Alert	In relation to systems: This refers to an electronic notification, to an on-screen user, which "alerts" the user to a system condition (e.g., error message, warning message).
Alien Information	All information about an alien, including biographic, biometric, medical, and transfer information.
Application	The use of capabilities (services and facilities) provided by an information system to satisfy a set of user requirements.
Application Programming Interface	A set of routines that an application uses to request and carry out lower-level services performed by a computer's operating system. Also, a set of calling conventions in programming that define how a service is invoked through the application.
Architecture Guiding Principles	General rules and guidelines, intended to be enduring and seldom amended, that inform and support the way in which an organization sets about fulfilling its mission.
Assets	In business and accounting, an asset is any economic resource controlled by an entity as a result of past transactions or events and from which future economic benefits may be obtained (e.g. Bed Space or Van).
Attribute	Physical feature of a detainee, or item of inventory.
Automated Data Capture (ADC)	The method of collecting and entering data about an object into a computer system without the use of a keyboard. Technologies typically considered as part of ADC include bar code, RFID and voice recognition
Automated Fingerprint Identification System (AFIS)	A system to store and match one or many unknown fingerprints against a database of known fingerprints.
Availability	In relation to CRS/TMS: The administration, set-up, and control of inventory for all initiating channels. This includes the request for

Term	Definition
	availability, the resulting response, as well as adjustments to inventory from physical inventory transactions and external applications.
Baseline	A specification or product that has been formally reviewed and agreed upon and, thereafter, serves as the basis for further development.
Basic Information	Key contact information associated with a detainee (e.g. name, address, phone numbers, ID numbers, next of kin, and closest relative's information).
Biographic Data	Also known as demographic or descriptive data, information associated with an individual that may be described alphanumerically and used for identification purposes, (e.g., color of eyes, date of birth, etc.).
Biometric Data	Information gathered from the unique features or behavioral characteristics of a person that can be digitized and used for the purpose of identification or verification. (E.g. fingerprints, palm prints, facial geometry, retina scan, iris scan, voice analysis and signature characteristics).
Block	A grouping of bed space inventory (e.g., beds, pods, barracks).
Book-in/Book-out	In relation to CRS: The initiation and completion of fulfilling a reservation for a bed. This includes administrative functions such as activation and deactivation of tracking technology, update of bed availability status and any associated communications.
Business Continuity	The ability of an organization to continue to function even after a disastrous event, accomplished through the deployment of redundant hardware and software, the use of fault tolerant systems, as well as a solid backup and recovery strategy.
Business Continuity Plan	All encompassing term covering both disaster recovery planning and business resumption planning. This umbrella term also refers to other aspects of disaster recovery, such as emergency management, human resources, media or press relations, etc.
Business Requirement	High-level statement of the goals, objectives, or needs of the enterprise describing such things as why a project was initiated, possible achievements, and the metrics which will be used to measure success. These requirements should be independent of technology.
Business Rule	A directive, policy or procedure within an organization.
Canned Report	A pre-designed, repeatable report.
Criminal Alien Program (CAP)	The Criminal Alien Program (CAP) focuses on identifying criminal aliens who are incarcerated within Federal, State and Local facilities

Term	Definition
	thereby, ensuring that once they are released, they do not enter into the community. This is accomplished by securing a final order of removal prior to the termination of their sentence.
Capacity	In relation to CRS: The maximum amount or number of beds a facility can provide to DRO.
Capture	In relation to systems: To enter data, images, or other information into a system; may be accomplished manually or automatically.
Case	An on-going activity or object, to gather, process, and document information about an individual or a group of individuals. Types of cases include alien, facility, custody, and removal cases.
Case Management	A system of controls that ensures that the appropriate action is taken on alien case files, when needed. This includes taking and recording appropriate actions, based on the applicable removal process and following up with other entities such as the Immigration Court, Federal Court and CBP to issue the removal order. This also includes working with foreign consulates when DRO has applied for a travel document and making travel arrangements for an alien.
Channel Services Layer	In a layered solution architectural model, this layer provides (users or systems) access to business processes through multiple channels or devices.
Charging Document	The written instrument which initiates a proceeding before Immigration Court. These documents include a <i>Notice to Appear</i> (Form I-862), a <i>Notice of Referral to Immigration Judge</i> (Form I-863), and a <i>Notice of Intention to Rescind and Request for Hearing by Alien</i> .
Checkpoint	A location that has been identified to register the individuals for tracking purposes.
Commercial Off-the-Shelf (COTS) Application and Systems	A pre-developed software package that is commercially sold, leased, or licensed to the general public; supported and evolved by the vendor who retains the intellectual property rights; available in multiple, identical copies; and used without modification of the internals; offered by a vendor trying to profit from it.
Common Application Services Layer	In a layered solution architectural model, this is where the applications or services reside which provide business functionality.
Conceptual Architecture	A high-level view of a solution architecture which provide insight into the operational organization and where the solution supports the organization. It provides a “concept” of what the application domain looks like.
Confirmation	In relation to CRS: A notification that a unit of bed space inventory has been reserved and is taken out of available inventory.

Term	Definition
Customization	The additional services and application coding required to extend a set of base-line COTS functionality in order to fit into an organization and fulfill its business functionality.
Data Layer	In a layered solution architectural model, this layer provides the necessary services to store and access data elements stored in a specific data format either structured or unstructured.
Data Access Layer	In a layered solution architectural model, this layer provides access to the data layer where the data is stored.
Data Warehouse	A data warehouse is a database geared towards the business intelligence requirements of an organization. The data warehouse integrates data from the various operational systems and is typically loaded from these systems at regular intervals. Data warehouses contain historical information that enables analysis of business performance over time.
Deportability	Term used to denote the grounds upon which removal proceedings, initiated on or after April 1, 1997, are conducted to expel aliens from the United States.
Deportation	Term used to denote proceedings initiated prior to April 1, 1997, to expel aliens from the United States.
Detainee Discovery	The collection of detainee's biographical attributes that drive bed type needs. This functionality is expected to be provided via integration with existing applications to leverage existing data (e.g., ENFORCE).
Determining Field	In relation to CRS: A field used in weighing and scoring to prioritize a bed space recommendation reservation.
Disaster Recovery	The ability to recover from the loss of a complete site, whether due to natural disaster or malicious intent. Disaster recovery strategies include replication and backup/restore.
Dispatch	In relation to TMS: The action of directing, from a central point, the use and routes of vehicles within a transportation system.
Document/Records	Information pertaining to a case.
DRO-Dedicated Facility	A detention facility either owned by DRO or one that is chartered to house detainees for DRO.
Enterprise Architecture	Enterprise architecture is a comprehensive framework used to manage and align an organization's business processes, Information Technology (IT) software and hardware, local and wide area networks, people, operations and projects with the organization's overall strategy.

Term	Definition
Enterprise Resource Planning (ERP)	An Information Technology term referring to a hardware or software system that serves all departments within an enterprise. ERP systems integrate (or attempt to integrate) all data and processes of an organization into a unified system.
Enterprise Service Bus	In computing, an enterprise service bus is an emerging standard for integrating enterprise applications in an implementation-independent fashion, at a coarse-grained service level (leveraging the principles of service-oriented architecture) via an event-driven and XML-based messaging engine (the bus). An enterprise service bus frequently is a delivery vehicle for an Enterprise Messaging System.
Expedited Removal	Expedited Removal is a provision in the Immigration and Nationality Act (INA) under which an alien who lacks proper documentation or has committed fraud or willful misrepresentation of facts to gain admission to the United States is inadmissible and may be removed from the United States without any further hearings or review unless the alien indicates either an intention to apply for asylum or a fear of persecution.
Export	When used in reference to data, implies the ability of the user to "bulk unload" information, typically to a spreadsheet or other structured data file.
eXtensible Markup Language	A standard for creating markup languages which describe the structure of data
Extract, Transform and Load Tool	Activities required to populate data warehouses and OLAP applications with clean, consistent, integrated and probably summarized data.
Facility Information	Facility information includes, but is not limited to, name, address, type, area of responsibility, phone numbers, bed space capacity, bed space occupancy/ availability and resources.
Federated Query	Technology that utilizes efficient middleware to search multiple geographically and technologically disparate computer systems to extract, transform and present uniform but separately recorded data in an interpretive and functional interface.
Final Order of Deportation or Removal	The order of the Immigration Judge, the Board of Immigration Appeals (BIA) or other such Administrative Officer to whom the Attorney General has delegated the responsibility which concludes that an alien is deportable, removable or excludable from the United States.
Fiscal Year	Yearly period, without regard to the calendar year, at the end of which the Government determines its financial condition.
Folio/Invoice	All charges or costs associated to a detainee.

Term	Definition
Form Factor	The physical size of a device as measured by outside dimensions.
Front End System	A system which is typically used to provide access to internal data for external users. For example, a banking web site which allows customers to access their financial accounts over the internet.
Fugitive Operations	The Fugitive Operations Program (FugOps) identifies, locates, apprehends and removes fugitive aliens from the United States.
Function	A useful capability provided by one or more components of a system.
Functional Requirement	Behaviors and tasks that the system must perform, the users must perform interacting with the system, or the users perform interacting with each other.
Funded Beds (DRO)	Bed space that is financially supported by DRO dollars.
Governance	The act of affecting Government and monitoring (through policy) the long-term strategy and direction of an organization.
Graphical User Interface (GUI)	Component that provides the automated interfaces that the users access to enter and retrieve information.
Hearing Information	Information including, but not limited to, docket, docket schedules, attorneys assigned, judge, charges, court case and decisions.
Hit	A potential or verified candidate resulting from a search in an automated search of a system (e.g. fingerprint, "A" number).
Home-grown (system)	System or architecture not supported by DHS/OCIO that does not meet the standardized operating procedures.
Horizontal Integration	In a layered solution architectural model, the integration between application services identified in the Common Application Services layer.
HTML Page	A hypertext markup language document which is delivered to a user's web browser.
IAFIS	The FBI's ten-print criminal history and latent fingerprint processing system. The system receives requests, performs a subject (name) search for ten-print requests, performs the AFIS search against the Bureau's repositories, transmits a response to the originating agency, and performs appropriate file maintenance.
IDENT	System provides the users with the capability to perform biometric searches with 2 fingerprints and a photo in order to identify subjects. Used for DHS immigration violation history and fingerprint processing system
IDENT/IAFIS	The working name for the proposed integration of IAFIS/FBI and IDENT/ICE.

Term	Definition
Import	When used in reference to data, implies the ability of the user to “bulk load” information, typically from a spreadsheet or other structured data file.
Ingress Protection rating	In relation to Tracking: Defined in ANSI/IEC 60529 classify the level of protection that electrical equipment provides against the intrusion of solid objects or dust, water and accidental contact.
Initiating Channels	The avenue by which a detainee is brought into DRO custody (e.g., CBP, OI, OFO, DRO).
Integration Layer	In a layered solution architectural model,
Inter-AOR Transfers	Transfers of detainees from one facility to another facility between different AOR’s.
Intra-AOR Transfers	Transfers of detainees from one facility to another facility within the same AOR.
Intranet	Secured DHS network that is inaccessible to outside users
Lane	In relation to TMS: A predefined path between two known points within the transportation network that is used to establish an optimized route to complete a trip.
Length of Detention (LOD)	The total length of time that a detainee has been detained at a given facility.
Lifecycle	A systematic approach to problem solving composed of several phases including: Planning, Analysis, Design, Development, Testing, Implementation and Maintenance.
Load Factor	A result or imposed parameter for utilization of a vehicle and optimizing its capacity. Often represented as a percentile of capacity
Load Tender	The offer of a transportation load to a contracted provider to supply the transportation for a trip or set of trips, which can be accepted or denied.
Logical Architecture	A high-level view of a solution architecture which describes the structures of the solution that solve the functional and non-functional requirements. This provides a structural view of the solution architecture in contrast to a Conceptual Architecture.
Maintain	In relation to systems: To update a record as required.
Manifest	A document issued by a carrier, acknowledging that specified transport has been completed and detainees have been received by the facility.
Mediator	An intermediate application or service which connects to different systems in order to abstract as well as integrate the communication between the two.

Term	Definition
Medical Information	Information pertaining to the medical history of an alien while he or she is in DRO's custody, including dates, diagnosis, and treatment administered.
Military Standard (MIL-STD)	A set of requirements to help achieve standardization objectives by the U.S. Department of Defense.
National Information Exchange Model	NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.
Non-DRO Dedicated Facility	A detention facility not owned by DRO and is not chartered with solely housing DRO detainees (e.g. local and county jails).
Non-functional Requirements	Requirements that specify criteria that can be used to judge the operation of a system (e.g., "performance", "security") rather than specific behaviors. This should be contrasted with functional requirements that specify specific behavior or functions (e.g., "find a bed space," "book transportation").
Notice to Appear	A charging document for removal cases. It is a formal notice ordering an individual to appear before an Immigration Judge and advises the alien of the nature of the proceedings, the alleged immigration law violations, the privilege of being represented by an attorney at no expense to the Government, and the consequences of failing to appear at scheduled hearings.
Notification/Notify	In relation to systems: This refers to a system mechanism which will send out a notification in the form of an e-mail, pager message, SMS text message, etc.
Off-the-market	In relation to CRS: An inventory status denoting bed space inventory not available for national viewing but available for local management only.
OMEGA	Central ticketing agency employed by DRO to make commercial air reservations for transfer or removal of aliens.
Out-of-order	In relation to CRS: An inventory status denoting inventory that is unavailable for use (e.g. maintenance).
Override	Counteract the normal operation.
Parole	The release of a prisoner whose term has not expired on condition of sustained lawful behavior that is subject to regular monitoring by an officer of the law for a set period of time.

Term	Definition
Personal Computer	A stationary device with will provide access to key system business processes at various key fixed locations and connects to the network over a physical cable. Also, known as a workstation.
Physical Inventory	In relation to CRS: The administration, set-up, assignment and management of physical inventory (beds) available to each area of responsibility. This would include the inventory for Service Processing Centers (SPC), Contract Detention Facilities (CDF), and Intergovernmental Service Agreements (IGSA/IGA).
Planning Horizon	The planning horizon is the amount of time an organization will look into the future when preparing a strategic plan.
Portal Server	An application server used to manage applications and communications between it and either other systems (i.e., web services) or a user's web browser (i.e., HTML web pages)
Portal Services	An application which constructs, manages, and delivers HTML web pages to a user's web browser.
Presentation Layer	As part of a layer architecture model, this layer consists of components that run on a server and prepare the presentation of the user interface that is sent to the client device to display to the users as well as interact with the external systems.
Process	A set of activities with a beginning and an end, that results in the accomplishment of a task or the achievement of an outcome.
Process Description	A documentation of a process, including its purpose, customers, customer requirements, entrance criteria, inputs, outputs, exit criteria and required tasks.
Product Segment	In relation to CRS: Separation of inventory by attribute/characteristic (e.g., minimum security, medium security, maximum security, isolation, medical).
Recidivist	A repeat offender.
Reinstate	To restore to a previous effective state
Removal	Term used to refer to all deportation proceedings initiated on or after April 1, 1997.
Removal Subject	Alien that is subject to removal from the United States.
Repatriation	To restore someone to his or her homeland.
Reporting	The creation and administration of reports including, but not limited to, standard trends, historical analysis, ad hoc, exception reports between systems, operation, productivity, inventory items, metrics, and detainee reservation history.
Reservations	In relation to CRS: The creation, modification, cancellation, and reinstatement/ reactivation of reservations for beds in facilities across the

Term	Definition
	nation. This includes, but is not limited to queries, wait-listing, and agency and special enforcement operations inventory blocks. This should also include the initiation and completion of fulfilling a reservation for a bed(s) (book-in/book-out).
Reservation Recommender	The collection of detainee attributes and administration of reservation strategies, which are then used to identify and prioritize bed space recommendations. Offered bed space will have been validated against the detainee's profile, pre-defined business rules and availability.
Route	The course taken to go from point A to point B, including the return to point A. Includes any necessary stops in between those points using predefined lanes.
Schedule	In relation to TMS: Booking a detainee for a specific transportation route for a specific day.
Service	An application component of a Service-Oriented Architecture.
Special Enforcement Operation	A coordinated or pre-planned event targeting a group of people (e.g., work-site operations).
Special Enforcement Operation Status	Value denoting the progress of a coordinated pre-planned event.
Services-Oriented Architecture	A service-oriented architecture is a collection of services that communicate with each other. The services are self-contained and do not depend on the context or state of the other service. They work within a distributed systems architecture.
Stipulated Release	Apprehended alien qualifies to see an immigration judge but foregoes his or her right to a hearing in order to be removed from the country faster.
Subject Information	Information pertaining to who is subject to any of DRO's internal or external processes.
Temp-outs	Term used to describe trips where detainees have been booked out of a facility for a short period of time and are expected to return to the same location. (e.g. court appearance, hospital visit, consular visit)
Ten-print	A 14-block fingerprint record consisting of ten rolled images and four flat images (one for each thumb, one for each four-finger group).
Third Party Agency Check	Identifies special interest aliens that enter ICE custody for clearance processing to ensure they are not subject to national security interest or pending criminal-related investigations by ICE or other outside agencies prior to being released from ICE custody or removed from the United States.

Term	Definition
Transfer Information	A history of the locations where an alien has been detained over a period of time, or the “A” Files, destination, date, time, and mode of transportation of one or more aliens scheduled for transfer.
Transportation Information	A history of the locations where a vehicle has been over a period of time and its list of pickup and drop-off passengers at each stop, as well as dispatch information.
Transport mechanism	The method by which data is transferred between systems.
Travel Document (TD)	Document that is issued by a consulate of a detainee’s home country and used to deport a removal subject.
Travel Document Certification	Act by the consulate certifying the travel document through an electronic signature.
Travel Document Package	Package that is prepared by DRO to be sent to a consulate for approval. This package contains the following artifacts: charging document, <i>Information for Travel Document or Passport</i> (Form I-217), removal order, other supporting documents, and the travel document.
Travel Document Request	The act by DRO of sending a travel document package to the consulate for approval.
Travel Information	Information including the mode of transport, transport documents, travel request, itinerary, country clearance, mission approval, manifest, tickets, escorts, and identification of special needs for removal subjects.
Trip	A single transportation transaction.
True Accept Rate (TAR)	In relation to Tracking: The percentage of time that a biometric system correctly produces a true claim of identity. TAR is a metric used to measure biometric performance when verifying identity.
Unfunded Beds (DRO)	Bed space that is financially supported by outside organizations (e.g. BOP, ORR).
Unified Modeling Language	An Object Management Group (OMG) standard for modeling software artifacts. Using UML, developers and architects can make a blueprint of a project, much like ERD diagrams are used for relational design.
Universal Identifier	A value associated to one detainee uniquely identifying that detainee (e.g. A#, FINS #).
URL Address	An address or location of a resource on the internet (e.g., http://www.dhs.gov/)
Vertical Integration	In a layered solution architectural model,

Term	Definition
Voluntary Departure	A type of discretionary judicial relief that enables an alien to leave the country at his/her own expense within a time limit specified by the judge.
Wait-List	In relation to CRS: To place on a waiting list for a given bed type in a facility.
Web Services	Open standard (XML, SOAP, etc.) based Web applications that interact with other web applications for the purpose of exchanging data. Initially used for the exchange of data on large private enterprise networks, web services are evolving to include transactions over the public Internet.
Wheels-up	Wheels-up refers to the physical act of when the JPATS flight is airborne and the wheels have retracted. This may represent the point of removal for a detainee.
Wireless Access Protocol	A secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smart phones and communicators.
Workflow	The movement of a process around an organization based upon a set of relationships between activities.

Released Systems Glossary

Acronym	Definition
AFIS	Automated Fingerprint Identification System
ANSIR	Automated Nationwide System for Immigration Review
APSS	Automated Prisoner Scheduling System (U.S. Marshals Service)
ATMS	Alien Transportation Management System
BMIS	Bond Management Information System
CAIS	Criminal Alien Information System
CASE	Case Access System for EOIR
CLAIMS	Computer-Linked Application Information Management System
CLASS	Consular Lookout and Support System (CLASS)
CRS	Central Reservation System
DACS	Deportable Alien Control System
DDOS	Detention and Deportation Optimization System
DEPORT	Detention Enforcement and Processing Offenders by Remote

Acronym	Definition
	Technology
DETS	Detection Section of DACS
DLT	Detainee Location tracking
DOC	State Department of Corrections Database
DRIMS	Detention and Removal Information Management System
DMTS	Detention Management Tracking System
EABM	Enforcement Apprehension and Booking Module
EADM	Enforcement Alien Detention Module
EARM	Enforcement Alien Removal Module
EFTS	<i>Electronic Fingerprint Transmission Specification</i> – FBI document number CJIS-RS-0010 (V7), January 29, 1999. Describes the FBI's implementation of the national standard. This standard specifies a common format to be used to exchange fingerprint, facial, scar, mark, and tattoo identification data, including biographic and demographic data about subjects across jurisdictional lines or between dissimilar systems made by different manufacturers.
EGov Environment	A protected environment to host sensitive data so that users outside of DHS (i.e. consular users) can access them. Data put in this environment is strictly enforced through an intranet application. Only users authorized by the application will be able to access the application.
EGov ETD Database	Database that is hosted on the eGov environment. Once a removal subject is identified in EID, the data is transferred into this database at which point, either system, intranet and eGov applications, can access and update the data. Inserting a new travel document request can only done by the DRO user through the intranet application.
FCMS	Fugitive Case Management System
FFMS	Federal Financial Management System
FINS	Fingerprint Identification Number System
GEMS	General Counsel Management System
IAFIS	Integrated Automated Fingerprint Identification System
IBIS	Interagency Border Inspection System
IDENT	Automated Biometric Identification System
JPATS	Justice Prisoner and Alien Transportation System
LEADS	Law Enforcement Analytical Data System
NFTS	National File Tracking System

Acronym	Definition
NICS	National Instant Criminal Background Check System
TECS	Treasury Enforcement Communications System
TMS	Transportation Management System

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE	PAGE OF PAGES 1 5
2. AMENDMENT/MODIFICATION NO. P00001	3. EFFECTIVE DATE 11/06/2008	4. REQUISITION/PURCHASE REQ. NO. 192109CIOSDD2DC02	5. PROJECT NO. (If applicable)
6. ISSUED BY ICE/TC/IT SERVIC	CODE ICE/TC/IT SERVIC	7. ADMINISTERED BY (If other than Item 6) ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW Washington DC 20536	CODE ICE/TC/IT SERVIC
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC 7575 COLSHIRE DRIVE MCLEAN VA 221027508		(x) 9A. AMENDMENT OF SOLICITATION NO.	9B. DATED (SEE ITEM 11)
CODE 0646810210000	FACILITY CODE	X 10A. MODIFICATION OF CONTRACT/ORDER NO. HSHQDC-06-D-00022 HSCETC-09-J-00002	10B. DATED (SEE ITEM 11) 11/04/2008

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers is extended, is not extended.
Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)
See Schedule

13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
X	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor is not, is required to sign this document and return _____ 0 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

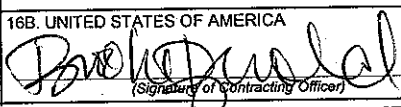
DUNS Number: 064681021
Due to system errors, this modification corrects the accounting information for CLINS 0001 through 0002C.

All other terms and conditions remain unchanged.

FOB: Destination
Period of Performance: 01/04/2009 to 01/03/2013

Continued ...

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Brooke Bernold
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED
16B. UNITED STATES OF AMERICA  (Signature of Contracting Officer)	16C. DATE SIGNED 11/7/08

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00022/HSCETC-09-J-00002/P00001

PAGE OF
 2 5

NAME OF OFFEROR OR CONTRACTOR
 NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001	<p>Change Item 0001 to read as follows (amount shown is the obligated amount):</p> <p>Detainee Location Tracking System: Labor Annual Cost: [REDACTED] b4 Fixed Fee: [REDACTED] Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: [REDACTED] b2Low Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4	
0001A	<p>Change Item 0001A to read as follows (amount shown is the obligated amount):</p> <p>Detainee Location Tracking System: Hardware/Software Annual Cost: [REDACTED] b4 Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount: [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: [REDACTED] b2Low Funded: [REDACTED] b4</p>	1	LO	[REDACTED] b4	
0001B	<p>Change Item 0001B to read as follows (amount shown is the obligated amount):</p> <p>Detainee Location Tracking System: Materials</p> <p>Annual Cost: [REDACTED] b4 Fixed Fee: [REDACTED] b4 Total Cost-Plus-Fixed-Fee: [REDACTED] b4 Continued ...</p>	1	LO	[REDACTED] b4	

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00022/HSCETC-09-J-00002/P00001

PAGE OF
 3 5

NAME OF OFFEROR OR CONTRACTOR
 NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0001C	<p>Incrementally Funded Amount: [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: [REDACTED] b2Low</p> <p>Funded: [REDACTED] b4</p> <p>Change Item 0001C to read as follows (amount shown is the obligated amount):</p> <p>Detainee Location Tracking System: Travel/Other Direct Costs (ODCs) Annual Cost: [REDACTED] b4</p> <p>Fixed Fee: [REDACTED] b4 Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount: [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: [REDACTED] b2Low</p> <p>Funded: [REDACTED] b4</p> <p>Change Item 0002 to read as follows (amount shown is the obligated amount):</p>	1	LO	[REDACTED] b4	[REDACTED]
0002	<p>Central Reservation System: Labor Annual Cost [REDACTED] b4 Fixed Fee: [REDACTED] b4 Cost-Plus-Fixed-Fee: [REDACTED] b4 Incrementally Funded Amount: [REDACTED] b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: Continued ...</p>	1	LO	[REDACTED] b4	[REDACTED]

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
 HSHQDC-06-D-00022/HSCETC-09-J-00002/P00001

PAGE 4 OF 5

NAME OF OFFEROR OR CONTRACTOR
 NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC.

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0002A	<p>b2Low</p> <p>Funded: b4</p> <p>Change Item 0002A to read as follows (amount shown is the obligated amount):</p> <p>Central Reservation System: Hardware/Software Annual Cost: b4 Fixed Fee: b4 Total Cost-Plus-Fixed-Fee: b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: b4 Accounting Info:</p> <p>b2Low</p> <p>Funded: b4</p>	1	LO	b4	0.00
0002B	<p>Change Item 0002B to read as follows (amount shown is the obligated amount):</p> <p>Central Reservation System: Materials Annual Cost: b4 Fixed Fee: b4 Total Cost-Plus-Fixed-Fee: b4 Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: b4 Accounting Info:</p> <p>b2Low</p> <p>Funded: b4</p>	1	LO	b4	0.00
0002C	<p>Change Item 0002C to read as follows (amount shown is the obligated amount):</p> <p>Central Reservation System: Travel/ODCs Annual Cost: b4 Fixed Fee: b4 Total Cost-Plus-Fixed-Fee: b4 Incrementally Funded Amount: b4 Continued ...</p>	1	LO	b4	

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSHQDC-06-D-00022/HSCETC-09-J-00002/P00001

PAGE OF
5 5

NAME OF OFFEROR OR CONTRACTOR
NORTHROP GRUMMAN INFORMATION TECHNOLOGY INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES</p> <p>Accounting Info: SEE ATTACHMENT A Funded: [REDACTED] b4 Accounting Info: [REDACTED] b2Low Funded: [REDACTED] b4</p>				

Form G-514

REQUISITION - MATERIALS-SUPPLIES-EQUIPMENT

Activity Symbols ATTACHMENT A

REQUISITION NUMBER: 192109C IOSDD2DC02

PROJECT	TASK	FUND PROGRAM	ORGANIZATION	OBJECT	UDF	AMOUNT
b2Low						\$12,209,426.00

APPROPRIATION SYMBOL CROSSWALK:

FUND	FY	TAS	TITLE	AMOUNT
AM	2009	70X0543	Automation Modernization, Immigration and Customs Enforcement, Border and Transportation Security, Department of Homeland Security	12,209,426.00

ATTACHMENT A

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

DRO Background



Office of Detention and Removal Operations

DRO

Briefing Book



U.S. Immigration
and Customs
Enforcement

I. Executive Summary

Mission Statements	I.1
U.S. Department of Homeland Security	I.1
U.S. Immigration and Customs Enforcement	I.1
Office of Detention and Removal Operations	I.1
Overview: U.S. Immigration and Customs Enforcement (ICE)	I.3
ICE Organization Chart	I.3
Overview: Office of Detention and Removal Operations (DRO)	I.4
DRO Headquarters Management and Reporting Structure	I.4
Facts and Figures	I.5
Budget	I.6
Key Initiatives	I.7
Secure Border Initiative	I.7
Criminal Alien Program	I.7
Fugitive Operation Teams	I.7
Centralized Ticketing System	I.8
Alternatives to Detention	I.8
Juvenile Program	I.8

II. Criminal Alien Division

Executive Summary: Criminal Alien Division	II.1
Mission	II.1
Criminal Alien Program Unit	II.1
Intelligence Operations Unit	II.1

III. Compliance Enforcement Division

Executive Summary: Compliance Enforcement Division	III.1
Mission	III.1
Fugitive Operations Unit	III.1
Alternatives to Detention Unit	III.1
Bond Management Unit	III.2
Fugitive Ops Deployment Map	III.2

IV. Detention Management Division

Executive Summary: Detention Management Division	IV.1
Mission	IV.1
Detention Acquisition Support Unit	IV.1
Detention Management and Planning Unit	IV.1
Detention Standards Compliance Unit	IV.2
Incident Response Unit	IV.2
Detention Health Care	IV.2
Juvenile Liaison	IV.3
DRO Operational Areas of Responsibility	IV.3
Service Processing Centers	IV.4
Contract Detention Facilities	IV.4

V. Removal Management Division

Executive Summary: Removal Management Division	V.1
Mission	V.1
Air Transportation Unit	V.1
Travel Document Unit	V.1
Custody Determination Unit	V.2
Centralized Ticketing Unit	V.2
Department of State Liaison	V.2
SBI Operations	V.2

VI. Mission Support Division

Executive Summary: Mission Support Division	VI.1
Mission	VI.1
Program Analysis and IT Unit	VI.1
Financial Management Unit	VI.1
Logistics and Fleet Management Unit	VI.1
Human Capital and Training Unit	VI.2
Planning and Performance Measurement	VI.2

VII. Appendices

Authorities	VII.1
Glossary	VII.2
Acronyms	VII.6

Executive Summary

A close-up, slightly blurred image of the American flag, showing the stars and stripes. The flag is positioned on the left side of the page, with the stars in the upper left and the stripes extending towards the right. The colors are vibrant, with a deep blue, bright red, and clean white.

U.S. Department of Homeland Security

Preserving our freedoms, protecting America...we secure our homeland. We will lead the unified national effort to secure America. We will prevent and deter terrorist attacks and protect against and respond to threats and hazards to the nation. We will ensure safe and secure borders, welcome lawful immigrants and visitors and promote the free-flow of commerce.

U.S. Immigration and Customs Enforcement (ICE)

As the largest investigative arm of the U.S. Department Homeland Security, ICE brings a unified and coordinated focus to the enforcement and investigation of homeland security crimes, including federal immigration law and custom laws. ICE brings to bear all of the considerable resources and authorities invested in it to fulfill its primary mission: to detect vulnerabilities and prevent violations that threaten national security.

ICE works to protect the United States and its people by deterring, interdicting and investigating threats arising from the movement of people and goods into and out of the United States; and by policing and securing federal government facilities across the nation.

Office of Detention and Removal Operations (DRO)

Promoting the public safety and national security by ensuring the departure from the United States of all removable aliens through the fair and effective enforcement of the nations immigration laws.

Overview: U.S. Immigration and Customs Enforcement

Established in March 2003, U.S. Immigration and Customs Enforcement (ICE) is the largest investigative arm of the Department of Homeland Security (DHS). ICE is comprised of four integrated operational divisions that form a 21st century law enforcement agency with broad responsibilities to accomplish key homeland security priorities. These divisions are the Office of Detention and Removal Operations, the Office of Investigations, the Federal Protective Service and the Office of Intelligence.

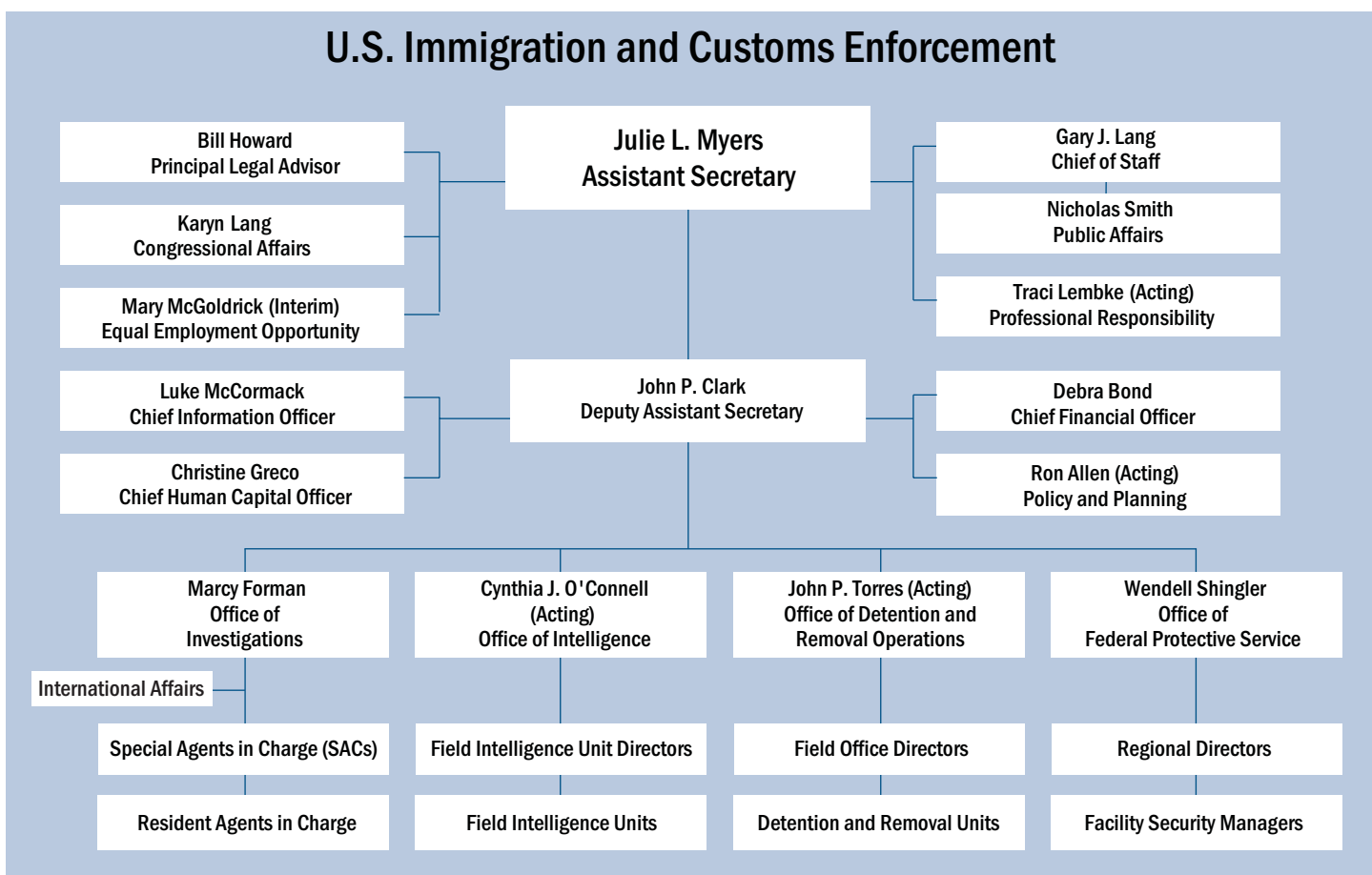
ICE derives its law enforcement authorities from the former U.S. Customs Service, U.S. Immigration and Naturalization Service and the Federal Protective Service. The combination of these law enforcement authorities expands ICE's jurisdiction and facilitates its unique ability to combat terrorists and other criminal organizations.

The ICE mission is derived from the statute that created the DHS: "...to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism." ICE adds to this mission



its responsibility to "ensure that the functions of the agencies and subdivisions within the Organization that are not related directly to securing the homeland are not diminished or neglected."

Approximately 15,000 Federal law enforcement officers and civil servants make up the ICE staff and are located at a multitude of domestic and international offices as well as its headquarters in Washington, DC.



Overview: Detention and Removal Operations

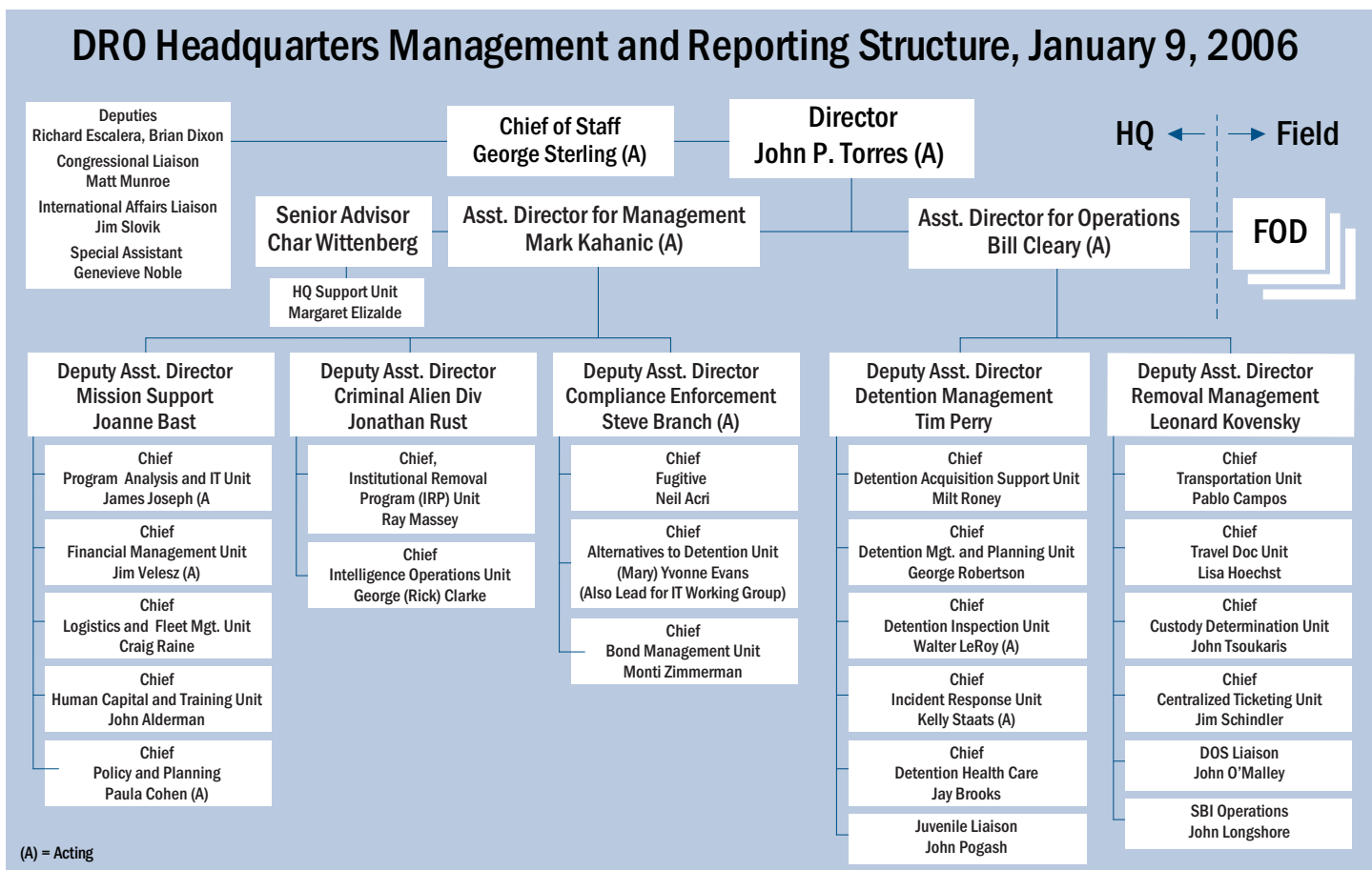
The Office of Detention and Removal Operations (DRO) is one of five divisions of the U.S. Immigration and Customs Enforcement (ICE). DRO's workforce consists of approximately 5,500 authorized employees, including over 4,200 law enforcement officers and 1,200 support personnel.

Through the fair enforcement of the nation's immigration laws, DRO promotes public safety and national security by ensuring the departure of all removable aliens from the United States. DRO employs its resources and expertise to locate and arrest fugitive aliens; to detain certain aliens while their cases are being processed; and to remove them from the United States when so ordered. As such, the goal of DRO is to develop the capacity to remove all removable aliens.

DRO is responsible for the operation of secure detention facilities called Service Processing Centers. The Service Processing Centers are located in Aguadilla, Puerto Rico; Batavia, New York; El Centro,

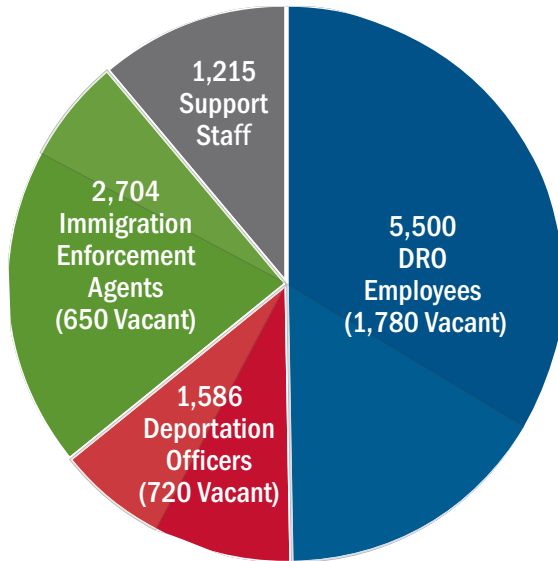
California; El Paso, Texas; Florence, Arizona; Miami, Florida; Los Fresnos, Texas; and San Pedro, California. Service Processing Centers are augmented with eight Contract Detention Facilities. The Contract Detention Facilities are located in Aurora, Colorado; Houston, Texas; Laredo, Texas; Seattle, Washington; Elizabeth, New Jersey; Queens, New York; and San Diego, California. DRO utilizes state and local jails on a reimbursable detention day basis and has joint federal facilities with the Bureau of Prisons, the Federal Detention Center in Oakdale, Louisiana, and the contractor owned and operated Criminal Alien Facility in Eloy, Arizona.

DRO is comprised of five specialized divisions at the headquarters level that support the ICE detention and removal mission. They are the Criminal Alien Division, the Compliance Enforcement Division, the Detention Management Division, the Removal Management Division and the Mission Support Division.



Facts and Figures

- Currently authorized 5,500 DRO employees (1,780 Vacant).
- Currently authorized 1,586 Deportation Officers (720 Vacant).
- Currently authorized 2,704 Immigration Enforcement Agents (650 Vacant).
- Currently authorized 1,215 support staff (408 vacant).

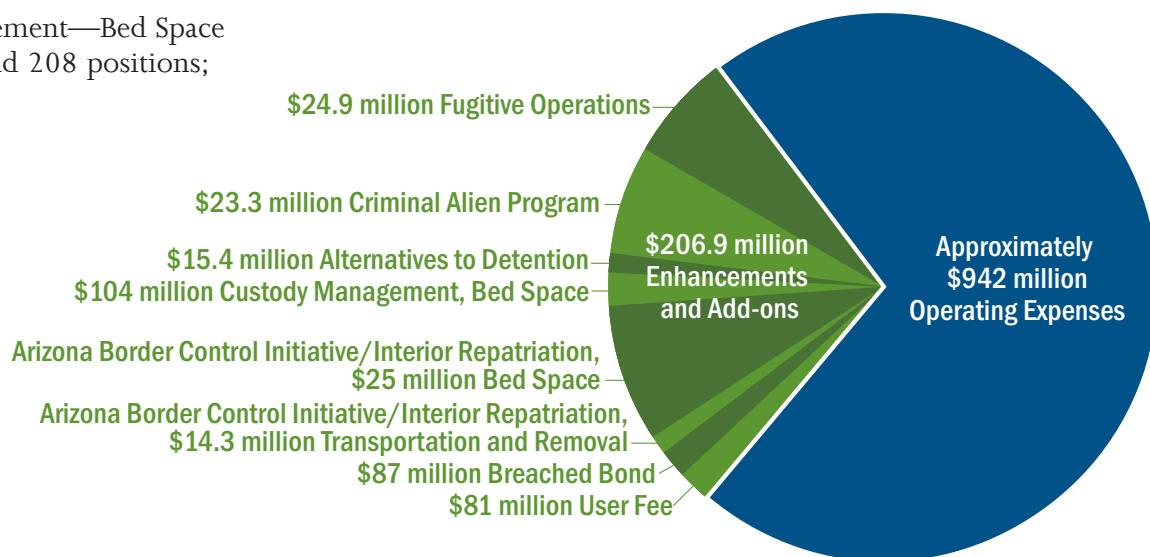


- More than 132,000 removals in Fiscal Year 2005, including over 78,000 criminals.
- On average, more than 20,000 aliens in ICE custody on any given day.
- More than 217,000 aliens admitted to detention during Fiscal Year 2005.
- More than 1.2 million active immigration cases being managed by the Deportation Officer staff.
- In Fiscal Year 2005, Fugitive Operations Teams made 15,208 apprehensions of which 11,198 were fugitive aliens.
- Since the creation of the Fugitive Operation Program (March 2003), approximately 37,193 aliens have been apprehended by Fugitive Operation Teams, of which 28,442 were fugitive aliens.

2006 Budget

\$1.4 billion total (all accounts):

- approximately \$942 million in operating expenses; and
- \$206.9 million enhancements and add-ons:
 - Fugitive Operations
\$24.9 million and 60 positions;
 - Criminal Alien Program
\$23.3 million and 137 positions;
 - Alternatives to Detention
\$15.4 million and 62 positions;
 - Custody Management—Bed Space
\$104 million and 208 positions;
 - Arizona Border Control Initiative/Interior Repatriation—Bed Space
\$25 million;
 - Arizona Border Control Initiative/Interior Repatriation—Transportation and Removal
\$14.3 million;
 - Breached Bond—authority reduction of
\$87 million; and
 - User Fee—authority \$81 million.



Key Initiatives

Secure Border Initiative

The Secure Border Initiative (SBI) is a comprehensive multi-year plan to secure America's borders and reduce illegal migration, which includes:

More agents to patrol our borders, secure our ports of entry and enforce immigration laws;

- Expanded detention and removal capabilities to eliminate “catch and release” once and for all;
- A comprehensive and systemic upgrading of the technology used in controlling the border, including increased manned aerial assets, expanded use of Unmanned Aerial Vehicles and next-generation detection technology;
- Increased investment in infrastructure improvements at the border—providing additional physical security to sharply reduce illegal border crossings; and
- Greatly increased interior enforcement of our immigration laws—including more robust work-site enforcement.

The Office of Detention and Removal Operations (DRO) is supporting the SBI by providing personnel who work with the DHS, ICE and other components of DRO to further the end of “catch and release” by the end of Fiscal Year 2006. Primarily, the DRO SBI Unit is identifying initiatives and new business processes to reduce the “cycle” time required to remove aliens from the United States.

Criminal Alien Program

The Criminal Alien Program Unit (CAP) focuses on identifying criminal aliens who are incarcerated within federal, state and local facilities thereby ensuring that they are not released into the community by securing a final order of removal prior to the termination of their sentence.

The Office of Investigations (OI) is working with the Office of Detention and Removal Operations (DRO) to transition responsibility of the Institutional Removal Program (IRP) and the Alien Criminal Apprehension Programs (ACAP) to DRO. By moving these programs to DRO, ICE will use less costly Immigration Enforcement Agents (IEA) to replace ICE Special Agents (SA) currently perform-

ing criminal alien duties, thus allowing Special Agents to do more complex investigative work.

The transition of the Institutional Removal Program and Alien Criminal Apprehension Program from OI to DRO has already occurred in a few select offices. DRO has consolidated these two related programs into one, titled the Criminal Alien Program (CAP). As of October 2005, 11 DRO field offices have transitioned employees to assume the responsibility of the CAP from OI.

Fugitive Operation Teams

DRO Fugitive Operation Teams have been created to identify, locate, apprehend and remove fugitive aliens from the United States. The highest priority of Fugitive Operation Teams is to locate those fugitives who pose a threat to national security and community safety. Additionally, the Fugitive Operation Teams are eliminating the backlog of alien fugitives and ensuring that the number of aliens removed from the United States equals the number of final orders of removal or grants of voluntary departure issued by the immigration courts in any given year.

To date, 52 DRO Fugitive Operation Teams have been funded and are being deployed at ICE field offices throughout the United States. In Fiscal Year 2005, Fugitive Operation Teams apprehended



11,198 fugitives, of whom 4,699 were criminal aliens. Additionally, the Fugitive Operation Teams made 2,361 apprehensions of collateral criminal aliens.

Centralized Ticketing System

The mission of the Centralized Ticketing Unit (CTU) is to manage the DRO Centralized Ticketing Program (CENTIX). The CTU functions as the coordinator for airline ticketing and country clearance support for DRO Headquarter and DRO field offices in support of the removal process. The CTU coordinates with the DRO field offices, external agencies and the travel and airline industry relating to removal requirements and recommends removal process efficiencies relating to commercial transportation. The CTU also provides related mission support to the Removal Management Division in the areas of process documentation, commercial transportation, financial management and IT/Web site support. The CTU is continuing to hire additional contract program support in the following areas: financial, analytical and information technology. The CTU will utilize these new personnel in order to enhance removal capabilities

The key program initiatives currently in progress include: the configuration of the new DHS e-Travel System (EDS Fed Traveler) to support removal operations by replacing the e-mail based system with an online system and the configuration and deployment of the Flyte Comm system to provide situational awareness of removal operations and improve our business process.

Alternatives to Detention

The Alternatives to Detention Unit (ATD) is responsible for developing and implementing programs that enhance the supervision of aliens released from ICE custody. There are two ATD programs currently used by the DRO, the Electronic Monitoring Program (EMP) and the Intense Supervision Appearance Program (ISAP).

The EMP was initially created and implemented with the goal of providing a cost effective alternative to detention and was piloted in seven field offices. DRO has since expanded the EMP nationwide.

The EMP currently utilizes the following technologies for monitoring detainees:

- telephonic reporting with voice verification;
- radio frequency with ankle bracelets; and
- global position satellite.

The ISAP is designed to supervise aliens released from custody and to ensure compliance with conditions of release, immigration hearings and immigration judge orders.

The ISAP employs case specialists to closely supervise participating aliens utilizing a variety of tools such as curfews, electronic monitoring devices and community collaborations that support the participant.

Juvenile Program

The overall mission of the Juvenile Operations Unit (JOU) is to treat juveniles who are in the custody of the DRO with respect, dignity and special concern for their particular vulnerability. In order to do this, the JOU strives to place juveniles in the appropriate facilities, ensure that their safety is maintained and provide them with the appropriate educational services. Additionally, the JOU provides the appropriate mental health and medical services to juveniles if required.

The JOU is currently working with other DRO components to address issues regarding families in federal custody as related to the SBI initiative. In addition, the JOU continues to work on operational issues with the Department of Health and Human Services and Office of Refugee Resettlement (ORR). In March of 2003, responsibilities related to the care and custody of unaccompanied alien juveniles was transferred to ORR.



Criminal
Alien
Division

Executive Summary: Criminal Alien Division

Mission

The mission of the Criminal Alien Division is to identify, exploit intelligence information and process criminal aliens incarcerated in federal, state and local correctional institutions and jails who have no legal right to remain in the United States after completing their sentence.

Criminal Alien Program Unit

The Criminal Alien Program Unit (CAP)—formerly the Institutional Removal Program—focuses on identifying criminal aliens who are incarcerated within federal, state and local facilities thereby ensuring that they are not released into the community by securing a final order of removal prior to the termination of their sentence. The identification and processing of incarcerated criminal aliens prior to release reduces the overall cost and burden to the Federal Government as the number of aliens detained by U.S. Immigration and Customs Enforcement (ICE), upon expiration of sentence will be minimized.

Historical evidence shows that the CAP is an effective approach for the prevention of criminal recidivism, which ensures that aliens are removed after a removal order is attained. The workload for each ICE officer is approximately 600 charging documents per year. This figure encompasses the number of interviews and record checks of individuals that are not amenable to removal, but are of foreign birth.

The Office of Investigations (OI) is working with the Office of Detention and Removal Operations (DRO) to transition the responsibility for the Institutional Removal Program (IRP) and the Alien Criminal Apprehension Programs (ACAP) to DRO. By moving these programs to DRO, ICE will use less costly Immigration Enforcement Agents (IEA) to replace ICE Special Agents (SA) currently performing criminal alien duties, thus allowing Special Agents to do more complex investigative work.

The transition of the Institutional Removal Program and Alien Criminal Apprehension Program from OI to DRO has already occurred in a few select offices. DRO has consolidated these two related programs into one, titled the Criminal Alien Program (CAP).



As of October 2005, 11 DRO field offices have transitioned employees to assume the responsibility of the CAP from OI. This transition effort is limited to primarily federal detention facilities of the Institutional Removal Program. Once the Criminal Alien Program is fully transitioned, all incarcerated criminal aliens will be the primary responsibility of DRO.

Intelligence Operations Unit

The Intelligence Operations Unit (IOU) manages the collection and dissemination of law enforcement information and intelligence within the DRO Program. The IOU ensures that all intelligence, developed or received, is evaluated and disseminated to the appropriate ICE operational entity as it pertains to homeland security, infrastructure protection and the illegal movement of people, money and cargo entering, transiting or operating within our national borders.

One of the most important ICE mandates is the enhancement of public safety and the security of the American public. The broad authority of ICE allows for the identification and removal of dangerous, often recidivist, criminals engaged in crimes such as murder, predatory sexual offenses, narcotics trafficking, alien smuggling and a host of other crimes that have a profoundly negative impact on our society.

A largely untapped source of information resides in the ICE detainee population. The IOU seeks to dedicate personnel to gather information in detention facilities, organize information and provide information locally to avert possible detention riots or other illegal activities within the ICE detainee population.

The information obtained from ICE detainees will be utilized to protect and maintain the security of the detention facilities and detainees, provide real time information on particular terrorist threats or organized criminal activities and provide an untapped source of intelligence that will benefit ICE as a whole.

Additionally, the IOU will work in conjunction with other DHS entities to coordinate border security intelligence in achieving the recommendations of the Secure Border Initiative (SBI).



Compliance Enforcement Division

Executive Summary: Compliance Enforcement Division

Mission

The mission of the Compliance Enforcement Division (CED) is to formulate policy and provide oversight to the Fugitive Operations program, the Alternatives to Detention program and the Bond Management operation. The CED also develops and implements strategies to ensure the compliance of aliens with conditions of release during the removal process.

Fugitive Operations Unit

The Fugitive Operations Unit (FOU) is an integral part of the Compliance Enforcement Division in that its mission is to oversee the National Fugitive Operations Program (NFOP), which has been created to identify, locate, apprehend and remove fugitive aliens from the United States. The highest priority of the NFOP is placed on those fugitives who pose a threat to national security and community safety.

The primary goal of the FOU is to eliminate the backlog of alien fugitives and ensure that the number of aliens removed from the United States equals the number of final orders of removal or grants of voluntary departure issued by the immigration courts in any given year.

The FOU is responsible for developing and implementing a strategic plan, both budgetary and operational, in the deployment of resources to the ICE Office of Detention and Removal Operations (DRO) field offices throughout the United States. To date,



52 fugitive operations teams have been funded and are being deployed at ICE field offices throughout the United States. In FY 2005, Fugitive Operation Teams apprehended 11,198 fugitives, of whom 4,699 were criminal aliens. Additionally, the Fugitive Operation Teams made 2,361 apprehensions of collateral criminal aliens.

Strategies developed and being monitored by the FOU include:

- participation of Fugitive Operations Teams on various federal, state and local task forces;
- prioritizing the entry of fugitive cases into the National Crime Information Center (NCIC), the Ten Most Wanted Operation and coordination with Interpol;
- exploring the availability and effectiveness in contracting with vendors who can provide services leading to the location of fugitives; and
- working closely with the U.S. Citizenship and Immigration Services (CIS), Bureau of Prisons (BOP) and other agencies to identify and apprehend fugitives.

Alternatives to Detention Unit

The Alternatives to Detention Unit (ATD) is responsible for developing and implementing programs that enhance the supervision of aliens released from ICE custody. There are two ATD programs currently used by the DRO, the Electronic Monitoring Program (EMP) and the Intense Supervision Appearance Program (ISAP).

The EMP was initially created and implemented with the goal of providing a cost effective alternative to detention and was piloted in seven field offices. DRO has since expanded the EMP nationwide.

The EMP currently utilizes the following technologies for monitoring detainees:

- telephonic reporting with voice verification;
- radio frequency with ankle bracelets; and
- global position satellite.

The ISAP is designed to supervise aliens released from custody and to ensure compliance with conditions of release, immigration hearings and immigration judge orders.

The ISAP employs case specialists to closely supervise participating aliens utilizing a variety of tools such as curfews, electronic monitoring devices and community collaborations that support the participant.

Bond Management Unit

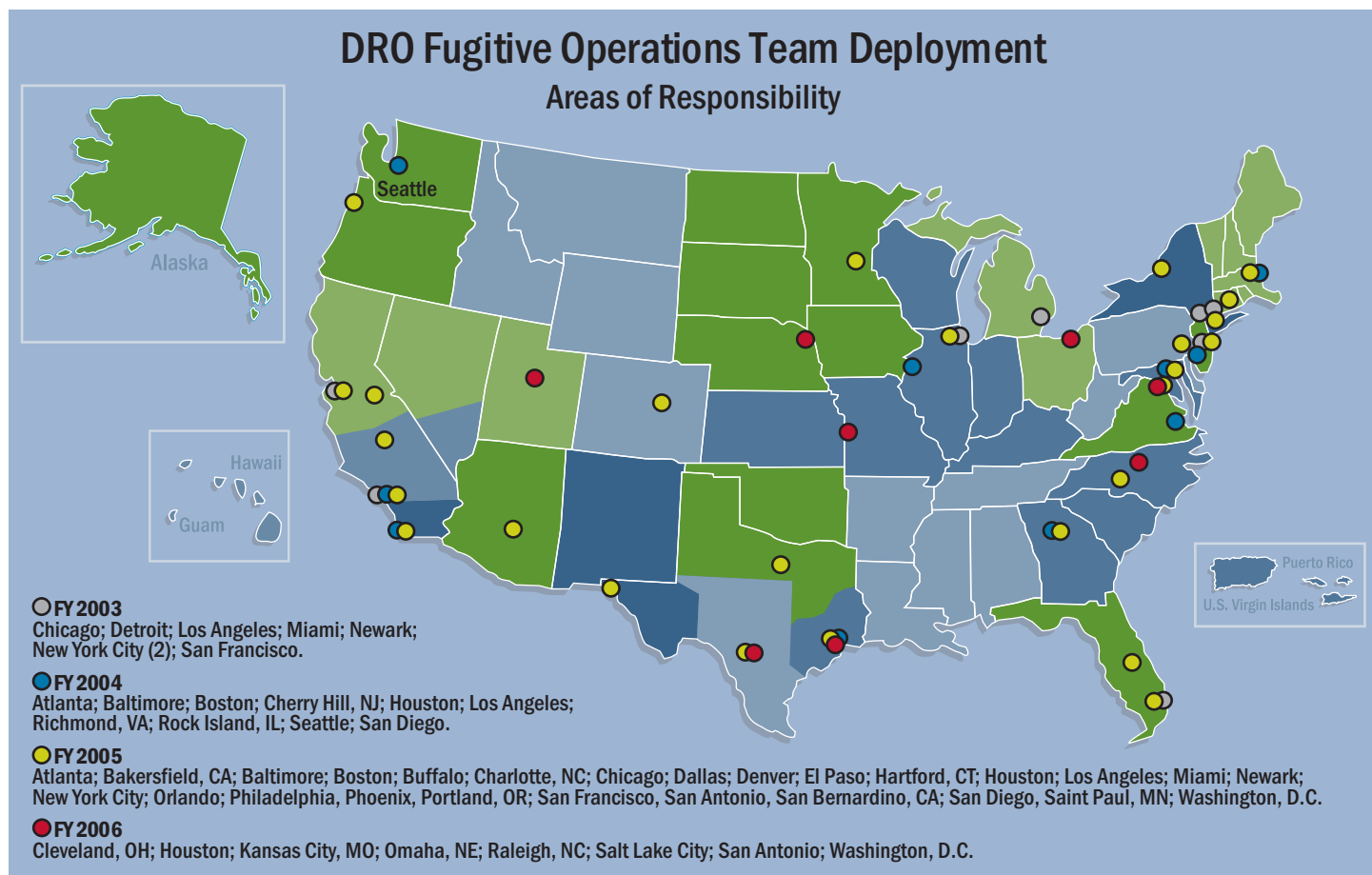
The Bond Management Unit (BMU) is responsible for developing and implementing a uniform bond policy. The BMU provides oversight to field offices and ensures that bond related issues are addressed and resolved in a timely manner. The BMU maintains liaison with the Debt Management Center (DMC), U.S. Department of Justice (DOJ) Attorneys and the Administrative Appeals Office (AAO), regarding bond related and litigation issues.

The BMU is constantly evaluating bond procedures and is currently working on an initiative that would allow the DRO field offices the ability to deposit bonds. Currently, CIS is performing this function for DRO. There are approximately 75,780 open bonds on aliens totaling \$348,255,083.



There are seven major surety companies that the DHS and DOJ are in litigation with, due to the surety companies' failure to turn over the individuals under bond, or to forfeit the bond money. DRO is working with the Department of Treasury to decertify any surety company that is not following their legal obligations as agreed upon with DHS and ICE.

DRO is also preparing the Bond Management Specialist program to ensure that bond management is properly focused nationwide.



Detention
Management
Division

Executive Summary: Detention Management Division

Mission

The endgame of immigration enforcement is the removal of illegal aliens from the

United States. Funding for detention capacity and staff to manage the adjudication and removal processes are absolutely essential to accomplish this ultimate goal.

Due to the nature of its mission, the immigration detention program maintains custody of one of the most highly transient and diverse populations of any correctional or detention system in the world. This administrative custody environment presents significant management challenges compared to the typical static prison environment. These challenges are compounded by the diverse population (individuals representing virtually every country of the world; every security classification; males, females, families of every age group; medical conditions ranging from healthy to terminally ill, etc.) in immigration detention custody every day.

The current ICE detention system consists of over 400 local and state facilities acquired through intergovernmental service agreements (IGSA); eight contract detention facilities; eight ICE-owned facilities and five Bureau of Prisons (BOP) facilities, which are either funded directly through congressional appropriations to BOP or through ICE reimbursement.

Approximately 52 percent of the ICE population is designated to IGSA, 19 percent in contract facilities, 18 percent in ICE-owned facilities and 11 percent in BOP facilities. Currently, the ICE detention program has a funded capacity of approximately 20,375 beds.

Detention Acquisition Support Unit

The Detention Acquisition Support Unit (DAS) is responsible for planning, management and acquisition of a full range of detention acquisition services, including full service contract detention facilities and services, which support detention operations.

The DAS coordinates and manages detention contracting policies and initiatives and oversees all detention related contracts. In acquiring these serv-

ices, the DAS works through the ICE Office of Procurement and the Department of Justice (DOJ), Office of the Federal Detention Trustee.

The DAS is responsible for facilities planning, capital construction and repair and alterations of all ICE owned facilities within the Office of Detention and Removal (DRO). Furthermore, the DAS manages detention design programs, technical standards and the planning of ICE owned detention facilities nationwide.

Detention Management and Planning Unit

The Detention Management and Planning Unit (DMP) oversee national detention operations and plans along the enforcement continuum for current and future detention capacity. DRO utilizes Service Processing Centers (government owned/government operated facilities), Contract Detention Facilities, Intergovernmental Service Agreements with local agencies and, on a limited basis, Bureau of Prison detention capacity to service our detention requirements.

Future detention planning involves acquiring sufficient capacity to support the interior enforcement wedge of the Secure Border Initiative (SBI) and the expansion of the operational control of the south-



west border wedge of SBI. Furthermore, the DMP is planning to sufficiently support the DRO Criminal Alien Program (CAP) and Fugitive Operations Program (FOP).

Detention Standards Compliance Unit

The Detention Standards Compliance Unit (DSC), through an aggressive inspections program, ensures facilities utilized by ICE to detain aliens in immigration proceedings do so in accordance with ICE National Detention Standards. The DSC provides ICE and the public the assurance that detainees in ICE custody, the vast majority of which are criminal aliens, are detained in safe and secure environments and under appropriate conditions of confinement.

The ICE National Detention Standards, promulgated in November 2000, are the result of negotiations between the American Bar Association (ABA), the U.S. Department of Justice (DOJ), the legacy Immigration and Naturalization Service (INS), and other organizations involved in pro bono representation and advocacy for immigration detainees. The 38 standards are comprehensive, encompassing areas from legal access to religious and medical services and marriage requests. The legal access standards concern visitation, access to legal materials, telephone access and group presentations on legal rights.



The standards further the goals of ICE to provide safe, secure and humane conditions for all detainees in ICE custody. ICE is committed to ensuring that our detention standards are met by all facilities utilized for detention.

The Detention Standards Compliance Unit conducts over 350 annual inspections of authorized detention facilities to measure compliance with the ICE National Detention Standards.

Incident Response Unit

The Incident Response Unit (IRU) facilitates DRO's rapid response to, and the management of, crisis incidents. Formed in 2004, the IRU assists the DRO Field Offices in precrisis planning and during responses to critical incidents.

The IRU has recently developed the Emergency Preparedness Manual that is utilized to aid the field in developing crisis response plans for Service Processing Centers. The Emergency Preparedness Manual establishes standardized guidelines and procedures to assist staff in conducting an appropriate and effective response to emergent situations inside and outside a Service Processing Center detention setting.

When implemented, the Emergency Preparedness Program will protect the health and safety of the public, and maintain a secure, safe and orderly living and working environment for detainees and staff by coordinating emergency preparedness planning, response and incident recovery activities.

The IRU also provides the field offices with guidance in developing Continuity of Operations (COOP) plans. The COOP program has been established to provide personnel with information on the policies, procedures, responsibilities, guidelines and controls used to ensure that DRO can perform its essential functions during an emergency that may disrupt normal operations.

Detention Health Care

The Division of Immigration Health Services Unit (DIHS), a component of the Bureau of Primary Health Care (BPHC) and the Health Resources and Services Administration (HRSA) at

the Department of Health and Human Services (HHS), serves as the health authority for ICE through an interagency agreement with HRSA. The DIHS provides direct patient care at 15 detention locations and oversees managed care services for detainees housed at 250 jails, state agencies, and contract detention facilities nationwide. In addition, the DIHS provides infectious disease control, medical consultation and guidance, foreign health care, foreign and domestic medical escorts, facility health assessments and reviews, post-release medical placements, year-round support to the U.S. Coast Guard and 24-hour deployment to any location in the world.

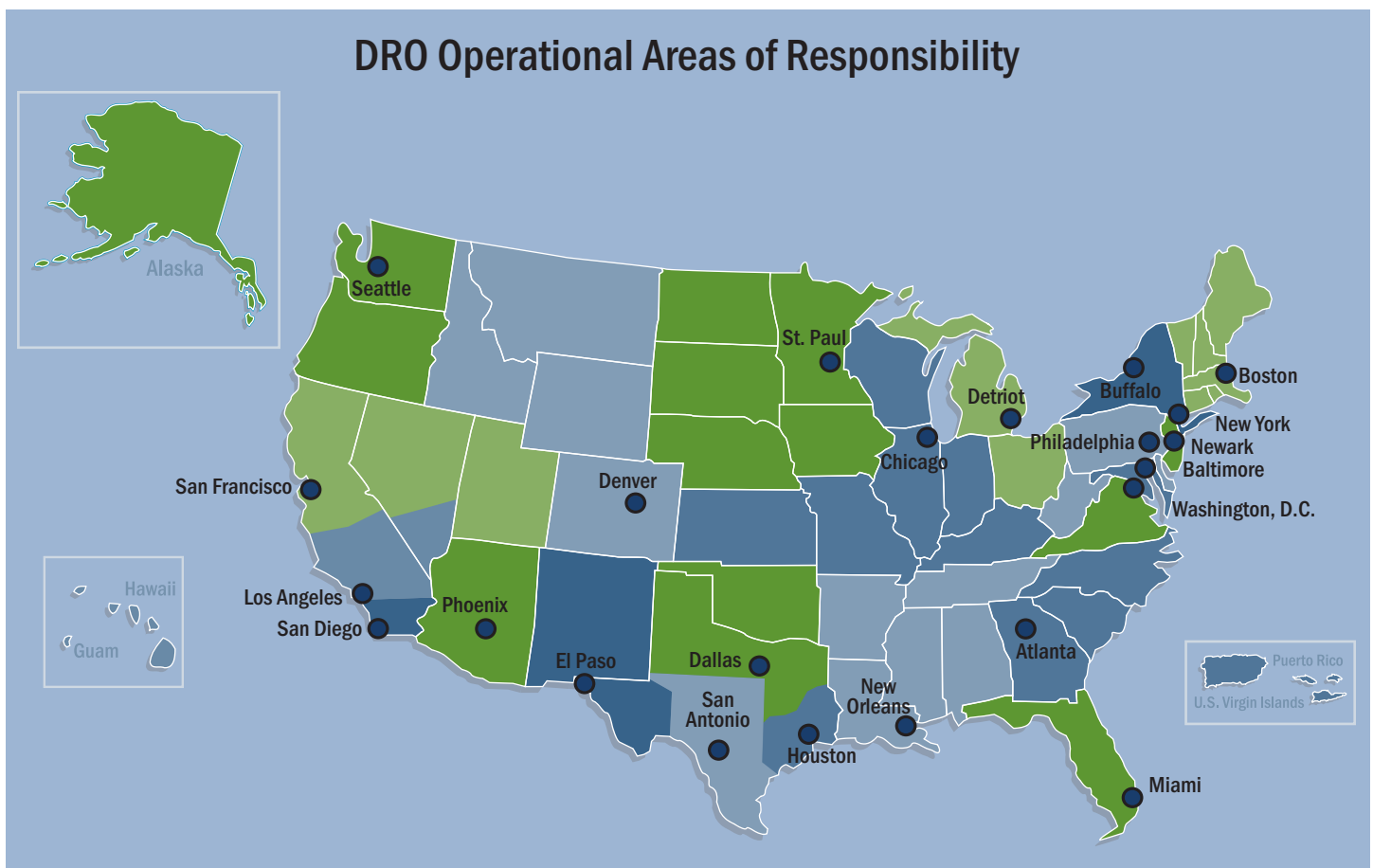
The DIHS medical program is overseen by the Detention Health Liaison Officer (DHLO), who serves as the point of contact to HHS, DHS, ICE, and state and local health authorities on issues related to medical standards and detainee health care. The DHLO is responsible for formulating and implementing policies and procedures for managing the day-to-day operations of detention health services, and for resolving congressional issues,

detainee complaints, allegations of medical negligence and other health concerns that rise to the headquarters level.

The DHLO oversees the DIHS budget, which is funded 100 percent by the DRO Detention Management Division. The DIHS operational cost for fiscal year 2006 is \$75 million, with \$32 million allocated for medical claims and \$43 million committed to operations and maintenance and HRSA administration support services.

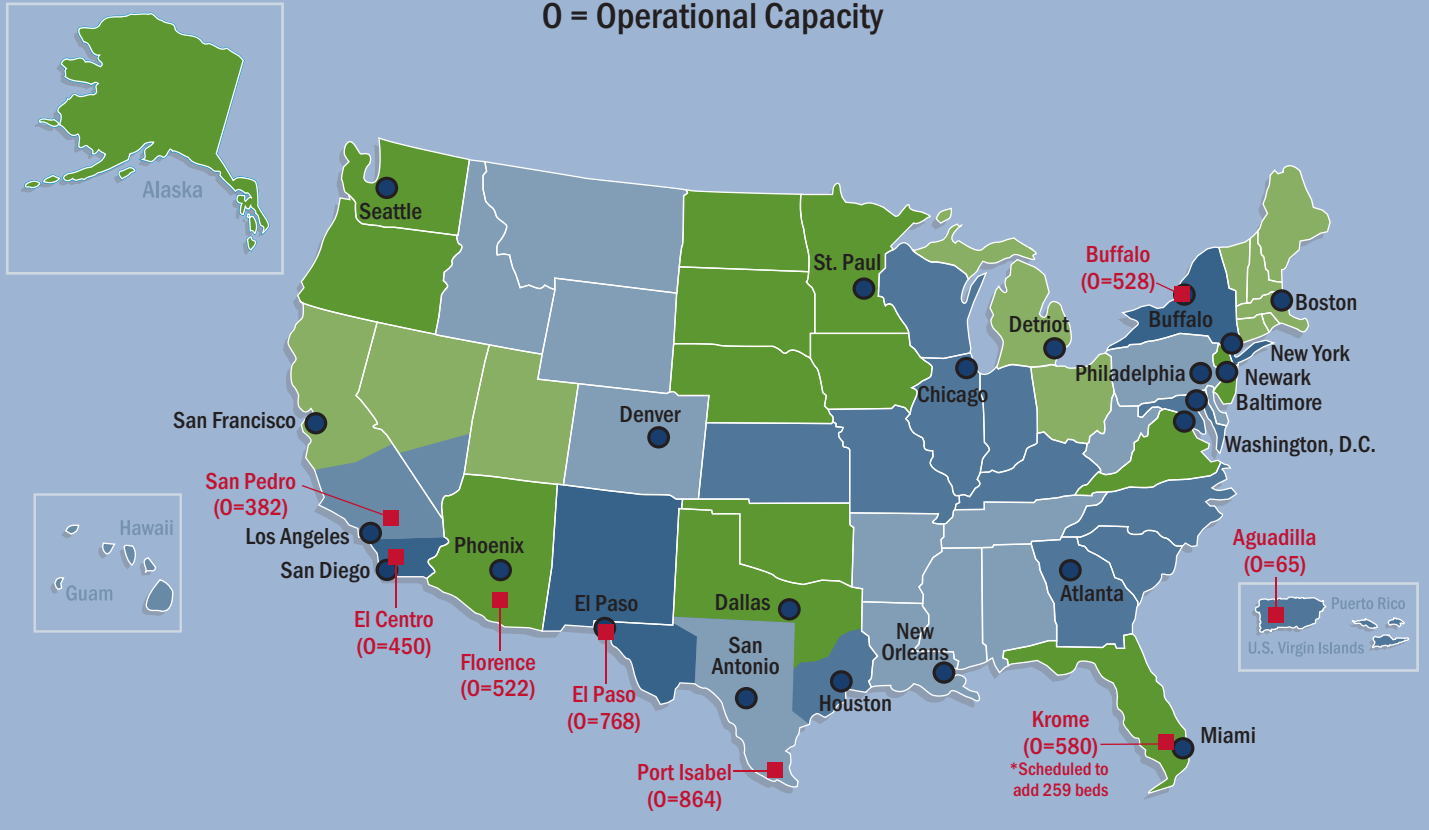
Juvenile Liaison

The overall mission of the Juvenile Operations Unit (JOU) is to treat juveniles who are in DRO custody with respect, dignity and special concern for their particular vulnerability. In order to do this, the JOU strives to place juveniles in the appropriate facilities, ensure that their safety is maintained and provide them with the appropriate educational services. Additionally, the JOU provides the appropriate mental health and medical services to juveniles if required.



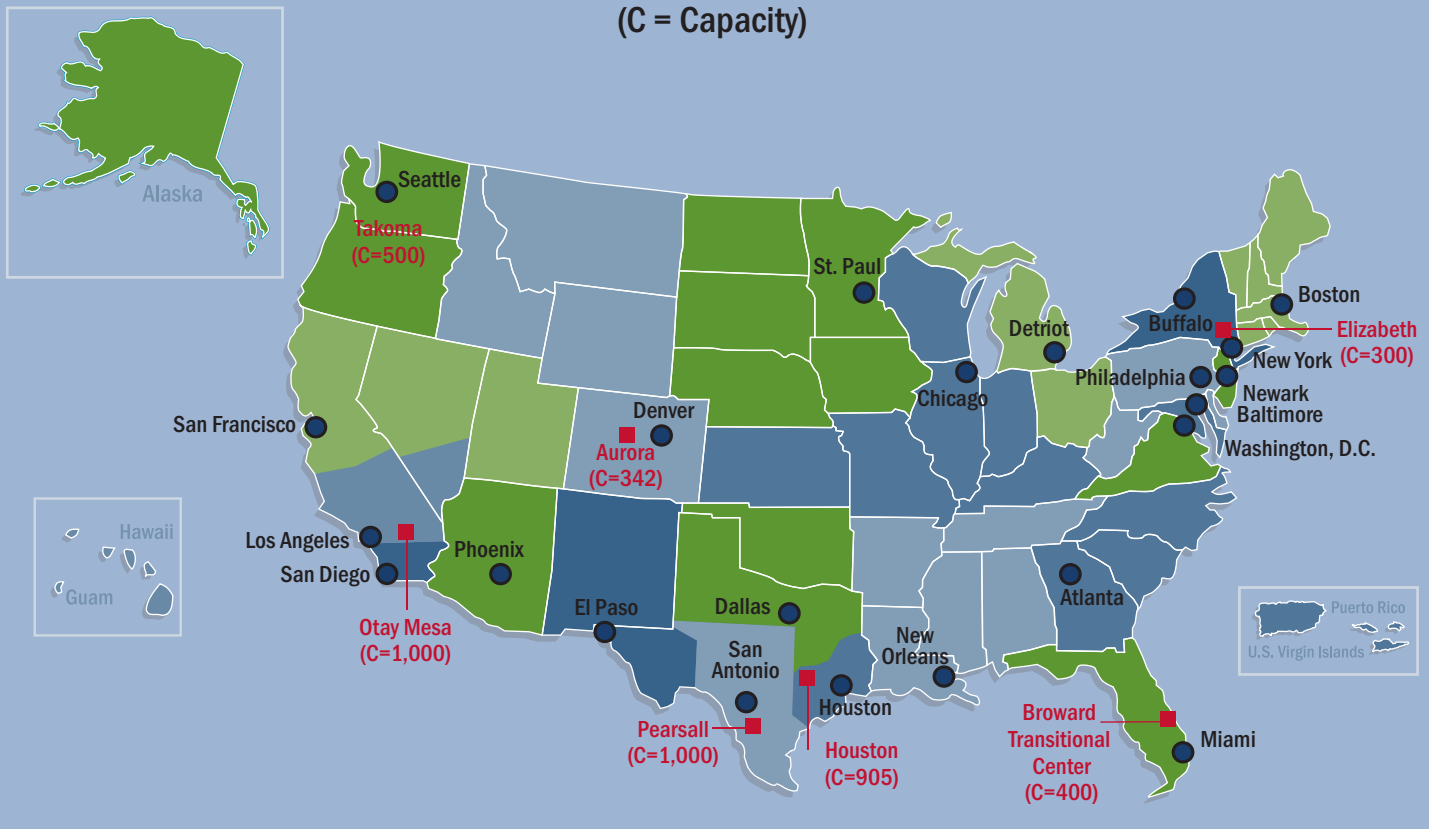
Service Processing Center (SPCs)

O = Operational Capacity



Contract Detention Facilities (CDFs)

(C = Capacity)



Removal Management Division

Executive Summary: Removal Management Division

Mission

The mission of the Removal Management Division (RMD) is to formulate all DRO transportation and removal policy, conduct transportation and removal planning, define and project transportation and removal requirements and oversee and support field office directors' execution of transportation and removal funding. Additionally, the RMD is responsible for developing and implementing efficiencies in the removal process by creating and implementing those parts of the DRO strategic plan that apply to the RMD mission.

Air Transportation Unit

The Air Transportation Unit (ATU) manages alien transportation and repatriation flights via Special Charter Missions and the Justice Prisoner and Alien Transportation System (JPATS).

JPATS is a shared program between ICE, the U.S. Marshals Service (USMS) and the Bureau of Prisons (BOP). Within the JPATS program, the ATU has operational control of four aircraft. In addition to using these aircraft to transfer aliens to different areas within the continental United States, they are used as the primary method of transportation to remove aliens to Central America. The ATU manages 8–12 flights to Central America per week using JPATS, which results in the removal of over 800 deportees



per week. In FY 2005, ATU transported and removed a total of 95,292 aliens via JPATS aircraft.

Special Charter Missions are stand-alone ICE operations using chartered aircraft primarily for the removal of large groups of aliens, to include special interest cases. In FY 2005, ATU coordinated 15 Special Charter Missions to 10 countries, resulting in the removal of 1,179 aliens. The ATU is responsible for the logistical and operational coordination of these missions with U.S. Embassies abroad.

ATU officers are also involved in discussions with foreign governments, along with the Department of State (DOS) and other Headquarter DRO Units regarding issues of repatriation and removals of aliens via ATU managed flights.

Travel Document Unit

The Travel Document Unit (TDU) conducts liaison activities for the sole purpose of removing persons from the United States. The TDU obtains documents pertaining to the repatriation of aliens, and liaisons with approximately 200 foreign embassies and consulates during this process. Furthermore, the TDU participates with the Department of State (DOS) and various foreign governments in negotiating return agreements. Additionally, the TDU coordinates the presentation of travel document requests and deals with projects relating to the imposition of sanctions for those countries that refuse to repatriate or delay the repatriation of their nationals.

In conjunction with the Secure Border Initiative (SBI), the TDU has been instrumental with setting forth proposals to add resources for improving travel document procurement and removal issues. The SBI will provide the TDU with resources to hire 72 additional personnel to streamline the travel document process, seven Immigration Enforcement Agents (IEA) to expedite the removal of Central Americans through the Houston Airport and eight Removal Liaison Officers at strategic locations overseas.

The overall goal of the TDU is to improve the efficiency of the removal process by reducing the time it takes to obtain travel documents, as well as the time in obtaining the appropriate government clearances to effect removals.



Custody Determination Unit

The Custody Determination Unit (CDU) is responsible for the development and oversight of programs relating to the proper processing of aliens in ICE custody that are subject to a final order of removal. The CDU makes custody decisions on long-term final order cases, issues operational guidance, develops training for the Office of Detention and Removal Operations (DRO) field offices and monitors the Post Order Custody Review (POCR) program nationwide. The CDU mission includes implementing effective case management and custody determination policies, while working towards the removal of all removable aliens.

The CDU is responsible for case management and removal issues, custody reviews and decisions, placement programs regarding aliens with mental problems and the continued detention of special circumstance cases. Additionally, the CDU is responsible for reviewing monthly case status reports from the field.

Centralized Ticketing Unit

The mission of the Centralized Ticketing Unit (CTU) is to manage the DRO Centralized Ticketing Program (CENTIX). The CTU functions as the coor-

dinator for airline ticketing and country clearance support for DRO Headquarter and DRO field offices in support of the removal process. The CTU coordinates with the DRO field offices, external agencies and the travel and airline industry relating to removal requirements and recommends removal process efficiencies relating to commercial transportation. The CTU also provides related mission support to the Removal Management Division in the areas of process documentation, commercial transportation, financial management and IT/Web site support.

In FY 2005, the CTU coordinated 25,885 removals (9,160 escorted and 16,725 unescorted) and transmitted 37,828 cables to U.S. Embassies and Consulates overseas.

Department of State Liaison

The Department of State Liaison (DSL) is the Senior Advisor to the Department of State (DOS) regarding Detention and Removal Operations (DRO) issues. The DSL officer serves to increase the coordination and cooperation between ICE and the DOS in regards to the issuance of travel documents. The focus of the position is to coordinate actions in order to increase the efficiency and speed of the issuance of travel documents for individuals ordered removed from the United States.

The DSL officer works with the DOS Office of Consular Affairs and the country desk officers to coordinate actions with the representatives of foreign governments in the United States, and with United States diplomatic representatives posted abroad. This coordinated approach allows for diplomatic pressure to be applied appropriately to problematic countries that refuse to issue travel documents for their citizens.

As a representative of DHS at the DOS, the DSL officer fills the role of aiding the two departments on connecting a multitude of issues; particularly those that involve the agencies formed from the legacy Immigration and Naturalization Service. By providing liaison and problem solving, the DSL officer improves relations and garners good will for DHS, and initiates and maintains contacts throughout the DOS and the diplomatic community.

SBI Operations

The Secure Border Initiative (SBI) is a comprehensive approach to immigration enforcement. The DRO SBI Unit is working with the DHS and other components of DRO to further the end of “catch and release” by the end of FY06. The unit works hand in hand with the DHS to identify initiatives and new business processes to reduce the “cycle” time required to remove aliens from the United States.

The DRO SBI Unit perform the following functions:

- Acts as a conduit between the DHS SBI Project Management Office (PMO) and DRO;
- Obtains and organizes information requested by DHS;
- Assists in the planning of initiatives involving DRO;
- Maintains a presence at meetings to ensure any impact to DRO is considered and included in future enforcement requirements;
- Keeps ICE management apprised by completing daily reports on the productivity levels and news of SBI activities.



VI

**Mission
Support
Division**

Executive Summary: Mission Support Division

Mission

The Mission Support Division (MSD) conducts strategic planning, establishes policy, develops and monitors performance measures, conducts program analyses, formulates and executes the budget and establishes and manages human capital needs and logistic resources. The MSD manages the Deportable Alien Control System (DACS), the database system of record for all aliens in ICE detention or deportation proceedings. The division carries out its responsibilities through five supporting units. These units are the Program Analysis and Information Technology (IT) Unit, the Financial Management Unit, the Logistics and Fleet Management Unit, the Human Capital and Training Unit and the Planning and Performance Management Unit.

Program Analysis and IT Unit

The Program Analysis and IT Unit (PAIT) is responsible for all analytical and statistical reporting requirements for the DRO program activities, and all elements of Systems Lifecycle Management for DRO IT systems. The PAIT prepares numerous internal reports that document past activities and analyze recent trends. These include monthly detention and removal reports and weekly updates. DRO senior level officials utilize this data to support decisions regarding changes in program direction, resource allocation and in formulating budgetary requests.

The PAIT has developed and maintained several new and specialized database systems that track and report fugitive operations, alternatives to detention, country clearance documentation and the migrant interdiction center at Guantanamo Bay, Cuba.

The PAIT also ensures compliance with IT security requirements, Systems Development Life Cycle Documentation and IT capital and operating budget submissions.

The PAIT has conducted aggressive outreach to Outside Government Agencies (OGA) resulting in over 30 information-sharing agreements. In addition to meeting the legislative requirements of the USA Patriot Act and being responsive to OGA information needs, these DRO information-



sharing initiatives have provided a direct cost saving benefit to ICE and DRO.

Financial Management Unit

The Financial Management Unit (FMU) is responsible for all aspects of budget formulation, execution and analysis as well as financial management of the Office of Detention and Removal Operations (DRO) programs. The FMU is also the primary liaison between DRO and the Office of Professional Responsibility (OPR), which includes responding to all outside audit agencies.

In line with the Homeland Security Act, the FMU has developed a Planning, Programming and Budget Execution System (PPBES) that identifies mission needs, matches the needs with resource requirements and translates the resource requirements into budget requests.

Logistics and Fleet Management Unit

The Logistics and Fleet Management Unit (LFMU) is responsible for the national procurement of vehicles, communications equipment, weapons, tactical equipment, uniforms, badges, credentials and office space and procurement policies. The unit also

performs required inventories and coordinates firearms training and quarterly qualifications for DRO Headquarters personnel.

Human Capital and Training Unit

The Human Capital and Training Unit (HCTU) are responsible for all aspects of strategic workforce management for DRO, and all DRO training and leadership development.

Planning and Performance Measurement

The Planning and Performance Measurement Unit (PPMU) conducts strategic planning, establishes associated policy, develops and monitors performance measures, cost-effectiveness measures and maintains the Detention and Deportation Officers Field Manual.



Appendices

Authorities

- Statutory Mandates and Presidential Directives that drive ICE strategic direction are as follows:
- Homeland Security Act, P.L. 107-296
- USA Patriot Act, P.L. 107-56
- Intelligence Reform and Terrorism Prevention Act
- Immigration and Nationality Act
- International Arms and Trafficking Act
- Federal Property and Administrative Services Act of 1949, P.L. 81-152
- Aviation and Transportation Security Act, P.L. 107-71
- National Security Strategy of the U.S.A.
- National Strategy for Homeland Security
- National Money Laundering Strategy
- Government Performance and Results Act
- Chief Financial Officer Act
- Clinger-Cohen Act
- Government Paperwork Elimination Act
- Federal Financial Management Improvement Act
- Federal Management Reform Act
- Title 8: Aliens and Nationality
- Title 12: Banks and Banking
- Title 13: Census
- Title 15: Commerce and Trade
- Title 18: Crimes and Criminal Procedure
- Title 19: Customs Duties
- Title 21: Food and Drugs
- Title 22: Foreign relations and Intercourse
- Title 26: Internal Revenue Code
- Title 31: Money and Finance
- Title 33: Navigation and Navigable Waters
- Title 39: Postal Service
- Title 42: Public Health and Welfare
- Title 46: Shipping
- Title 49: Transportation
- Title 50: War and National Defense

Glossary

Administrative Removals

A means of processing a criminal alien for removal if the alien is not a lawful permanent resident, has been convicted of an aggravated felony and is not eligible for any relief from removal. A DHS officer issues the final order.

Alien

Any person not a citizen or national of the United States.

Apprehension

The seizure, taking or arrest of a person on a criminal or administrative charge based on a violation of the immigration laws of the United States.

Centralized Ticketing Program (CENTIX)

The Centralized Ticketing Program (CENTIX) functions as the coordinator for airline ticketing and country clearance support for DRO Headquarter and DRO field offices in support of the removal process.

Contract Detention Facilities

Secure detention facilities contracted by ICE DRO to process illegal aliens. There are seven secure contract detention facilities utilized by ICE DRO.

Continuity of Operations

Internal Executive Branch department and agency efforts to assure continuance of their minimum essential functions across a wide range of potential emergencies, including localized acts of nature, accidents, technological and/or attack-related emergencies.

Criminal Alien

An illegal alien who is removable based on criminal conviction in accordance with the Immigration and Nationality Act.

Custody Management

The act, manner, or practice of managing, caring for, supervising, or controlling the temporary holding of individuals charged with federal crimes or pending immigration hearing and removal proceedings and all applicable resources necessary to complete this function. Such resources include, but are not limited to, staff, facilities, equipment and transportation (ground and air).

Deportable Alien

An alien in and admitted to the United States subject to any grounds of removal specified in the Immigration and Nationality Act. This includes any alien illegally in the U.S., regardless of whether the alien entered the country by fraud or misrepresentation or entered legally but subsequently violated the terms of his or her non-immigration classification or status.

Deportation

The formal removal of an alien from the U.S. when the alien has been found removable for violating the immigration laws. An immigration judge orders deportation without any punishment being imposed or contemplated. Prior to April 1997, deportation and exclusion were separate removal procedures. The Illegal Immigration Reform and Immigration Responsibility Act of 1996 consolidated these procedures. After April 1, 1997, aliens in and admitted to the U.S. may be subject to removal based on deportability.

Detention

The temporary holding of individuals charged with federal crimes or pending immigration hearings and removal proceedings.

Detention and Removal Operations

The ICE division responsible for the detention and removal of illegal aliens.

Division of Immigration Health Services:

Executive Office of Immigration Review

Department of Justice agency responsible for administering fair immigration hearings and determining the consequences of such hearings.

Expedited Removal

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 authorizes the DHS to quickly removal certain inadmissible aliens from the United States. The authority covers aliens who are inadmissible because they have no entry documents or because they have used counterfeit, altered or otherwise fraudulent or improper documents. The authority covers aliens who arrive in, attempt to enter, or have entered the United States without having been admitted or paroled by an immigration officer at a port-of-entry. The DHS has the authority

to order the removal, and the alien is not referred to an immigration judge except under certain circumstances after an alien makes a claim to legal status in the United States or demonstrates a credible fear of persecution if returned to his or her home country.

Final Order of Deportation or Removal

The order of the Immigration Judge, the Board of Immigration Appeals or other such Administrative Officer to whom the Attorney General has delegated the responsibility for determining whether an alien is removable, concluding that the alien is deportable, removable or excludable or ordering removal.

Fugitive

An alien who has failed to depart the United States or report to a DHS officer after receiving a legal order to do so, or any alien wanted by the DHS for a violation of status, order or law. This includes aliens who have violated an order of supervision, failed to appear for a hearing, or one who has reentered the United States after having been previously removed. An absconder is also a subset of this definition as an alien who has an unexecuted final order of removal and whose whereabouts are unknown.

Fugitive Operation Teams

Specially trained teams of DRO Employees that identify, locate, apprehend and remove fugitive aliens from the United States. The ultimate goal of the Fugitive Operation Teams is to eliminate the backlog of alien fugitives and ensure that the number of aliens removed from the United States equals the number of final orders of removal or grants of voluntary departure issued by the immigration courts in any given year.

Goal

Broadly defines what an agency will do to carry out its mission over a 5- or 10-year period of time. Need not be quantitative or measurable, but it is expressed in a manner that allows a future assessment to be made of whether the goal was or is being achieved. Sometimes called a Strategic Goal.

Green Notices

An Interpol generated advisory that “provides information on career criminals who have committed, or are likely to commit, offenses in several countries (habitual offenders, child molesters, pornographers).” Operation Predator cases meet this definition and, therefore, Interpol will be made aware of

Operation Predator cases through the completion of Green Notice applications.

ICE Fusion Web Site

The ICE Fusion Web site is an intranet Web-based platform at the law enforcement sensitive level where the ICE Office of Intelligence and other entities (Federal Documents Laboratory, Border Patrol, Federal Protective Service) post documents that can be both referenced and researched.

ICE Storm

A DHS operation which aims to eliminate violent crime in Phoenix, Arizona, through the identification and dismantling of smuggling organizations, prosecution of smugglers, seizure of assets and developing a working partnership with U.S. and Mexican intelligence and enforcement agencies.

Immigration Judge

An attorney appointed by the Attorney General to act as an administrative judge within the Executive Office of Immigration Review. They are qualified to conduct specified classes of proceedings, including removal proceedings.

INA 287(g)

A section in the Immigration and Nationality Act concerning the performance of immigration officer functions by state officers and employees.

Infrastructure

Systems and assets so vital to the United States that the incapacity of destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Critical infrastructures are categorized into the following sectors: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Communications, Energy, Transportation, Banking and Finance, Chemical Industry and Hazardous Materials, Postal and Shipping.

Institutional Removal Program (IRP)

The IRP is a cooperative effort between ICE, the Executive Office of Immigration Review and federal, state and local correctional agencies to identify, process and remove criminal aliens while they are still incarcerated. Upon completion of their prison sentences, aliens who have been found removable through the IRP are taken into ICE custody and expeditiously removed.

Integrated Border Enforcement Teams (IBET)

Intelligence-driven enforcement teams comprised of federal (United States and Canadian), state/provincial and local law enforcement personnel to address terrorism and other forms of criminality in the context of the border. IBET enhance border integrity and security at our shared border by identifying, investigating and interdicting persons and organizations that pose a threat to national security or are engaged in other organized criminal activity.

Justice Prisoner and Alien Transportation System (JPATS)

JPATS is a shared program between ICE, the U.S. Marshals Service (USMS) and the Bureau of Prisons (BOP). JPATS supports ICE DRO by transporting removable aliens via aircraft to their countries of origin.

Judicial Removals

Ordered as part of the criminal convictions of an alien in a federal district court. The order to remove is handed down by the federal judge as part of the sentence.

Key Assets

A broad array of unique facilities, sites and structures whose disruption or destruction could have significant consequences across multiple dimensions. Categories of key assets include: national monuments, symbols and icons; facilities and structures that represent national economic power and technological advancement; and structures where large numbers of people congregate.

MAX^{HR}

DHS' proposed new human resources system. MAX^{HR} will ensure a stronger correlation between pay and performance and be more sensitive to market changes. The goals of the new system are to enable DHS to act swiftly and decisively in response to mission needs; allow DHS to adapt to the changing nature of work; attract and maintain a highly skilled and motivated workforce; recognize and reward performance; and ensure due process and protect basic employee rights.

Mission

A statement that concisely summarizes what the organization does, as required by law, presenting the main purpose(s) for all its major functions and operations.

Objective

Defines what an agency will do to achieve its stated goals, basically a goal statement but at a more detailed level. Usually looks out over a three-to ten-year horizon. Usually consists of specific and measurable outcomes one expects to accomplish in pursuit of a goal (e.g. your goal may be to drive a car. Objectives may then be to pass a written driver's test; buy a car, etc.). Sometimes called a Strategic Objective.

Partners

Those individuals inside or outside the agency who play a supportive role in achieving the objectives of the agency's core business functions and key processes.

Prevent

To take offensive steps to target and preclude (prevent) the movement, deployment and integration efforts of terrorists or criminals prior to their attack on a system/infrastructure; Stop or hinder an action or eliminating a situation or condition that could produce an action; Make an event or action impossible, or largely ineffectual, by removing the necessary conditions.

Prosecutorial Discretion

Decisions on who to investigate, who to arrest, who to charge, what to charge and when to terminate removal proceedings and evaluating whether a case has a potentially negative impact upon the Department and whether prosecuting a particular case has little law enforcement value to the cost and time required.

Protect

To take defensive steps designed to provide the last line of defense to stop an attack if preventative actions are unable to preclude a terrorist or criminal operation from being initiated; to shield or safeguard; to keep from harm, injury or attack.

Removal

The formal enforcement of the departure of an alien from the United States pursuant to a violation of immigration law.

Secure Border Initiative

The Secure Border Initiative (SBI) is a comprehensive multi-year plan to secure America's borders and reduce illegal migration. The Office of Detention and Removal Operations (DRO) is supporting the

SBI by providing personnel who work with the DHS, ICE and other components of DRO to further the end of “catch and release” by the end of Fiscal Year 2006. Primarily, the DRO SBI Unit is identifying initiatives and new business processes to reduce the “cycle” time required to remove aliens from the United States.

System (Terrorist or Criminal)

an integrated collection of people, money or materials that seeks to harm homeland security.

Smuggling (People)

The procurement, in order to obtain a profit, of illegal entry of a person into a country of which that person is not a national.

Service Processing Center

Government owned and operated secure detention facility utilized by ICE DRO to process illegal aliens. There are currently eight Service Processing Centers utilized by ICE DRO.

Strategic Plan

Sets out the long-term programmatic, policy, and management goals of an agency. Provides the framework for more detailed annual and operational plans.

Strategy

A description of how an objective will be achieved. They are the methods by which we intend to achieve strategic goals and objectives.

Student Exchange and Visitor Information System (SEVIS)

A Web-based system for maintaining information on international students and exchange visitors in the U.S. administered by ICE. SEVIS is designed to keep our nation safe while facilitating the entry and exit process for foreign students in the U.S. and for students seeking to study in the U.S.

Terrorism

The unlawful use of force or violence against persons or property to intimidate or coerce a

government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Trafficking (In Persons)

The recruitment, transportation, transfer, harboring or receipt of persons by any form of coercion, abduction, fraud, deception and abuse of power. This involves the giving or receiving of payments or benefits to achieve the consent of a person having control over another person for exploitation.

US-VISIT

Foreign visitors arriving at U.S. international airports and seaports will have their travel documents scanned and their photo and a fingerprint taken. This information will be checked against lists of those who should be denied entry for reasons such as terrorist connections, criminal violations, or past visa violations.

Visa Security Program

A DHS initiative to ensure the security of the visa issuance process to prevent the entry of terrorists and other criminals into the United States, while allowing legitimate trade, travel and immigration.

Vision

A guiding statement that describes where an organization ideally wants to be in the future.

Vulnerable Persons

Men, women and children who are generally impoverished and uneducated from rural or refugee groups who are lured into prostitution, forced labor, slavery and servitude.

Workforce

All the people working or available to work for the organization, regardless of employment type.

Worksite Enforcement

The investigation of lead-driven employer cases having a nexus to alien smuggling, trafficking, worker exploitation and other egregious criminal or national security violations.

Acronyms

ACAP—Alien Criminal Apprehension Program

BOP—Bureau of Prisons

CDF—Contract Detention Facilities

CENTIX—Centralized Ticketing Program

DHS—Department of Homeland Security

DHLO—Detention Health Liaison Officer

DSL—Department of State Liaison

HHS—Health and Human Services

DIHS—Division of Immigration Health Services

DRO—Detention and Removal Operations

EREM—ENFORCE Removal Module

FOT—Fugitive Operation Teams

FDL—Forensic Document Laboratory

FPS—Federal Protective Service

HR—Human Resources

IBET—Integrated Border Enforcement Teams

ICE—U.S. Immigration and Customs Enforcement

IMAGE—ICE Mutual Agreement between Government and employees

IOU—Intelligence Operations Unit

IRP—Institutional Removal Program

IT—Information Technology

JPATS—Justice Alien and Prisoner Transportation System

JTTF—Joint Terrorism Task Force

LESC—Law Enforcement Support Center

MAX^{HR}—DHS' proposed new human resources system

NCIC—National Crime Information Center

OI—Office of Investigations

OMB—Office of Management and Budget

OPLA—Office of Principal Legal Advisor

SBI—Secure Border Initiative

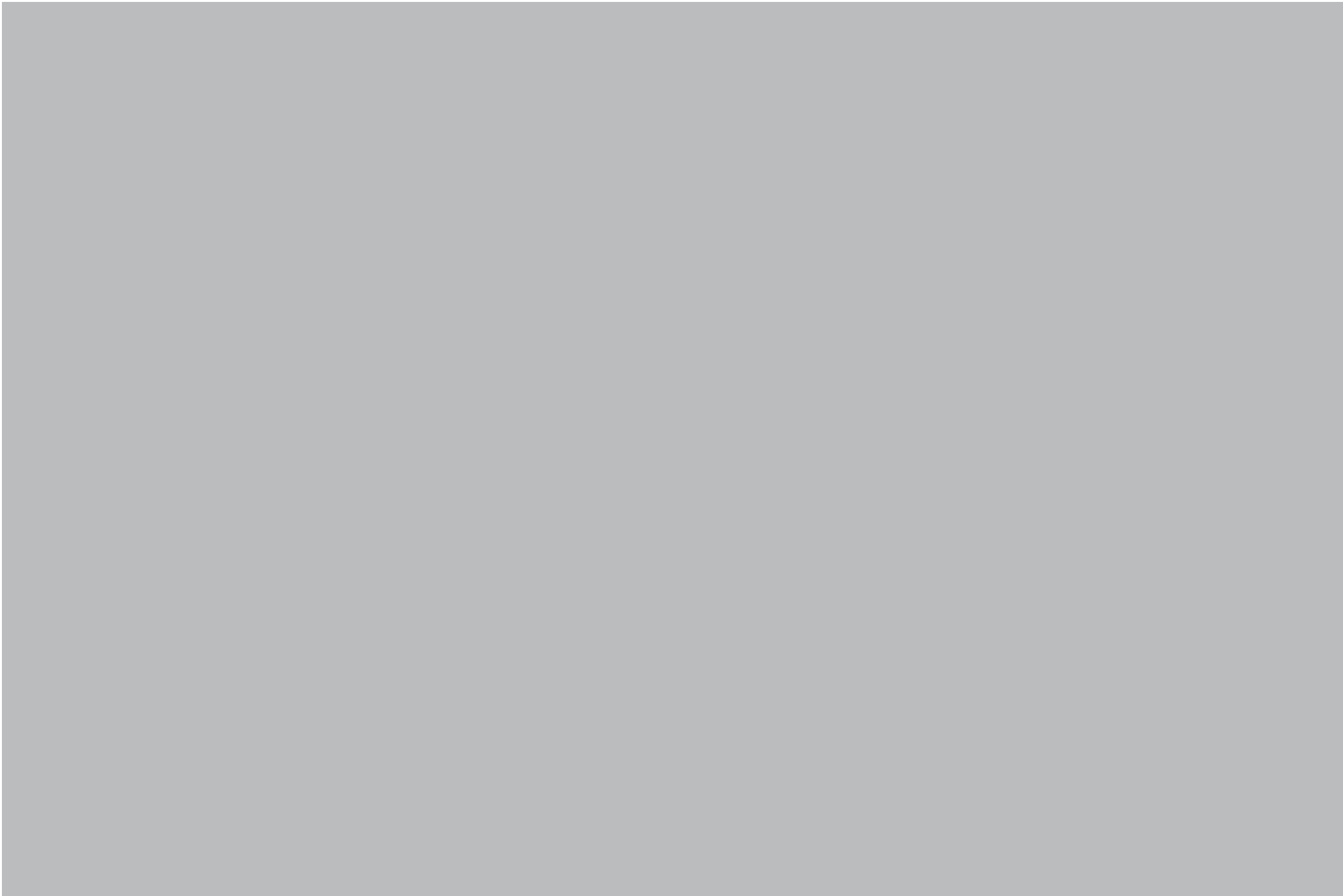
SEVIS—Student Exchange and Visitor Information System

SEVP—Student Exchange and Visitor Program

SOP—Standard Operating Procedures

SPC—Service Processing Centers

US-VISIT—Visitor and Immigrant Status Indicator Technology



U.S. Immigration
and Customs
Enforcement

www.ice.gov

ATTACHMENT B

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

User Requirements

Pages 1 through 48 redacted for the following reasons:

b2High

ATTACHMENT C

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

**Bed Space and
Transportation Study**

Pages 50 through 264 redacted for the following reasons:

b2High

ATTACHMENT D

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

Architecture Guidelines

Pages 266 through 826 redacted for the following reasons:

b2High



DHS Sensitive Systems Policy Directive 4300A

INFORMATION TECHNOLOGY SECURITY PROGRAM

Version 5.5

September 30, 2007

This implements
DHS Management Directive 4300.1

DEPARTMENT OF HOMELAND SECURITY

DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g, 4.1.5b, 4.8.4a. Modified policies: 3.7b, c, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c;

Version	Date	Description
		5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, <i>Sensitive But Unclassified to For Official Use Only</i>
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	<p>Section 1.0: 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards.</p> <p>Section 2.0: 2.0 – Insert the following after the first sentence in the second paragraph: "Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions." 2.3 – Removed parentheses from "in writing."</p> <p>Section 3.0: 3.9 – Inserted new policy element "I" regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs.</p>

Version	Date	Description
		<p>Section 4.0: 4.1.1 – Capitalized “Background,” and added “(BI).” 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted “where required or appropriate” before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment.</p> <p>Section 5.0: 5.1c – Changed inactive accounts to “disable user identifiers after 45 days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”</p>

TABLE OF CONTENTS

1.0	INTRODUCTION.....	1
1.1	IT Security Program Policy	1
1.2	Authorities.....	1
1.3	Policy Overview.....	2
1.4	Definitions.....	3
1.4.1	Classified National Security Information	3
1.4.2	National Security Information	3
1.4.3	Sensitive Information.....	3
1.4.4	Public Information	3
1.4.5	Information Technology (IT).....	3
1.4.6	DHS IT System.....	4
1.4.6.1	General Support System (GSS).....	4
1.4.6.2	Major Application (MA)	4
1.4.7	Component.....	4
1.4.8	Trust Domain	4
1.4.9	Operational Data.....	4
1.5	Waivers and Exceptions.....	4
1.6	Information Sharing and Communication Strategy	5
2.0	ROLES AND RESPONSIBILITIES.....	6
2.1	Secretary of Homeland Security	6
2.2	Under Secretaries and Heads of DHS Components.....	6
2.3	DHS Chief Information Officer (CIO)	6
2.4	Component Chief Information Officers.....	7
2.5	Chief Information Security Officer (CISO).....	8
2.6	Office of the Chief Privacy Officer (CPO).....	8
2.7	DHS Chief Security Officer (CSO)	9
2.8	Component Information Systems Security Manager (ISSM).....	9
2.9	Component Privacy Offices and Privacy Points of Contact (PPOC)	10
2.10	Program Managers (PM).....	11
2.11	United States Computer Emergency Readiness Team (US-CERT)	11
2.12	Certifying Official.....	11
2.13	Designated Accrediting Authority (DAA).....	12
2.14	Information Systems Security Officer (ISSO).....	12
2.15	System Owners	13
2.16	Users of DHS Supplied Computing Resources	13
2.17	Additional Personnel.....	14
2.18	DHS Chief Financial Officer designated Financial Systems	14
2.18.1	DHS CFO.....	14
2.18.2	DHS CIO.....	15
2.18.3	Component CFO	15
2.18.4	Component CIO	16
2.18.5	System Owners	17
3.0	MANAGEMENT POLICIES	18
3.1	Basic Requirements	18

3.2	Capital Planning and Investment Control	18
3.3	Contractors and Outsourced Operations	19
3.4	Performance Measures and Metrics.....	19
3.5	Continuity Planning for Critical DHS Assets	19
	3.5.1 Continuity of Operations Planning (COOP).....	20
	3.5.2 IT Contingency Planning (CP).....	20
3.6	System Development Life Cycle	21
3.7	Configuration Management	21
3.8	Risk Management	22
3.9	Certification and Accreditation, Remediation, and Reporting.....	22
3.10	IT Security Review and Assistance	24
3.11	Security Working Groups and Forums	24
	3.11.1 DHS Information Systems Security Board.....	24
	3.11.2 DHS IT Security Training Working Group	24
	3.11.3 DHS Wireless Security Working Group (WSWG)	25
3.12	IT Security Policy Violation and Disciplinary Action.....	25
3.13	Required Reporting.....	26
3.14	Privacy and Data Security.....	26
	3.14.1 Personally Identifiable Information (PII).....	26
	3.14.2 Privacy Impact Assessments.....	27
	3.14.3 Privacy Incident Reporting	27
	3.14.4 E-Authentication	28
3.15	DHS Chief Financial Officer Designated Financial Systems	28
4.0	OPERATIONAL POLICIES.....	31
4.1	Personnel.....	31
	4.1.1 Citizenship, Personnel Screening, and Position Categorization	31
	4.1.2 Rules of Behavior	31
	4.1.3 Access to Sensitive Information	31
	4.1.4 Separation of Duties.....	32
	4.1.5 IT Security Awareness, Training, and Education	32
	4.1.6 Separation from Duty.....	33
4.2	IT Physical Security	33
	4.2.1 General Physical Access	33
	4.2.2 Sensitive Facility.....	33
4.3	Media Controls.....	34
	4.3.1 Media Protection.....	34
	4.3.2 Media Marking.....	34
	4.3.3 Media Sanitization and Disposal	34
	4.3.4 Production, Input/Output Controls	34
4.4	Voice Communications Security	35
	4.4.1 Private Branch Exchange.....	35
	4.4.2 Telephone Communications	35
	4.4.3 Voice Mail	35
4.5	Data Communications.....	35
	4.5.1 Telecommunications Protection Techniques	35
	4.5.2 Facsimiles	35

4.5.3	Video Teleconferencing.....	35
4.5.4	Voice over Data Networks.....	36
4.6	Wireless Communications	36
4.6.1	Wireless Systems	37
4.6.2	Wireless Portable Electronic Devices (PED).....	38
4.6.2.1	Cellular Phones.....	39
4.6.2.2	Pagers	39
4.6.2.3	Multifunctional Wireless Devices	39
4.6.3	Wireless Tactical Systems	39
4.6.4	Radio Frequency Identification (RFID).....	40
4.7	Overseas Communications.....	41
4.8	Equipment.....	41
4.8.1	Workstations	41
4.8.2	Laptop Computers and Other Mobile Computing Devices	41
4.8.3	Personally Owned Equipment and Software (Not owned by or contracted for by the Government).....	41
4.8.4	Hardware and Software.....	42
4.8.5	Personal Use of Government Office Equipment and DHS IT Systems/Computers.....	42
4.8.6	Wireless Settings for Peripheral Equipment.....	43
4.9	Security Incidents and Incident Response and Reporting.....	43
4.9.1	Law Enforcement Incident Response	44
4.10	Documentation (Manuals, Network Diagrams).....	44
4.11	Information and Data Backup.....	45
4.12	Converging Technologies	45
5.0	TECHNICAL POLICIES	46
5.1	Identification and Authentication	46
5.1.1	Passwords.....	46
5.2	Access Control.....	47
5.2.1	Automatic Account Lockout.....	47
5.2.2	Automatic Session Termination.....	47
5.2.3	Warning Banner	47
5.3	Auditing	48
5.4	Network and Communications Security	48
5.4.1	Remote Access and Dial-In	48
5.4.2	Network Security Monitoring.....	49
5.4.3	Network Connectivity.....	49
5.4.4	Firewalls.....	50
5.4.5	Internet Security.....	50
5.4.6	Email Security.....	51
5.4.7	Personal Email Accounts	51
5.4.8	Testing and Vulnerability Management.....	51
5.4.9	Peer-to-Peer Technology	52
5.5	Cryptography	52
5.5.1	Encryption.....	53
5.5.2	Public Key Infrastructure.....	53

5.5.3	Public Key/Private Key.....	54
5.6	Virus Protection	56
5.7	Product Assurance	56
6.0	DOCUMENT CHANGE REQUESTS.....	57
7.0	QUESTIONS AND COMMENTS.....	57

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Technology (IT) Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication: DHS 4300A Sensitive Systems Handbook. The handbook serves as a foundation for Components to develop and implement their IT security programs. The baseline security requirements (BLSRs) included in the handbook must be addressed when developing IT security documents.

1.1 IT Security Program Policy

The DHS IT Security Program provides a baseline of policies, standards, and guidelines for DHS Components. This document provides direction to managers and senior executives for managing and protecting sensitive systems. It also outlines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation within the DHS IT infrastructure and operations.

The policies and direction contained in this document apply to all DHS Components. IT security policies and implementing procedures for National Security Systems are covered in DHS National Security Systems Policy Directive 4300B and DHS 4300B National Security Systems Handbook.

The DHS IT Security Program does not apply to systems that process, store, or transmit National Intelligence Information.

Policy elements are effective when issued. Any policy elements that have not been implemented within 90 days shall be considered a weakness. Either a system or program POA&M must be generated by the Component for the identified weaknesses. When DHS Security Compliance tools (RMS and TAF) are required to be updated to reflect policy element changes, tool changes shall be available to the Department within 45 days of the policy changes.

1.2 Authorities

The DHS has established a Department-wide IT security program and organization based on the following Executive orders, public laws, and national policy:

- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002
- Federal Financial Management Improvement Act of 1996 (FFMIA), P.L. 104-208
- Federal Managers' Financial Integrity Act of 1982 (FMFIA), P.L. 97-255
- The National Security Act of 1947, dated July 26, 1947
- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996
- Public Law 107-296, Homeland Security Act of 2002

- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984
- Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, dated November 18, 1988, as amended
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Circular A123, *Management's Responsibility for Internal Control*, Revised, December 21, 2004
- OMB Circular A-127, *Financial Management Systems*, Revised December 1, 2004
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements* August 23, 2006
- Department of Homeland Security Acquisition Regulation (HSAR), June 2006
- DHS Management Directives (e.g., MD 0470.1, MD 1030, MD 4400.1, MD 4500.1, MD 4600.1, MD 11042.1, MD 11050.2)
- National Institute of Standards and Technology (NIST) Special Publications (e.g., 800-16, 800-34, 800-37, 800-50, 800-53) and Federal Information Processing Standards (FIPS) (e.g., FIPS 199, 200)
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000

1.3 Policy Overview

DHS IT security policies delineate the security management structure and foundation to measure progress and compliance. Policies in this document are organized under three areas: management, operational, and technical.

- **Management Controls** – Focus on managing both the IT security system and system risk. These controls consist of risk mitigation techniques and concerns normally addressed by management.
- **Operational Controls** – Focus on mechanisms primarily implemented and executed by people. These controls are designed to improve the security of a particular system, or group of systems. These controls require technical or specialized expertise and often rely on management and technical controls.
- **Technical Controls** – Focus on security controls executed by IT systems. These controls provide automated protection from unauthorized access or misuse. They facilitate detection of security violations, and support security requirements for applications and data.

1.4 Definitions

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in the National InfoSec Glossary (http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf).

1.4.1 Classified National Security Information

Information that has been determined, pursuant to Executive Order 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status.

1.4.2 National Security Information

Information that has been determined, pursuant to Executive Order 12958 (as amended) or any predecessor order, to require protection against unauthorized disclosure.

1.4.3 Sensitive Information

“Sensitive information” is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security Number; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. This type of information concerning financial systems will be identified as Sensitive Financial Information, if on another system it would be identified as system vulnerability information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

With the exception of certain types of information protected by statute (e.g. Sensitive Security Information, Critical Infrastructure Information), there are no specific Federal criteria and no standard terminology for designating types of sensitive information. Such designations are left to the discretion of each individual Federal agency. “For Official Use Only” (FOUO) is the term used within DHS to identify unclassified information of a sensitive nature that is not otherwise categorized by statute or regulation.

1.4.4 Public Information

This type of information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration. (e.g. Public Web sites)

1.4.5 Information Technology (IT)

The Clinger-Cohen Act defines information technology as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency.

For purposes of the preceding definition, “equipment” refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product.

The term “information technology” includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

1.4.6 DHS IT System

A DHS system is any IT that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include general support systems and major applications.

1.4.6.1 General Support System (GSS)

A general support system (GSS) is an interconnected set of information resources under the same direct management control that share common functionality. A GSS normally includes hardware, software, applications, data and users. Examples of a GSS include a local area network (LAN), an agencywide backbone, a communications network, a data processing center, a tactical radio network, or a shared information processing service organization.

1.4.6.2 Major Application (MA)

A major application (MA) is an automated information system (AIS) that “requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.¹” An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications.

1.4.7 Component

A DHS Component is any of the entities within DHS, including all DHS offices and independent agencies.

1.4.8 Trust Domain

A Trust Domain consists of a group of people, information resources, data systems, and/or networks subject to a shared security policy (set of rules governing access to data and services). (For example, a Trust Domain may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

1.4.9 Operational Data

Operational data is information used in the execution of any DHS mission.

1.5 Waivers and Exceptions

Components may request waivers to, or exceptions from, any portion of this policy, for up to 6 (six) months, whenever they are unable to fully comply with policy requirements. Requests are made, through the Information Systems Security Board (ISSB), to the Chief Information Security Officer (CISO) and shall include the operational justification, risk acceptance, risk mitigation measures, and a plan for bringing the system into compliance. A second waiver request for up to 6 (six) months may be made only by the Head of the Component and only if the waiver is reported as a material weakness in the Component’s Federal Information Systems Management Act (FISMA) report.

¹ OMB Circular A-130

A Component may request an Exception to Policy whenever it is unable to bring the system into compliance. Exceptions are generally limited to mission-specific systems that are not part of the DHS Enterprise Infrastructure. This request is made, through the ISSB, to the CISO and shall include the operational justification, risk acceptance, and risk mitigation measures.

The Waiver Request Form, located in Attachment B of the DHS 4300A Sensitive Systems Handbook, shall be used.

NOTE: Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. Citizens (policy 4.1e). Under normal conditions, only U.S. Citizens are allowed access to DHS systems and networks, however, at times there is a need to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to appropriate policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. Citizenship requirement flows through the Component Head, the Office of Security, and the Chief Information Officer. Attachment J to the DHS 4300A Sensitive Systems Handbook provides an electronic form for requesting exceptions to the U.S. Citizenship requirement.

1.6 Information Sharing and Communication Strategy

The DHS SOC exchanges information with Component SOC, NOCs, the HSDN SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from “raw” fault, configuration management, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOC.

The DHS SOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to the Component SOC, ISSMs or other identified Component points of contact.

The DHS SOC portal implements role-based user profiles that allow Components to use the website’s incident database capabilities. Users assigned to Component groups will be able to perform actions such as:

- Entering incident information into the DHS SOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers
- Automating portions of the Information Security Vulnerability Management (ISVM) program
- Automating portions of the vulnerability assessment program

2.0 ROLES AND RESPONSIBILITIES

Persons and organizations must understand their roles and responsibilities and adhere to all relevant Federal and Departmental regulations and guidance.

Designated personnel play a major role in the planning and implementation of IT security requirements. Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions. The following presents a list of roles and responsibilities for implementing these requirements.

2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for ensuring that DHS IT systems and their data are protected in accordance with Congressional and Presidential directives. To that end, the Secretary:

- Ensures the integrity, confidentiality, availability, authenticity, and nonrepudiation of information and information systems.
- Ensures that DHS implements its IT Security Program throughout the life cycle of each DHS system.
- Submits (1) the Chief Information Officer's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance, and (2) the results of an independent information security program evaluation performed by the DHS Inspector General, annually to the Director of the Office of Management and Budget (OMB)

2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and the heads of DHS Components:

- Appoint Chief Information Officers (CIO) and Information System Security Managers (ISSM) as appropriate.
- Ensure that an IT Security Program is established and managed in accordance with DHS policy and implementation directives.
- Ensure that the security of IT systems is an integral part of the life cycle management process for all IT systems developed and maintained within their Components.
- Ensure that adequate funding for IT security is provided for Component IT systems and that adequate funding requirements are included for all IT systems budgets.
- Ensure that IT system data are entered into the appropriate DHS Security Management Tools to support DHS IT security oversight and FISMA reporting requirements.
- Ensure that the requirements for an IT security performance metrics program are implemented.

2.3 DHS Chief Information Officer (CIO)

The DHS Chief Information Officer (CIO) will establish and oversee the Department-wide IT Security Program, ensure proper computer security incident response, and provide consulting assistance to all DHS offices for their individual programs. The DHS CIO provides management

direction for the DHS Security Operations Center (SOC) and overall direction for Component SOCs. The DHS CIO, or designated representative, has the sole responsibility for public release of information concerning computer security incidents. The CIO will consult with the DHS Privacy Office and Public Affairs Office prior to releasing any information.

The DHS CIO:

- Appoints a Federal employee in writing to serve as the DHS Chief Information Security Officer (CISO).
- Serves as the Designated Accrediting Authority (DAA) for DHS enterprise IT systems. This responsibility may be delegated in writing as appropriate.
- Participates in developing DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program.
- Ensures that all IT systems acquisition documents, including existing contracts, include appropriate IT security requirements and comply with DHS IT security policies.
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes.
- Ensures that system owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control.
- Reviews and evaluates the IT Security Program annually.
- Ensures that an IT security performance metrics program is developed, implemented, and funded.
- Reports to the Under Secretary for Management on matters relating to the security of DHS IT systems.

2.4 Component Chief Information Officers

Component CIOs provide management direction to their security operations and are the principal advocates for computer security incident response.

Component Chief Information Officers (CIO):

- Establish and oversee their Component IT security programs.
- Ensure that a Component Information System Security Manager (ISSM) has been appointed.
- Ensure that a Designated Accrediting Authority (DAA) has been appointed for all Component IT systems and serve as the DAA for any IT system where a DAA has not been appointed or where a vacancy exists.
- Ensure that IT security concerns are addressed by Component Configuration Control Boards, Architecture Review Board, and Investment Review Board.
- Ensure that an accurate IT systems inventory is established and maintained.
- Ensure that an IT security performance metrics program is developed, implemented, and funded.

- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or issues that may cause public concern or loss of credibility.
- Ensure that incidents are reported to the DHS SOC within reporting time requirements as defined in Attachment F of the DHS Sensitive Systems Handbook
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. *The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.*

2.5 Chief Information Security Officer (CISO)

The Chief Information Security Officer (CISO) reports directly to the CIO, serves as the Department-wide Information Systems Security Manager (ISSM), and is the principal advisor for IT security matters.

The CISO:

- Issues Department-wide IT security policy, guidance, and architecture requirements for all DHS IT systems and networks
- Implements and manages the Department-wide IT Security Program and ensure compliance with FISMA and OMB requirements.
- Serves as the principal Departmental liaison with organizations outside the DHS for matters relating to IT security.
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and accrediting DHS IT systems. This includes Security Test and Evaluation (ST&E) plans, contingency plans, and risk assessments.
- Reviews requests for waivers and exception to DHS IT security policy.
- Consults with the DHS Chief Security Officer on matters pertaining to physical security, personnel security, information security, investigations, and SCI systems, as they relate to IT security and infrastructure.
- Briefs the DHS CIO and senior management on the status and outcome of ongoing and completed computer security incidents.
- Tests and evaluates periodically the effectiveness of information security policies, procedures, and practices.
- Develops and implements procedures for detecting, reporting, and responding to computer security incidents.
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems.

2.6 Office of the Chief Privacy Officer (CPO)

The Chief Privacy Officer (CPO) is responsible for Departmental compliance with privacy policy, including measures for securing information security assets and activities. The CPO works to maintain privacy requirements, while supporting security requirements.

The CPO serves as the senior official responsible for:

- Oversight of privacy incident management
- Responding to suspected or confirmed privacy incidents or incidents involving Personally Identifiable Information (PII)
- Coordinating with the DHS CIO and senior management when dealing with high-impact privacy incidents
- Providing the status and outcomes of ongoing and completed privacy incidents
- Distributing reports to the DHS and Component CIOs
- Receiving reports that impact DHS privacy programs
- Working with the DHS CIO and DHS CISO in preparation for release of computer security incident information involving PII or other privacy issues
- Convening and chairing incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)

2.7 DHS Chief Security Officer (CSO)

The Chief Security Officer (CSO) reports directly to the Deputy Secretary on all matters pertaining to security within the DHS. Pursuant to Executive Order 12958, as amended, the CSO is designated the Senior Agency Official. In that capacity, the CSO:

- Directs and administers the Department's program under which information is classified, safeguarded, and declassified.
- Coordinates the Department's classification management program and serve as the DHS point of contact with the Information Security Oversight Office.
- Provides support and coordinates with the Department's emergency planning and response efforts and activities.
- Provides guidance and oversight on meeting physical security requirements.

2.8 Component Information Systems Security Manager (ISSM)

The Information Systems Security Manager (ISSM) are the principal interface between the Office of the CISO, Component Information Systems Security Officers (ISSOs) and other security practitioners. As such, the ISSM plays a critical role in ensuring that the DHS IT Security Program is implemented and maintained throughout the Component. The ISSM must be a DHS employee and must be appointed by the appropriate Component executive.

ISSMs:

- Oversee the Component IT security program.
- Ensure that IT security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons within their Component.
- Ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems.
- Approve and/or validate all Component IT system security reporting.

- Consult with the Component Privacy Office or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents.
- Manage IT security resources including oversight and review of Exhibit 300 funding documents.
- Review and approve the security of hardware and software prior to implementation into the Component SOC.
- Test the security of implemented systems
- Implement and manage the Plan of Action and Milestones (POA&M) process.
- Maintain an inventory of all IT systems.
- Ensure the Component IT security program is structured to support DHS and appropriate FISMA and OMB requirements.
- Develop and publish procedures necessary to implement the requirements of DHS IT security policy within the appropriate Component.
- Ensure that Information Systems Security Officers (ISSO) are appointed for each IT system managed at the Component level.
- Review and approve ISSO appointments.
- Ensure that the CISO-approved Risk Management System (RMS) automated tool is utilized for conducting certification and accreditation evaluations.
- Ensure that the CISO-approved Trusted Agent FISMA (TAF) automated tool is utilized for conducting self-assessment evaluations and for reporting required IT security program status information.
- Ensure that weekly incident reports are submitted to the DHS SOC.
- Acknowledge receipt of Information Security Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers.

2.9 Component Privacy Offices and Privacy Points of Contact (PPOC)

The Component Privacy Offices and Privacy Points of Contact (PPOC) are responsible for compliance with Federal laws and DHS privacy policy at the Component level. The Privacy Officers and PPOCs work with the Component CIO and DHS CPO to maintain privacy requirements. SOCs will work with their Component Privacy Offices, PPOCs, or with the DHS CPO to address suspected or confirmed privacy incidents (PI) or incidents involving PII.

Component Privacy Offices and Privacy Points of Contact:

- Advise the Component CIO and management regarding privacy issues relevant to the Component.
- Receive and evaluate reports that impact DHS privacy programs.
- Work with system owners to complete privacy impact assessments
- Coordinate with program managers, Component ISSMs, CSIRC, or SOC in evaluating and reporting suspected or confirmed incidents involving PII.

- Inform the DHS CPO of the status of ongoing and completed privacy incidents in a timely manner.
- Advise the CPO regarding the handling of reported privacy Incidents.
- Provide privacy incident updates to US-CERT as further information is obtained.
- Work with the DHS CPO, Component CIO and Component CISO in preparation for release of computer security incident information involving PII or other privacy issues
- Work with the Component CIO and DHS Privacy Officer in preparation for release of computer security incident information involving PII or other privacy issues

2.10 Program Managers (PM)

Program Managers are responsible for ensuring compliance with applicable Federal laws, directives and Departmental policy governing the security, operation, maintenance and privacy protection of IT systems, information and programs under his or her control.

Program Managers:

- Work with system owners, Component ISSMs, and their staffs to ensure information systems are properly secured.
- Understand how to recognize and respond to suspected or confirmed security incidents, privacy incidents or incidents involving PII.
- Consult with Component privacy offices or PPOCs concerning privacy incidents and other privacy issues affecting IT systems and programs under his or her control.
- Prepare and transmit written Privacy Event Notification (PEN) simultaneously to Component privacy offices/PPOCs, the Component CIO and ISSM.
- Supplement privacy incidents reports to the DHS SOC and US-CERT as information becomes available.

2.11 United States Computer Emergency Readiness Team (US-CERT)

The United States Computer Emergency Readiness Team (US-CERT) is designated as the central reporting organization within the Federal Government and serves as the central repository for Federal incident data. The DHS SOC will report security incidents to the US-CERT. The US-CERT may notify law enforcement, the Identity Theft Task Force, the Social Security Administration, and the Executive Office of the President, as appropriate.

2.12 Certifying Official

A Certifying Official (typically the ISSM) is assigned to each IT system by an appropriate Component official. A Certifying Official may be responsible for more than one system.

Certifying Officials must be Federal employees and must be designated in writing for each IT system. Designation letters shall be signed by the appropriate Under Secretary or Component Head. The Certifying Official:

- Ensures that required Certification and Accreditation (C&A) activities are completed, and that the test results are documented.

- Ensures that a risk analysis is performed and that it identifies risks, determines their magnitude, and identifies areas needing safeguards.
- Ensures that a system test and evaluation is conducted and the results of such tests are documented or updated annually.
- Ensures that rules of behavior and security procedures/guides are developed.
- Ensures that a contingency plan is prepared and tested annually
- Ensures that the C&A documentation is recorded in the DHS C&A Tool and FISMA Reporting Tool
- Reviews the C&A package (SSP, Security Assessment Report, and POA&M) and recommends to the DAA whether or not the system should be accredited.
- Prepares the security accreditation decision letter for the DAA's signature.

2.13 Designated Accrediting Authority (DAA)

The Designated Accrediting Authority (DAA) controls personnel, operations, maintenance, and budgets for the systems or field site and has the authority to formally assume responsibility for operating an IT system at an acceptable level of risk. The DAA should control the resources necessary to mitigate risks.

A DAA shall be assigned to each IT system and may be responsible for more than one system. The DAA should be the system owner or an appropriate program official. (i.e., A Component CFO would be assigned as the DAA for a CFO designated financial system) The Component CIO shall serve as DAA anytime the system owner or an appropriate program official cannot be named.

DAAs:

- Review Notices of Findings and Recommendations (NFR) and Plans of Action and Milestones (POA&M)
- Review and approve corrective actions necessary to mitigate residual risks.
- Approve/disapprove system accreditation, or issue an Interim Authorization to Operate (IATOs may be issued only for systems in development testing or for prototypes).
- Terminate system operation if security conditions warrant such action.

2.14 Information Systems Security Officer (ISSO)

An Information Systems Security Officer (ISSO) shall be appointed in writing, by the appropriate official, for each IT system. An ISSO may either be a Federal employee or an appropriately cleared support contractor and may be assigned to more than one system. For financial or privacy systems, ISSOs shall not be assigned collateral duties.

ISSOs:

- Serve as the principal points of contact for all IT security aspects pertaining to their systems.
- Work closely with the Component ISSM and DHS CISO staff to interpret and apply IT security policies and implementing procedures.

- Serve as liaison between system owners and the ISSM.
- Work with system owners to document weaknesses in POA&Ms and initiate corrective action.
- Employ automated tools (approved by the DHS CISO) such as the Risk Management System (RMS) and Trusted Agent FISMA (TAF).

2.15 System Owners

System owners use information technology to help achieve the mission needs within their program area of responsibility. As such, they are responsible for the successful operation of the IT systems within their program area and are ultimately accountable for the security of the IT systems and programs under their control.

System owners:

- Serve as the Designated Accrediting Authority (DAA) for systems under their purview
- Ensure that an ISSO is formally assigned to each IT system under their control and that this assignment is appropriately documented
- Ensure that required computer security functions and documentation are included in system life cycle planning and budgets
- Work closely with the CIO and other program and IT managers to ensure a complete understanding of risks, especially the increased risks resulting from interconnectivity with other programs and systems
- Document and manage accepted security risks in risk assessments
- Update the security of IT systems within their program area annually
- Ensure that system POA&Ms are prepared and maintained and that points of contact and resources are identified
- Prioritize security weaknesses for mitigation based on material weaknesses, external audits and program assessments
- Work with the Component Privacy Office or PPOC to Conduct Privacy Impact Assessments (PIA)
- Report Privacy and Computer Security incidents as appropriate, in coordination with the ISSM and Program Manager

2.16 Users of DHS Supplied Computing Resources

DHS employees, contractors, and vendors working on behalf of the DHS or its agencies, are responsible for reporting suspected or confirmed computer security incidents to their Component-level capability, or to the DHS SOC, in accordance with the Component's incident response procedures.

Successful situational awareness depends on effective security awareness and incident handling. Each Component will review its security awareness training requirements annually to ensure they reflect the evolving and changing nature of incidents.

2.17 Additional Personnel

Other personnel throughout DHS are responsible for various aspects of the IT security program. Contracting Officers and their Technical Representatives, project managers, system and network administrators, managers, supervisors, and users all play a role in helping to ensure the security of the Department's IT systems. The DHS 4300A Sensitive Systems Handbook provides a description of the roles and responsibilities of these additional personnel.

In implementing DHS IT security policy, Component heads will include these additional personnel in their security plans.

2.18 DHS Chief Financial Officer designated Financial Systems

The DHS CFO-designated financial systems require additional management accountability and effective internal control over financial reporting, as outlined in Section 3.15.

For CFO-designated financial systems, additional roles and responsibilities are summarized in this section.

2.18.1 DHS CFO

The Department CFO oversees application control definitions for financial systems as defined in OMB Bulletin No. 06-03, Audit Requirements for Federal Financial Statements, and DHS Technical Guidance No. 03-06–Laws and Regulations, Cross Servicing Assertion, and Draft OMB Bulletin 01-02. The Department CFO has committed to:

- Identifying financial systems subject to OMB A-123 and Internal Controls over Financial Reporting (ICOFR) requirements (“CFO-designated financial systems”).
- Working with the Department CIO to ensure the confidentiality, integrity and availability of financial data processing.
- Overseeing the development and establishment of policies and procedures regarding automated application controls for Department-wide application software processing financial data.
- Remediating automated application control deficiencies related to financial application policies and procedures at the Department level.
- Tracking and monitoring progress of automated application controls corrective action plans and remediation efforts at the Department and Component Levels.
- Working with the Department CIO to identify and incorporate user requirements for new financial applications or existing Departmental financial applications.
- Working with the DHS CIO to integrate and test the Department-wide business continuity plan.
- Coordinating with the DHS CIO to identify the financial data to be backed up and recovered and developing policies to ensure that procedures are in place for backing up and recovering critical financial data.

2.18.2 DHS CIO

The Department CIO is responsible for overseeing compliance of CFO-designated financial systems with Federal system security regulations and guidelines as documented in DHS Sensitive Systems Policy Directive 4300A, including support for OMB Circular A-123. The Department CIO:

- Ensures sufficient resources are provided to support the Department's compliance tracking.
- Reviews and evaluates the Department-wide IT Security Program.
- Categorizes information system deficiencies by OMB A-123 information technology general controls (ITGC) domains and TrustedAgent FISMA (TAF) risk levels.
- Remediate Information Technology General Control (ITGC) deficiencies related to policies and procedures at the Department level.
- Tracks and monitors progress of ITGC Plans of Action and Milestones (POA&M) and remediation efforts at the Department and Component levels.
- Ensures that Contracts and Interagency Agreements (IAA) include Homeland Security Acquisition Regulation (HSAR) security clauses.
- Develops Department-wide system development lifecycle methodology and monitor Component compliance with this methodology.
- As part of developing new financial applications or updating existing Departmental applications, integrates CFO feedback to ensure user requirements are adequately addressed.
- Develops and tests Department-wide disaster recovery plan. Coordinate with CFO to incorporate business continuity requirements and test on a periodic basis.
- Based on coordination with Department CFO, develops and implement Department-wide procedures for the routine backing up and recovering of financial data.

2.18.3 Component CFO

The Component CFO, working with the Component system owners, is responsible for overseeing implementation and compliance of IT controls for CFO-designated financial systems at the Component level. The Component CFO:

- Works with the Component CIO and owners of CFO-designated financial systems to help ensure the reliability of financial data processing through Component systems.
- Develops and establishes policies and procedures regarding automated application controls for software processing of financial data.
- Remediate automated application controls deficiencies at the Component level.
- Works with system owners to designate an Information System Security Officer (ISSO) for each of the CFO-designated financial systems, as defined in Section 3.15 of DHS Sensitive Systems Policy Directive 4300A.

- Tracks and monitors progress of automated application controls remediation efforts at the Component level.
- Works with system owners of CFO-designated financial systems to ensure remediation of ITGC deficiencies related to IT policies and procedures.
- Approves accreditation of enterprise CFO-designated financial systems, if not already identified as the Designated Accrediting Authority (DAA). In this role, accept security risk identified during audits of CFO-designated financial systems, on behalf of the Department.
- Works with Component CIO to incorporate user requirements for new financial applications or upgrades to existing financial applications.
- Works with Component CIO to integrate and test Component-wide business continuity plan.
- Coordinates with Component CIOs to identify the financial data needed to be backed up and recovered.

2.18.4 Component CIO

The Component CIO is responsible for overseeing implementation and compliance of CFO-designated financial systems at the Component level. The Component CIO:

- Reviews and evaluates the Component's CFO-designated financial systems to ensure ITGCs are in place and working effectively.
- Works with the system owners to ensure remediation of ITGC deficiencies related to CFO-designated financial systems.
- Tracks and monitors progress of ITGC POA&Ms and remediation efforts at the Component level.
- Ensures completion of Memorandums of Understanding (MOUs) and Interconnection Security Agreements (ISAs) for CFO-designated financial system interconnections with any system not owned by DHS; ensures that they include appropriate security clauses; and monitors service provider for compliance with MOUs and ISAs.
- Implements the Department-wide system development lifecycle methodology and monitor user compliance with this methodology.
- As part of developing new financial applications or updating existing applications, integrates CFO feedback to ensure user requirement are adequately addressed.
- Develops and tests Component-wide disaster recovery plan. Coordinate with Component CFO to incorporate business continuity requirements and test on a periodic basis.
- Based on Component CFO requirements, executes policies for the routine backing up and recovery of financial data. Implements policies and procedures for rotating back-up media off-site.

2.18.5 System Owners

Systems owners are responsible for implementing and monitoring DHS policies, processes, and procedures related to the integrity of the data processed through the application and ongoing business processes. They are required to maintain the security of the technical and operational environment hosting the financial applications. Owners of CFO-designated financial systems:

- Work with Component ISSMs and their staffs to ensure CFO-designated financial systems are properly secured.
- Designate an ISSO as defined in Section 3.15, Directives 4300 and 4300A (draft).
- Ensure ITGCs are implemented and tested as required in DHS policy.
- Develop, implement, and test application controls, as appropriate.
- Ensure the completeness, accuracy, validity, and security of data inputs into, processed by, and output from the financial application.
- Ensure that Interconnection Security Agreements (ISA) are completed and enforced.
- Ensure that system POA&Ms are prepared and implemented with resources identified.
- Ensure resources are available for correcting weaknesses.
- Review and update the security of IT systems within their program area, in consultation with the Component CIO and ISSM, at least annually.
- Prioritize security weaknesses based on material weaknesses, external audits, and program assessments.
- Comply with Department system development life cycle methodology for new system implementations or modifications to existing systems.
- Participate in the developing and testing of disaster recovery plans for CFO-designated financial systems.

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of DHS IT resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

Component ISSMs will submit all security reports concerning DHS IT systems (major applications and general support systems) to the Component senior official or designated representative. ISSMs will interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. They will also answer data queries from the Compliance and Oversight Program Director and develop and manage information security guidance and procedures unique to Component requirements.

ISSOs are the primary points of contact for the IT systems assigned to them. They develop and maintain System Security Plans and are responsible for overall system security.

DHS Policy
a. Every DHS computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized IT system.
b. The CIO, in cooperation with each Component senior official, shall be responsible for ensuring that every DHS computing resource is designated as a part of an IT system (major application or general support system).
c. A System Security Plan shall be prepared and accurately maintained for each DHS IT system.
d. An ISSO shall be designated for every DHS IT system.
e. Component IT Security Programs shall be structured to support DHS and applicable FISMA and OMB requirements.
f. IT security reports regarding DHS IT systems shall be submitted to the Component senior official or designated representative.
g. The ISSO for each IT system shall serve as the POC for all security matters related to that system.
h. ISSMs shall ensure that their IT systems comply with the DHS Enterprise Architecture (EA) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO.

3.2 Capital Planning and Investment Control

DHS Policy
a. System owners shall include IT security requirements in their capital planning and investment business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP).
b. System owners or DAAs shall ensure that IT security requirements and POA&Ms are adequately

DHS Policy
funded, resourced and documented in accordance with current OMB budgetary guidance.
c. Component Investment Review Boards (IRBs) shall not approve any capital investment in which the IT security requirements are not adequately defined and funded.

3.3 Contractors and Outsourced Operations

DHS Policy
a. All statements of work and contract vehicles shall identify and document the specific security requirements for IT services and operations required of the contractor.
b. Contractor IT services and operations must adhere to all DHS IT security policies.
c. Requirements shall address how sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems, the background investigation and/or clearances required, and the facility security required.
d. Statements of work and contracts shall require that at the end of the contract, the contractor must return all information and IT resources provided during the life of the contract and must certify that all DHS information has been purged from any contractor-owned system used to process DHS information.
e. Components shall conduct reviews to ensure that the IT security requirements are included within the contract language and are implemented and enforced.
f. Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.

3.4 Performance Measures and Metrics

DHS Policy
a. Components shall define performance measures to evaluate the effectiveness of their IT security program.
b. Components shall provide quarterly and annual OMB FISMA data on their progress in implementing IT security performance measures.

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS IT Security Program and consists of two integrated elements:

- Continuity of Operations Planning (COOP)
- IT Contingency Planning (CP)

3.5.1 Continuity of Operations Planning (COOP)

DHS Policy
a. A standard DHS-wide process for continuity planning shall be developed, documented, and maintained in order to ensure continuity of operations under all circumstances
b. Components shall develop, test, implement, and maintain comprehensive COOPs to ensure the continuity and recovery of essential DHS functionality.
c. All COOPs shall be tested/exercised annually.
d. All CFO designated financial systems requiring high availability shall be identified in COOP plans and exercises.
e. All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.

3.5.2 IT Contingency Planning (CP)

DHS Policy
a. Guidance, direction, and authority for IT contingency planning activities for all DHS Components are centralized in the DHS Office of the CIO.
b. To ensure critical IT system availability under all circumstances, a standard DHS-wide process for IT contingency planning shall be developed, documented, and maintained.
c. Components shall implement and enforce backup procedures for all sensitive IT systems, data, and information. Recommended intervals are daily for incremental data backups and weekly for full data backups. System and application software should be backed up whenever modifications to the software make backups necessary.
d. The rigor of the IT system contingency planning, training, testing and capabilities shall be dependent upon the FIPS 199 defined potential impact level. The availability security objective alone shall be applied to the NIST SP 800-53 contingency planning (CP) controls defined for the low, moderate, and high potential impact level systems.
e. Comprehensive IT Contingency Plans to continue and recover critical DHS major applications and general support systems shall be developed, tested, exercised, and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the availability security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution.
f. When testing is required, IT Contingency Plans shall be tested/exercised annually.
g. All personnel involved in IT contingency planning efforts shall be identified and trained in the procedures and logistics of IT contingency planning and implementation as required.
h. Personnel involved in IT contingency planning efforts shall receive IT Contingency Plan training or refresher training annually.

3.6 System Development Life Cycle

DHS Policy
a. Components shall ensure that system security is integrated into all phases of the System Development Life Cycle (SDLC).
b. Components shall ensure that security requirements for sensitive IT systems are incorporated into life-cycle documentation.
c. All custom developed code shall be reviewed, approved and signed by the Program Manager prior to deployment into production environments. The Program Manager may delegate this authority to another DHS employee in writing. This authority shall not be delegated to contractor personnel.

3.7 Configuration Management

Configuration management (CM) relates to managing the configuration of all hardware and software elements within IT systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component shall utilize appropriate levels of configuration management.

CM will apply to all systems, subsystems, and components of the DHS infrastructure, thereby ensuing implementation, and continuing life-cycle maintenance. CM begins with base lining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline will be applied to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. The Change Control Board (CCB) will ensure that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process. Configuration management has security implications in three areas:

- Ensuring that the configuration of subordinate IT system elements are consistent with the certification and accreditation requirements of the parent system
- Ensuring that any subsequent changes, including an analysis of any potential security implications, are approved
- Ensuring that all recommended and approved security patches are properly installed

DHS Policy
a. Components shall prepare configuration management plans for all IT systems, as part of their SSPs.
b. Components shall establish, implement, and enforce configuration management controls on all IT systems and networks and address significant deficiencies as part of a Plan of Action and Milestones (POA&M).
c. IT security patches must be installed in accordance with configuration management plans and within the timeframe or direction stated within the Information Security Vulnerability Management (ISVM)

DHS Policy
message published by the DHS SOC.

3.8 Risk Management

Risk management is a process that allows system owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the IT systems and data that support their organization's missions.

DHS Policy
a. Components shall establish a risk management program in accordance with National Institute of Standards and Technology Special Publication (NIST SP) 800-30, <i>Risk Management Guide for Information Technology Systems</i> .
b. Components shall conduct and document risk assessments every three years, when high impact weaknesses are identified, or whenever significant changes to the system configuration or to the operational/threat environment have been made, whichever occurs first.
c. Special rules apply to CFO designated financial systems. See Section 3.15 for additional information.

3.9 Certification and Accreditation, Remediation, and Reporting

FISMA directs that all Federal agencies develop and implement a Department-wide information system security program designed to safeguard IT assets and data. DHS bases its C&A policy on the recommendations set forth in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Certification is the comprehensive testing and evaluation of the management, operational, and technical security features of an IT system. It primarily addresses software and hardware security safeguards; considers procedural, physical, and personnel security measures; and establishes the extent to which a particular design and implementation meets a specified set of security requirements.

Accreditation is the official management decision by the DAA, that authorizes the operation of an IT system. It includes explicitly accepting the risk to agency operations, assets, or individuals, based on the implementation of an agreed-upon set of security controls. The DAA accepts security responsibility for the operation of certified IT systems and officially declares that a specified IT system is approved to operate (ATO) based on these protections. DAAs shall be identified in TrustedAgent FISMA (TAF). The Component CIO will serve as the DAA for any system in which another DAA has not been appointed.

DHS Policy
a. Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) and shall apply NIST 800-53 controls specific to the security objective at the determined impact level. Impact levels shall be assigned according to the

DHS Policy
standards set in FIPS Pub 199, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , and following the guidance from NIST SP 800-60, <i>Guide for Mapping Types of Information and Information Systems to Security Categories</i> . DHS C&A policy is based on guidance from NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i> . [Note: See 4300A Sensitive Systems Handbook for information on the security objective(s) relevant to each of the NIST 800-53 controls.]
b. All Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, <i>Minimum Security Requirements for Federal Information and Information Systems</i> methodology, based on the impact level established for each security objective (confidentiality, integrity, availability). A minimum impact level of “ moderate ,” shall be assigned and a risk-based assessment shall be performed to determine whether the confidentiality security objective warrants being assigned an impact level of “ high ,” for all CFO designated financial systems and for systems processing or hosting personally identifiable information (PII).
c. Components should pursue type C&A for IT resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. Type C&A will consist of a master C&A package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.
d. The DAA for a system shall be identified in TrustedAgent FISMA. The Component CIO shall serve as the DAA when the system owner or an appropriate program official has not been named as the DAA.
e. Component ISSMs shall ensure that all new or major upgrades of existing sensitive IT systems and networks are formally certified through a comprehensive evaluation of their management, operational, and technical security features.
f. The certification, made as part of and in support of the accreditation process, shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.
g. Component ISSMs shall ensure that a risk assessment is conducted whenever any modifications are made to sensitive IT systems, networks, or to their physical environments, interfaces, or user community. SSPs shall be updated and re-certification conducted if warranted.
h. Components shall accredit systems at initial operating capability and every 3 years thereafter, or whenever a major change occurs, whichever occurs first.
i. DAAs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system must be certified and accredited in an Authorization to Operate (ATO) letter prior to passing the Key Decision Point 3 milestone in the development life cycle. IATOs are not appropriate for operational systems. The DAA may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension.

DHS Policy
j. If the system is not fully accredited and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.
k. As a result of IG auditing experience, components shall request concurrence from CISO for all accreditations for six months or less.
l. All DHS IT systems shall be accredited using the automated tools, TAF and RMS, approved by the DHS CISO.

3.10 IT Security Review and Assistance

DHS Policy
a. Components shall submit their IT security policies to the DHS CISO for review.
b. Components shall establish an IT Security Review and Assistance Program within their respective security organization.
c. Components shall conduct their reviews in accordance with FIPS 200/NIST SP 800-53, for specification of security controls. NIST SP 800-53A must be used for the assessment of security control effectiveness and for quarterly and annual FISMA reporting.
d. The DHS CISO shall conduct IT security review and assistance visits throughout the Department in order to monitor the Components' security program compliance with DHS policies and procedures.

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional areas convene on a regular basis.

3.11.1 DHS Information Systems Security Board

The DHS Information Systems Security Board (ISSB) consists of Component ISSMs and is chaired by the CISO. The ISSB is a decision-making body that considers a broad range of IT security matters of importance to the DHS IT Security Program.

DHS Policy
a. Component Information Systems Security Managers (ISSM) shall actively participate in the ISSB.
b. ISSMs shall ensure that the Component CIO is kept apprised of all pertinent matters involving the security of IT systems and that security-related decisions and information, including updates to the 4300 series of IT security publications, are distributed to the ISSOs and other appropriate persons.

3.11.2 DHS IT Security Training Working Group

The DHS IT Security Training Working Group is established to promote collaboration on IT security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby saving costs and avoiding duplication

of effort. The IT Security Training Working Group is chaired by the DHS Program Director for IT Security Training.

DHS Policy
a. Components shall appoint a representative to the DHS IT Security Training Working Group.
b. Each representative shall be responsible for managing the Component's IT security training program.
c. Component members shall actively participate in the DHS IT Security Training Working Group.

3.11.3 DHS Wireless Security Working Group (WSWG)

The DHS Wireless Security Working Group (WSWG) coordinates and evaluates DHS-wide approaches to wireless security on behalf of the Wireless Management Office (WMO) and the CISO. The WSWG focuses on policy, planning, and risk management; wireless security in major IT programs; and risk assessment of emerging technologies. The group assists the CIO in formulating and coordinating Department-wide security policies and guidelines related to wireless services and technologies.

DHS Policy
The DHS CIO and Components shall designate representatives to the DHS Wireless Security Working Group (WSWG).

3.12 IT Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component heads are responsible for taking corrective actions when security incidents and violations occur and for holding personnel accountable for intentional transgressions. Each Component must determine how to best address each individual case.

DHS Policy
a. IT security-related violations are addressed in the <i>Standards of Ethical Conduct for Employees of the Executive Branch</i> and DHS employees may be subject to disciplinary action for failure to comply with DHS security policy, whether or not the failure results in criminal prosecution.
b. Non-DHS Federal employees or contractors who fail to comply with Department security policies are subject to having their access to DHS IT systems and facilities terminated, whether or not the failure results in criminal prosecution.
c. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

3.13 Required Reporting

The Federal Information Security Management Act (FISMA) requires that the status of the DHS IT Security Program be reported to the Office of Management and Budget (OMB) on a recurring basis.

DHS Policy
a. Components shall collect and submit quarterly and annual IT security program status data as required by FISMA.
b. Components shall utilize the automated tool approved for use by the DHS CISO.

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Department information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to personally identifiable information (PII). Questions concerning privacy-related policy should be directed to the DHS Privacy Office (privacy@dhs.gov; 571-227-3813). Please refer to the DHS Chief Privacy Officer web page for additional information.

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations also place requirements on agencies to protect PII, which is defined as information in a system or online collection that directly or indirectly identifies an individual (e.g., information about an individual's education, financial transactions, medical history, and criminal or employment history and information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records).

A Privacy Threshold Analysis (PTA) must be performed for IT systems to determine whether or not a full Privacy Impact Assessment (PIA) is required. The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the system's lifecycle.

3.14.1 Personally Identifiable Information (PII)

OMB M-06-16 (Protection of Sensitive Agency Information) requires that agencies protect PII that is physically removed from the agency location or that is accessed remotely. Physical removal includes both removable media as well as media within mobile devices (i.e., laptop hard drive).

General policies relating to PII are provided below. Additional PII-related policies are included in the following sections of the DHS 4300A *Sensitive Systems Handbook*:

- Section 3.9: Certification and Accreditation, Remediation, and Reporting. For systems involving PII, the confidentiality security objective shall be assigned an impact level of at least moderate.
- Section 4.8.2: Laptop Computers and Other Mobile Computing Devices. All information stored on any laptop computer or other mobile computing device is to be encrypted.

- Section 5.2.2: Automatic Session Lockout. Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after 20 minutes of inactivity.
- Section 5.3: Auditing. Policies on audit logs of computer-readable extracts of personally identifiable information from databases and on erasure of these extracts are provided.
- Section 5.4.1: Remote Access and Dial-in. Remote access of PII must be approved by the DAA. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. Restrictions are placed on the downloading and remote storage of PII accessed remotely.

DHS Policy
a. PII shall not be physically removed from a DHS facility without written authorization from the system DAA or person designated in writing by the DAA.
b. PII removed from a DHS facility shall be encrypted.
c. If PII can be physically removed from an IT system (printouts, CDs, etc), the System Security Plan shall document the specific procedures, training, and accountability measures in place to ensure remote use of the encrypted data does not bypass the protections provided by the encryption.

3.14.2 Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are required whenever a new IT system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the IT Program Manager as part of the system development lifecycle process. OMB Memorandum M-03-22 and DHS MD 0470.1 discuss the requirements for conducting PIAs.

DHS Policy
Privacy Impact Assessments shall be conducted as part of new IT system development or whenever an existing system is significantly modified.

3.14.3 Privacy Incident Reporting

Reporting of privacy incidents and incidents that may involve PII are a special case, subject to strict reporting standards and timelines. These types of incidents are reported using the Privacy Event Notification (PEN).

DHS Policy
a. Any Component discovering a suspected or confirmed incident must coordinate with the Component Privacy Office or PPOC and ISSM in order to evaluate and subsequently report the incident to the DHS SOC.
b. The Component Privacy Officer or PPOC, in cooperation with the ISSM, shall jointly evaluate the incident, but the ISSM is responsible for reporting the incident to the Component CSIRC/SOC (or directly to the DHS CSIRC if the Component does not have its own SOC/CSIRC).

DHS Policy
<p>c. The ISSM shall report ALL types of privacy incidents, whether or not they involve IT resources. This unitary reporting process shall remain in effect until each Component has a Privacy Office or PPOC who can fulfill the reporting duties.</p>
<p>d. DHS personnel must also report suspected or confirmed privacy incidents or incidents involving PII to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.</p>

3.14.4 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS IT system must be evaluated to determine whether or not e-authentication requirements apply.

E-authentication guidance is provided in the following:

- OMB M-0404: E-Authentication Guidance for Federal Agencies, December 16, 2003
- NIST SP 800-63: Electronic Authentication Guideline, April 2006

DHS Policy
<p>a. Components shall determine whether or not Government e-authentication security requirements apply to their systems allowing online transactions.</p>
<p>b. Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, E-Authentication Guidance for Federal Agencies.</p>
<p>c. Components shall implement the technical requirements described in NIST SP 800-63, <i>Electronic Authentication Guideline</i>, at the appropriate assurance level for those systems for which e-authentication requirements apply.</p>

3.15 DHS Chief Financial Officer Designated Financial Systems

DHS CFO designated financial systems are systems that require additional management accountability and effective internal control over financial reporting. This section provides additional requirements for these systems based on OMB Circular A-123, *Management's Responsibility for Internal Control (A-123)* Appendix A. These requirements are in addition to the other security requirements established in this document and other CFO developed financial system Line of Business requirements. *Wherever there is a conflict between this and other sections of this policy regarding requirements for CFO designated financial systems, this section takes precedence.*

These additional requirements provide a strengthened assessment process and management assurance on the internal control over financial reporting. The strengthened process requires management to document the design and test the effectiveness of controls over financial reporting. The system owner is responsible for ensuring that all requirements, including security

requirements, are implemented on DHS systems. Component ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

DHS Policy
a. System owners are responsible for ensuring that Security Test and Evaluation (ST&E) plans and security assessments of key security controls for CFO designated financial systems are completed annually. The assessment shall be performed during the first quarter of each fiscal year.
b. The DHS Chief Financial Officer (CFO) shall designate the financial systems that must comply with additional internal controls and the Office of the CFO shall review and publish this list during the fourth quarter of every fiscal year.
c. ISSMs shall ensure that semi-annual vulnerability assessments and verification of critical patch installations are conducted on all CFO designated financial systems. Vulnerability assessment shall be performed during the second quarter of each fiscal year.
d. All CFO designated financial systems shall be assigned a minimum impact level of “ moderate ” for confidentiality, integrity, and availability as described in Section 3.9.1 of the 4300A <i>Sensitive Systems Handbook</i> .
e. All security accreditations for CFO designated financial systems shall be approved and signed by the DAA <i>and</i> by the Component CFO.
f. System owners are responsible for ensuring that Disaster Recovery (DR) plans are created for <i>all</i> CFO designated financial systems requiring high availability and that each plan is tested annually, no later than the third quarter of each fiscal year.
g. ISSMs shall ensure that weekly incident response tracking is performed for all CFO designated financial systems.
h. ISSMs shall ensure that incidents related to CFO designated financial systems are reported to the Component CFO.
i. System owners are responsible for ensuring that risk assessments for all CFO designated financial systems are updated annually.
j. Financial application mission owners shall update CFO designated financial systems’ System Security Plans (SSP) annually. Key controls that address the relevant assertions for a material activity shall be identified in the SSP.
k. Component ISSMs must request a waiver from the DHS CISO if a key control weakness is identified for a CFO designated financial system and not remediated within 12 months.
l. Component CFOs shall ensure that a full-time dedicated ISSO is assigned to each CFO designated financial system. ISSOs should not be assigned collateral duties outside information security responsibilities. Designated financial system ISSOs may be assigned to more than one CFO designated financial system.

DHS Policy
<p>m. CFO designated financial system ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.</p>
<p>n. Component CFOs shall work with their Component ISSMs to approve any major system change to CFO designated financial system identified in the DHS inventory.</p>

4.0 OPERATIONAL POLICIES

4.1 Personnel

DHS systems face threats from a myriad of sources. The intentional and unintentional actions of system users can potentially harm or disrupt DHS systems and facilities and could result in the destruction or modification of the data being processed, denial of service, and unauthorized disclosure of data. It is thus highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

DHS Policy
a. Components shall designate the position sensitivity level for all Government positions that use, develop, operate, or maintain IT systems and shall determine risk levels for each contractor position.
b. Components shall ensure the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.
c. No Federal employee shall be granted access to DHS systems without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS MD 11050.2, <i>Personnel Security and Suitability Program</i> .
d. No contractor personnel shall be granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in DHS MD11055, <i>Suitability Screening Requirements for Contractor Employees</i> .
e. Only U.S. Citizens shall be granted access to DHS systems processing sensitive information. An exception to the U.S. Citizenship requirement may be granted by the Component senior official or designee with the concurrence of the Office of Security and the DHS CIO or their designees.

4.1.2 Rules of Behavior

DHS Policy
a. Components shall define rules of behavior for all IT systems and ensure that users are trained regarding these rules and are aware of the disciplinary actions that may result from violations.
b. Users shall sign rules of behavior prior to being granted IT accounts or access to any DHS IT systems or data.

4.1.3 Access to Sensitive Information

DHS Policy
System owners shall ensure that users of the IT systems supporting their programs have a valid requirement to access these systems.

4.1.4 Separation of Duties

Separation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

DHS Policy
Components shall divide and separate duties and responsibilities of critical IT system functions among different individuals to minimize the possibility that any one individual would have the necessary authority or system access to be able to engage in fraudulent or criminal activity.

4.1.5 IT Security Awareness, Training, and Education

DHS Policy
a. Components shall establish an appropriate IT Security Training Program for users of DHS systems.
b. DHS personnel and contractors accessing DHS IT systems shall receive initial training and annual refresher training, in security awareness and accepted security practices.
c. DHS personnel and contractors with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities prior to being granted access to DHS IT systems.
d. Components shall maintain training records, to include name and position, type of training received, and costs of training. IT awareness training must be completed before IT accounts are authorized.
e. Unless a waiver is granted by the ISSM, user accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training.
f. Components shall prepare and submit an annual training plan, outlining their plans for IT Security Awareness, Training and Education. This plan shall follow the guidance in the DHS Component Information Technology (IT) Security Awareness, Training and Education Plan template, issued by the DHS IT Security Training Office.
g. Training plans shall include awareness of internal threats and basic IT security practices.
h. Components shall prepare and submit IT security Awareness, Training, and Education statistics to the DHS IT Security Training Program Director on a quarterly basis. These statistics shall include: <ul style="list-style-type: none"> – Total number of personnel and number of personnel that have received awareness. – Total number of personnel with significant security responsibility and the number that have received role-based training. – The cost of any agency-provided IT security training or materials for the year. Components must also provide: <ul style="list-style-type: none"> – Brief descriptions of the awareness and training provided to personnel. – Information concerning how they have explained policies relating to Peer-to-Peer (P2P) file sharing to all system users.
i. Components shall provide evidence of training by submitting copies of training schedules, training

DHS Policy

rosters, training reports, etc., upon request of the DHS IT Security Training Office, or during onsite validation visits performed on a periodic basis.

4.1.6 Separation from Duty**DHS Policy**

a. Components shall implement procedures to ensure that system accesses are revoked for employees or contractors who leave the Component or are reassigned to other duties. Accounts for personnel on extended absences shall be temporarily suspended.

b. Components shall establish procedures to ensure that sensitive information stored on any media is transferred to an authorized individual upon termination or reassignment of an employee or contractor.

4.2 IT Physical Security**4.2.1 General Physical Access****DHS Policy**

a. Access to DHS buildings, rooms, work areas, spaces, and structures housing IT systems, equipment, and data shall be limited to authorized personnel.

b. Controls for deterring, detecting, restricting, and regulating access to sensitive areas shall be in place and will be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.

c. Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy.

d. Visitors must sign in upon entering DHS facilities, be escorted during their stay, and sign out upon leaving. Non-DHS contractors' access shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one year.

e. These requirements will extend to DHS assets, located at non-DHS facilities or non-DHS assets and equipment hosting DHS data.

4.2.2 Sensitive Facility**DHS Policy**

a. Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk should be determined in accordance with Departmental security policy.

b. Any sensitive information or data not suitable for public dissemination shall be secured in one of the following: a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons.

4.3 Media Controls

4.3.1 Media Protection

DHS Policy
<p>a. Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, or other storage prohibiting access by unauthorized persons) when not in use.</p>
<p>b. Components shall ensure that backup media are stored off site in accordance with their business continuity and IT Contingency plans.</p>
<p>c. DHS personnel and contractors are prohibited from using any non government issued removable media (USB drives, in particular) or connecting them to DHS equipment or networks or to store DHS sensitive information.</p>
<p>d. All DHS USB drives must be compliant with FIPS 140-2 and FIPS 197</p>

4.3.2 Media Marking

DHS Policy
<p>Media determined by the information owner to contain sensitive information should be appropriately marked in accordance with DHS MD 11042.1: <i>Safeguarding Sensitive but Unclassified (For Official Use Only) Information</i>.</p>

4.3.3 Media Sanitization and Disposal

DHS Policy
<p>a. Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.</p>
<p>b. Components shall maintain records of the sanitization and disposition of information systems storage media.</p>
<p>c. Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.</p>

4.3.4 Production, Input/Output Controls

DHS Policy
<p>a. Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.</p>
<p>b. These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.</p>

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

DHS Policy

Components shall provide adequate physical and IT security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST SP 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)

4.4.2 Telephone Communications

DHS Policy

Components shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior Component official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed over unsecured telephones.

4.4.3 Voice Mail

DHS Policy

Sensitive information shall not be communicated over nor stored in voice mail.

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

DHS Policy

Components shall carefully select the telecommunications protection techniques that meet their security needs, in the most cost-effective manner, consistent with Departmental and Component IT policies. Approved guided media techniques or approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.

4.5.2 Facsimiles

DHS Policy

a. Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.

b. Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.

4.5.3 Video Conferencing

DHS Policy

a. Components shall implement controls to ensure that only authorized individuals are able to

DHS Policy
participate in each videoconference.
b. Components shall ensure appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.
c. Video teleconferencing equipment and software shall be disabled when not in use.

4.5.4 Voice over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line.

DHS Policy
a. Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for their use. Any IT systems that employ this technology must be certified and accredited for this purpose with residual risks clearly identified in the Accreditation Package.
b. Voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.
c. Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every component of their voice over data networks.
d. Components shall ensure that physical access to voice over data network components is restricted to authorized personnel.

4.6 Wireless Communications

Wireless communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, IT systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols.
- Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)

- Radio Frequency Identification (RFID).

General policies pertaining to all wireless communications technologies are provided in this section. Policies more specific to wireless systems, wireless PEDs, wireless tactical systems, and RFID are provided in Sections 4.6.1, 4.6.2, 4.6.3, and 4.6.4, respectively.

DHS Policy
a. Wireless communications technologies are generally prohibited from use within DHS unless the appropriate DAA specifically approves a technology and application.
b. Components using PKI-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.
c. The DHS WMO shall be notified within 30 days of all wireless communications systems acquisitions.

4.6.1 Wireless Systems

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN), peer-to-peer wireless networks (i.e., ad hoc wireless networks), and IT systems that leverage commercial wireless services.

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. Annual security assessments shall be conducted on all approved wireless systems. Wireless security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.
b. Risk mitigation plans shall be developed to address wireless security vulnerabilities. These plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless system being approved for use.
d. System Security Plans shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure security solutions and secure connections to external interfaces are consistently enforced.
e. Legacy wireless systems that are not compliant with DHS IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception to policy from the CISO, as appropriate.

4.6.2 Wireless Portable Electronic Devices (PED)

Wireless PEDs include personal digital assistants (PDA), smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services (PCS) devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

Wireless PED policy and procedures are described more completely in Attachment Q2 (*Wireless Portable Electronic Devices*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. The use of wireless PEDs and accessory devices in areas where sensitive or classified information is discussed is prohibited unless specifically authorized by the DAA in writing.
b. Wireless PEDs shall not be connected physically or wirelessly to the DHS-wired core network without written consent from the DAA.
c. Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.
d. Wireless PEDs such as BlackBerry devices and smartphones shall implement strong identification, authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smartphones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to 10 minutes.
e. System Security Plans shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.
f. Wireless PEDs shall be operated only when current DHS Technical Reference Model (TRM)-approved versions of antivirus software and software patches are installed.
g. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.
h. Components shall maintain a current inventory of all approved wireless PEDs in operation.
i. Wireless PEDs shall be cleared of all information before being reused by another individual, office, or Component within DHS or before they are surplus; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.
j. Legacy wireless PEDs that are not compliant with DHS IT security policy shall implement a migration plan that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the CISO, as appropriate.
k. Personally owned PEDs shall not be used to process, store, or transmit sensitive DHS information.
l. The DAA shall approve the use of Government-owned PEDs to process, store, or transmit sensitive

DHS Policy

information.

m. The use of add-on devices such as cameras and recorders is not authorized unless approved by the DAA. Functions that can record or transmit sensitive information via video, IR, or RF shall be disabled in areas where sensitive information is discussed.

4.6.2.1 Cellular Phones

DHS Policy

Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO and the DHS Wireless Management Office. Under no circumstances shall classified information be discussed on cellular phones.
--

4.6.2.2 Pagers

DHS Policy

Pagers shall not be used to transmit sensitive information.

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures, etc). Most of these functions have no security.

DHS Policy

a. Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.

b. Functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.

c. Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used and shall be disabled whenever possible.

4.6.3 Wireless Tactical Systems

Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical system policy and procedures are described more completely in Attachment Q3 (*Wireless Tactical Systems*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. DAAs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.
b. Wireless tactical systems shall implement strong identification, authentication, and encryption.
c. Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless tactical system being approved for use.
d. Components shall maintain a current inventory of all approved wireless tactical systems in operation.
e. Legacy tactical wireless systems that are not compliant with DHS IT security policy shall implement a migration plan to outline the provisions, procedures, and restrictions for transitioning these systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the CISO, as appropriate.
f. The security configuration of Land Mobile Radio (LMR) subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.
g. All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.

4.6.4 Radio Frequency Identification (RFID)

Radio Frequency Identification allows wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

RFID policy and procedures are described more completely in Attachment Q4 (*Sensitive RFID Systems*) to the DHS 4300A Sensitive Systems Handbook.

DHS Policy
a. Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordinance, and personnel before deployment of the RFID technology.
b. Components shall limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control.
c. Components shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.
d. Components shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel

DHS Policy

outside the Component's physical perimeter.

e. When the RFID system is connected to a DHS data network, Components shall implement network security controls to appropriately segregate RFID network components such as RFID readers, middleware, and databases from other non-RFID network hosts.

f. Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.

4.7 Overseas Communications**DHS Policy**

Where required or appropriate, all overseas communications shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.

4.8 Equipment**4.8.1 Workstations****DHS Policy**

a. Components shall ensure that all unattended workstations are either logged off, locked, or use a password-protected screensaver, activated after 5 minutes of inactivity.

b. Components shall ensure that workstations are protected from theft.

4.8.2 Laptop Computers and Other Mobile Computing Devices**DHS Policy**

a. Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall be encrypted using FIPS 140-2-approved encryption. Passwords and smart cards shall not be stored on or with the laptop or other mobile computing device.

b. Laptop computers and other mobile computing devices in offices shall be secured when unattended via a locking cable, locked office, or locked cabinet or desk.

c. Employees shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device overseas.

4.8.3 Personally Owned Equipment and Software (Not owned by or contracted for by the Government)**DHS Policy**

a. Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the Designated Accrediting Authority (DAA).

DHS Policy
<p>b. Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component ISSM.</p>

4.8.4 Hardware and Software

DHS Policy
<p>a. Components shall ensure that the installation of hardware and software products meets the requirements specified in applicable DHS secure baseline configuration guides.</p>
<p>b. Components shall limit access to system software and hardware to authorized personnel.</p>
<p>c. Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.</p>
<p>d. Components shall manage systems to reduce vulnerabilities through vulnerability testing, promptly installing patches, and eliminating or disabling unnecessary services, if possible.</p>
<p>e. Maintenance ports shall be disabled and shall only be enabled during maintenance.</p>

4.8.5 Personal Use of Government Office Equipment and DHS IT Systems/Computers

DHS Policy
<p>a. DHS employees may use Government office equipment and DHS IT systems/computers for authorized purposes only. “Authorized use” includes limited personal use as described in DHS MD 4600.1, <i>Personal Use of Government Office Equipment</i>, and DHS MD 4900, <i>Individual Use and Operation of DHS Information Systems/Computers</i>.</p>
<p>b. Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties or cause degradation of network services. DHS users must comply with the provisions of DHS MD 4500, <i>DHS Email Usage</i>, and DHS MD 4400.1, <i>DHS Web and Information Systems</i>.</p>
<p>c. DHS users do not have any right to or expectation of privacy while using Government office equipment and/or DHS IT systems/computers, including Internet and email services.</p>
<p>d. The use of Government office equipment and DHS IT systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.</p>
<p>e. DHS users are required to sign rules of behavior prior to being granted IT accounts or access to DHS IT systems or data. The rules of behavior shall contain a “Consent to Monitor” provision and an acknowledgement that the user has no expectation of privacy.</p>
<p>f. Contractors or other non-DHS employees are not authorized to use Government office equipment or IT systems/computers for personal use, unless limited personal use is specifically permitted by the</p>

DHS Policy

contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 shall apply.
--

4.8.6 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines, etc) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on DHS networks.

DHS Policy

a. Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.
--

b. In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication <i>and</i> obtain a waiver or exception in accordance with Section 1.5, Exceptions and Waivers.

4.9 Security Incidents and Incident Response and Reporting

The DHS SOC is currently the central coordinating and reporting authority for all "For Official Use Only" (FOUO) information, Component SOC's and computer security incidents throughout the Department. The HSDN SOC is the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department. The DHS SOC works closely with the HSDN SOC, the DHS Office of Intelligence and Analysis (DHS I&A) and the DHS Chief Security Officer to coordinate security operations.

DHS Policy

a. Components shall establish and maintain a Component incident response capability.

b. Components shall report <i>significant incidents</i> to the DHS SOC as soon as possible via phone (703-921-6505) but not later than one hour from "validation," e.g. a security event being confirmed as a security incident. Other means of communication, such as the SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet), are acceptable, but the Component is responsible for <u>positively verifying</u> that the notification is received and acknowledged by the DHS SOC.
--

c. Significant HSDN incidents shall be documented with a preliminary report that will be provided to the HSDN GWO or DHS CSIRC within one hour. An initial report detail will be provided to DHS CSIRC within four hours. Subsequent updates and status reports will be provided to DHS CSIRC every 24 hours until incident resolution or when new information is discovered. Significant incidents are reported individually on a per incident basis and will not be reported in the monthly summary report. Refer to DHS 4300A Attachment H Section 2.6 for guidance.
--

d. Components shall report minor incidents on systems in the weekly incident report. SBU systems

DHS Policy
may report via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email to dhs.soc@dhs.gov . HSDN incidents will be documented in a summary report provided to the HSDN GWO or DHS CSIRC on a weekly basis
e. All reports must be classified at the highest classification level of the information contained in the document. Unsanitized reports are marked and handled appropriately. Refer to MD4300A Attachment F for guidance.
f. If a DHS Component has no incidents to report for a given week, a weekly “No Incidents” report shall be sent via the DHS SOC portal (https://soconline.dhs.gov) (Accessible only via the DHS Intranet). Components with no portal access will report minor incidents via email sent to dhs.soc@dhs.gov .
g. The DHS CSIRC shall report incidents to US-CERT, in accordance with the DHS SOC CONOPS, as they arrive. Components should not send incident reports directly to US-CERT.

4.9.1 Law Enforcement Incident Response

The DHS SOC will notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement will coordinate with the DHS SOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

DHS Policy
a. Components shall coordinate all external law enforcement involvement through the DHS SOC. Exceptions are only made during emergencies where time is critical to saving lives or protecting property. In cases of emergency notification, the Component will notify the DHS SOC as soon as possible, by the most expedient means available.
b. Components should obtain guidance from the DHS SOC before contacting local law enforcement.

4.10 Documentation (Manuals, Network Diagrams)

DHS Policy
a. Components shall ensure that IT systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.
b. Documentation shall be updated whenever system changes occur.
c. Documentation shall be kept on hand and be accessible to authorized personnel (including DHS auditors) at all times.
d. System documentation may be categorized as FOUO if deemed appropriate by the ISSM. This category shall not be used as a means to restrict access to auditors or other personnel.

4.11 Information and Data Backup

DHS Policy
Components shall implement and enforce backup procedures as part of their contingency planning.

4.12 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, fax machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive data and may also be connected to data communications networks.

DHS Policy
<p>a. The policies in this document, including C&A requirements, apply to any devices that process or host DHS data,</p>
<p>b. Component ISSMs shall determine whether or not automated process devices should be included as part of an IT system's C&A requirements.</p>

5.0 TECHNICAL POLICIES

The design of IT systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person having access to sensitive IT systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

DHS Policy
a. Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.
b. For IT systems requiring authentication controls, the IT system shall ensure that each user is authenticated before IT system access occurs.
c. For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after 90 days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after 45 days of inactivity.
d. DHS users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user's identity.
e. All user authentication materials shall be treated as sensitive material and shall carry a level as high as the most sensitive data to which that user is granted access using that authenticator.

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as smart cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

DHS Policy
a. In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.
b. The ISSO shall determine and enforce the appropriate frequency for changing passwords but in no case shall the frequency be less often than every 180 days.
c. DHS users shall not share personal passwords.
d. Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password must be approved by the appropriate DAA.
e. Scripted passwords shall not be used.

The use of a personal password by more than one individual is prohibited throughout the DHS. However, it is recognized that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

5.2 Access Control

DHS Policy
a. Components shall implement access control measures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.
b. Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. <i>Social Security Numbers shall not be used as login IDs.</i>
c. Users shall not provide their passwords to anyone, including system administrators.
d. Emergency and temporary access authorization shall be strictly controlled and must be approved by the ISSM prior to being granted.

5.2.1 Automatic Account Lockout

Components shall configure each IT system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts.

DHS Policy
a. Components shall implement and enforce an account lockout policy that limits the number of consecutive failed logon attempts to three.
b. Components shall configure systems to lock a user's account for 20 minutes after three consecutive failed logon attempts.

5.2.2 Automatic Session Termination

Components shall configure each IT system to deactivate any user session immediately and automatically following a specified period of inactivity, in such a way that will require the user to re-authenticate his identity before resuming interaction with the system.

DHS Policy
Components shall ensure that sessions on workstations, laptops, and PEDs are terminated after 20 minutes of inactivity.

5.2.3 Warning Banner

DHS Policy
a. IT systems internal to the DHS network shall display a warning banner stipulated by the DHS CISO.
b. IT systems accessible to the public shall provide both a security and privacy statement at every

DHS Policy
entry point.

5.3 Auditing

DHS Policy
<p>a. Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the IT System Security Plan. The audit record shall contain at least the following information:</p> <ul style="list-style-type: none"> – Identity of each user and device accessing or attempting to access an IT system – Time and date of the access and the logoff – Activities that might modify, bypass, or negate IT security safeguards – Security-relevant actions associated with processing. – All activities performed using an administrator’s identity.
<p>b. Audit records for financial systems or for systems hosting or processing PII shall be reviewed by the system administrator monthly. Unusual activity or unexplained access attempts shall be reported to the system owner and ISSM.</p>
<p>c. Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.</p>
<p>d. Components shall ensure that audit logs are recorded and retained in accordance with the Component’s Record Schedule or the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least 90 days.</p>
<p>e. Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SSP.</p>
<p>f. Computer-readable data extracts involving PII shall be erased within 90 days unless the information included in the extracts is required beyond the 90 days. Erasure of the extracts or the need for continued use of the data shall be documented by the Component Privacy Officer or PPOC.</p>

5.4 Network and Communications Security**5.4.1 Remote Access and Dial-In**

DHS Policy
<p>a. Data communication connections via modems shall be limited and shall be tightly controlled as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component ISSM.</p>
<p>b. Components shall ensure that remote access and approved dial-in capabilities provide strong</p>

DHS Policy
authentication and access control and audit and protect sensitive information throughout transmission. In addition, remote access solutions shall comply with the encryption requirements of FIPS 140-2, <i>Security Requirements for Cryptographic Modules</i> . Dial-up connections shall be centrally managed by each Component to ensure integrity of network security. Strong authentication for remote access should consider two-factor authentication.
c. The Risk Assessment and SSP shall document any remote access of PII, and the remote access shall be approved by the DAA prior to implementation.
d. Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption and two-factor authentication. Any two-factor authentication shall be based on agency-controlled certificates or hardware tokens issued directly to each authorized user.
e. Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SSP.

5.4.2 Network Security Monitoring

Security Monitoring, Detection and Analysis are key functions and are critical to maintaining the security of DHS information systems. Monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

DHS Policy
a. Components shall provide continuous monitoring of their networks for security events or outsource this requirement to the DHS SOC.
b. Components shall report any event that is a security incident to the DHS SOC.

5.4.3 Network Connectivity

DHS Policy
a. Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network component.
b. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnect service agreements.
c. Components shall document interconnections with other external networks with an Interconnection Security Agreement (ISA). Interconnections between DHS Components shall require an ISA when there is a difference in the security categorizations for confidentiality, integrity, and availability for the two networks. ISAs shall be signed by both DAAs or by the official designated by the DAA to have

DHS Policy
signatory authority.
d. ISAs shall be reissued every three years or whenever any significant changes have been made to any of the interconnected systems.
e. ISAs shall be reviewed as a part of the annual FISMA self-assessment.

5.4.4 Firewalls

DHS Policy
a. Components shall restrict physical access to firewalls to authorized personnel.
b. Components shall implement strong identification and authentication for administration of the firewalls.
c. Components shall encrypt remote maintenance paths to the firewalls.
d. Components shall conduct quarterly testing to ensure that firewall configurations are correct.
e. Component SOCs shall ensure reports on security operations status and incident reporting are provided to the CISO Security Operations Program Director as required.

5.4.5 Internet Security

DHS Policy
a. Any direct connection of DHS networks to the Internet or to extranets must occur through firewalls that have been certified and accredited.
b. Firewalls shall be configured to prohibit any protocol or service that is not explicitly permitted.
c. Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by an appropriate senior official prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be “Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS IT systems.”]
d. Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by the Component shall be used instead.
e. File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange, etc.) and is approved by the Component shall be used instead.

5.4.6 Email Security

The DHS email gateway Steward provides email monitoring for spam and virus activity at the gateway.

A relationship has been established between the email Steward and the DHS SOC to enable communications. DHS SOC personnel will be trained to respond to incidents pertaining to email security and will assist the email Steward as necessary.

DHS Policy
Components shall provide appropriate security for their email systems and email clients by:
a. Correctly securing, installing, and configuring the underlying operating system.
b. Correctly securing, installing, and configuring mail server software.
c. Securing and filtering email content.
d. Deploying appropriate network protection mechanisms, such as: <ul style="list-style-type: none"> – Firewalls – Routers – Switches – Intrusion detection systems.
e. Securing mail clients.
f. Conducting mail server administration in a secure manner. This includes: <ul style="list-style-type: none"> – Performing regular backups – Performing periodic security testing – Updating and patching software – Reviewing audit logs at least weekly.

5.4.7 Personal Email Accounts

DHS Policy
DHS employees or contractors shall not transmit FOUO information to any personal email account.

5.4.8 Testing and Vulnerability Management

The DHS SOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information Security Vulnerability Management (ISVM) messages, and conducting Vulnerability Assessments (VA).

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security

advisories, and system security testing such as automated vulnerability scanning or security tests and evaluations (ST&E).

A core element of vulnerability management is mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

DHS Policy
<p>a. Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on IT systems containing sensitive information annually or whenever significant changes are made to the IT systems. This should include scanning for unauthorized wireless devices. Evidence that annual assessments have been conducted should be included with Security Assessment Reports (SAR).</p>
<p>b. ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SDLC support.</p>
<p>c. Anyone within DHS may request to be added to the ISVM distribution list. Those wishing to be added must provide a DHS email address and obtain management approval. ISVMs contain sensitive, "For Official Use Only," information and must not be forwarded to non-DHS email accounts.</p> <p>Although ISVM messages can be sent to anyone, <i>only Component ISSMs</i> or their designated representatives may acknowledge receipt of messages, report compliance with requirements or notify the granting of waivers.</p>
<p>d. Components should report compliance with the ISVM message within the specified timeframe. Components unable to meet the designated compliance timeframe must submit documentation of a waiver request via the DHS SOC Online Portal (https://soconline.dhs.gov)</p>
<p>e. ISSMs shall ensure coordination among the DHS SOC, the Component SOC, and the Information Security Vulnerability Management (ISVM) Program when vulnerability assessment responsibilities encompass more than one Component.</p>

5.4.9 Peer-to-Peer Technology

DHS Policy
<p>Peer-to-peer software is not authorized on DHS computers or on any computer or IT system that might be connected to the DHS network.</p>

5.5 Cryptography

Cryptography is a branch of mathematics that is based on the transformation of data. Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Cryptography relies on two basic components: an algorithm (e.g., Advanced Encryption Standard [AES]) and a key. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

There are two basic types of cryptography: secret key systems (also call symmetric systems) and public key systems (also called asymmetric systems). In secret key systems, the same key is used for both encryption and decryption; that is, all parties participating in the communication share a single key. In public key systems, there are two keys: a public key and a private key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

Refer to NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, for more in-depth information on cryptography.

A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the originator did in fact sign the message. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key that corresponds to, but is not the same as, the private key. The security of a digital signature system is dependent on maintaining the secrecy of users' private keys.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

DHS Policy
<p>a. Components shall identify IT systems transmitting sensitive information that may require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:</p> <ul style="list-style-type: none"> – Products using Advanced Encryption Standard (AES) algorithms that have been validated under FIPS 140-2. (Note: The use of triple DES [3DES] and FIPS 140-1 is no longer permitted. A waiver is required for systems where AES cannot currently be used.) – NSA Type 2 or Type 1 encryption.
<p>b. Components shall develop and maintain encryption plans for their sensitive IT systems.</p>
<p>c. Components shall use only cryptographic modules that have been validated in accordance with FIPS 140-2.</p>

5.5.2 Public Key Infrastructure

A public key infrastructure (PKI) is an architecture that provides the means to bind public keys to their owners' private keys and helps in the distribution of reliable credentials in large heterogeneous networks. Public keys are bound to their owners by public key certificates. These certificates, which contain information such as the owner's name and the associated public key, are issued by a reliable certification authority (CA). Reliable identification of individuals is an inherently governmental activity. In order to establish and maintain the trust required to support DHS missions, the root certificate must be controlled by the DHS.

Any DHS Component that implements a PKI or CA for a PKI must ensure that its CA is subordinate to the DHS Root CA. The use of self-signed certificates has minimal security value and violates Executive Office Directives. The use of any non-DHS service provider for CA or PKI support is inconsistent with DHS Mission requirements and must be approved by the CISO.

DHS Policy
a. PKI policy oversight shall be provided at the Department level by a PKI Policy Authority (PKI PA). The CISO shall be the PKI PA.
b. PKI operational oversight shall be provided at the Department level by a PKI Operational Authority (PKI OA) appointed by the PKI PA.
c. The DHS PKI shall be governed by a DHS X.509 Certificate Policy (DHS CP). The DHS CP shall be approved by the PKI PA.
d. The DHS CP must comply with the U.S. Federal PKI Certificate Policy for the Federal Bridge CA, at the high, medium, and basic assurance levels.
e. DHS shall have a single High Assurance Root CA. All additional CAs within DHS must be subordinate to the DHS Root CA. The requirements and process for becoming a subordinate CA to the DHS Root CA shall be specified in the DHS CP.
f. The DHS Root CA shall cross-certify with the Federal Bridge CA at the high, medium, and basic assurance levels.
g. Every DHS CA shall operate under an X.509 Certificate Practices Statement (CPS). The CPS for each CA must comply with the DHS CP. The DHS PKI PA must approve each CPS.
h. All DHS CAs shall undergo a compliance audit on a regular basis as required by CP. The DHS PKI PA shall specify a DHS PKI Auditor to review compliance audits.
i. All operational PKI facilities should be established in accordance with the requirements commensurate with the CA's assurance level as well as its intended use. Location/protection of the authority will be determined by its level of assurance. Measures to ensure continuity of operations of the certificate authority should be taken that are at least equal to the measures of the system being supported.
j. A DHS PKI archive facility shall be established to store PKI records, as required by the CP and CPSs.
k. Certificates that are issued by test, pilot, third party, or other CAs in DHS and that are not established as a subordinate CA to the DHS Root CA shall not be used to protect sensitive DHS data, or to authenticate to DHS operational systems containing sensitive data.

5.5.3 Public Key/Private Key

The recipient of public key certificates is referred to as a subscriber. A subscriber can be a human (e.g., an employee or contractor), an organization, an application, a code signer (e.g., digitally signs released software to enable users to authenticate its source, legitimacy, and integrity), or a device (e.g., a web server or VPN server.) Registrars are trusted PKI officials

who administer the process that results in a CA issuing or revoking public key certificates for each subscriber. As part of the PKI registration process, a public key/private key pair is generated in a hardware or software cryptographic module that is under the control of the subscriber. The private key remains under the sole possession of the subscriber. A CA enters the public key into an electronic public key certificate that also identifies the owner of the key, i.e. the subscriber. The trusted CA digitally signs the certificate thereby binding the public key to the subscriber, and makes the signed certificate available for use by other subscribers.

A subscriber's public key certificate is used by other subscribers, referred to as relying parties, to obtain the subscriber's public key in a trusted manner. Once obtained, the public key is then used: (1) to encrypt data for that subscriber so that only that subscriber can decrypt it with their private key, or (2) to verify that digitally signed data was signed by that subscriber using their private key, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data.

DHS Policy
a. Separate public/private key pairs must be used for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.
b. Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.
c. A human sponsor shall represent each organization, application, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.
d. A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, organization, application, code signer, or device to receive one or more certificates.
e. A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the authorized human sponsor for each organization, application, code signer, or device.
f. Human subscribers shall be responsible for the security of and use of their private keys. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.
g. The sponsor of an organization, application, code-signing, or device subscriber shall be responsible for the security of and use of the subscriber's private keys.
h. Ensure that only private keys that correspond to a public key on a certificate issued to an organization or code-signing subscriber are authorized to be used by more than one person. If more than one person is authorized to use the key, ensure that auditable records are kept to maintain individual accountability for each use of the private key.
i. Every human subscriber shall read, understand, and sign a DHS PKI Subscriber Agreement for Human Users as a pre-condition for receiving certificates from a DHS CA.
j. Every sponsor shall read, understand, and sign a DHS PKI Subscriber Agreement for Sponsors as a

DHS Policy

pre-condition for receiving certificates from a DHS CA for the nonhuman subscriber they sponsor.
--

5.6 Virus Protection

DHS Policy

a. ISSMs shall establish and enforce Component-level virus protection control policies.
--

b. Components shall implement a defense-in-depth strategy that:
--

- | |
|---|
| <ul style="list-style-type: none"> – Installs antivirus software on desktops and servers – Configures antivirus software on desktops and servers to check all files, downloads, and email – Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update – Installs security patches to desktops and servers in a timely and expeditious manner. |
|---|

c. Components may implement appropriate file/protocol/content filtering to protect their data and networks in accordance with their Internet usage policy.

5.7 Product Assurance

DHS Policy

a. Information Assurance (IA) shall be considered a requirement for all systems used to enter, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.
--

b. <i>Strong preference</i> shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following:

- | |
|---|
| <ul style="list-style-type: none"> – The NIST FIPS validation program. – The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program – The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement |
|---|

c. The evaluation and validation of COTS IA and IA-enabled IT products shall be conducted by accredited commercial laboratories or by NIST.
--

6.0 DOCUMENT CHANGE REQUESTS

Changes to this DHS Sensitive Systems Policy Directive 4300A and to the DHS 4300A Sensitive Systems Handbook can be requested by filling out the form included as Attachment P to the handbook.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS IT security policies or procedures, contact the DHS Director for IT Security Policy at INFOSEC@dhs.gov.

ATTACHMENT E

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

Deployment Strategy

Pages 893 through 1097 redacted for the following reasons:

b2High

ATTACHMENT F

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

Process Flows

Pages 1099 through 1293 redacted for the following reasons:

b2High

ATTACHMENT G

**Bed Space, Transportation, and Detainee
Location Tracking Automation
(BST&T)**

DOCUMENTATION ARTIFACTS

**U.S. Immigration and Customs
Enforcement (ICE)**

Office of the CIO



**U.S. Immigration
and Customs
Enforcement**

**Sample Field Office
Documentation**

Pages 1307 through 1362 redacted for the following reasons:

b2High

ICE DRO and JPATS Documentary Requirements

(Updated December 5, 2006)

Purpose

The purpose of this document is to outline the policy governing Immigration and Customs Enforcement (ICE) Detention and Removal Operations (DRO) use of Justice Prisoner and Alien Transportation System (JPATS). These requirements will be appended into Appendix 16-7 of the DRO Policy and Procedures Manual, Chapter 16.

Guidelines

JPATS is managed by the Department of Justice (DOJ) United States Marshals Service (USMS). USMS, the Bureau of Prisons (BOP), and ICE utilize JPATS services, with ICE being the major stakeholder. The services performed by JPATS for ICE are the providing of safe, secure transportation of persons and property. As such, case management for ICE movements remain the responsibility of DRO, which will receive, process, transport, handle property for, and maintain custody of all aliens moved via JPATS aircraft. ICE detainees traveling on JPATS aircraft continue to remain in DRO custody. While JPATS is responsible for transporting DRO detainees, the sending DRO field offices retain responsibility for case management, custody, and resolution of any issues that may arise until completion of the movement. Movements via JPATS often include requirements requested by HQDRO's Detention Operations Coordination Center (DOCC) to ensure efficient management of ICE detention resources. All DOCC movements must be coordinated with HQDRO DOCC.

Scheduling ICE/DRO Movements via JPATS

The following are personnel involved in the coordination of JPATS movements. ICE/DRO JPATS Liaison Officers are the Air Transportation Unit (ATU) staff located in the Kansas City, MO office. They are responsible for the coordination and resolution of issues relating to movements using JPATS and may be contacted at [REDACTED]. Additional contact information may be found on the ATU website found within <https://dhsonline.dhs.gov/>.

Personnel

Air Transportation Unit (ATU) - The ATU within the Removal Management Division of DRO is responsible for managing and coordinating all ICE/DRO JPATS and charter movements. ATU offices are located in Washington, D.C. and Kansas City. ATU is responsible for policy issues relating to these movements, as well as for the liaison and coordination of ICE/DRO JPATS flights.

ICE/DRO JPATS Liaison Officers - JPATS Liaison Officers are the ATU staff located in the JPATS office in Kansas City, MO. These officers are responsible for the coordination and resolution of issues relating to ICE/DRO movements using JPATS.

Prisoner Transportation Specialists - Prisoner Transportation Specialists are the scheduling personnel for all DRO JPATS missions. They are also located in Kansas City. The Transportation Specialists are JPATS employees and are responsible for the scheduling and monitoring of all DRO JPATS missions. They may also be contacted at the numbers listed above.

Security Officer in Charge (SOIC)- The SOIC's are JPATS employees responsible for overseeing the rear cabin crew and detainees, communicating with JPATS regarding the progression at each leg of the flight, communicating with JPATS as to any changes to the manifest and itinerary, ensuring required documents are correctly completed before dissemination to appropriate parties, coordination of aircraft security matters, and advising the flight crew when exchange operations are complete for continuation of the flight mission.

Ground Officer in Charge (GOIC) - At each JPATS detainee exchange location the DRO coordinator will designate a GOIC who will take direction from the SOIC. The GOIC is responsible for identifying and assigning ground personnel and establishing communication with airport security and the SOIC.

ICE/DRO Immigration Enforcement Agent (IEA) Liaison Officer on JPATS Aircraft - IEA's are responsible for reviewing all required documentation to ensure completion within the established guidelines. IEA's also identify and verify required documentation and property for detainees on all continental United States (CONUS) and outside the CONUS (OCONUS) flights.

Pilot in Command (PIC) - The PIC is responsible for flight operations to include all matters relating to flight safety and service of the aircraft. The PIC is responsible for notifying the SOIC of any unscheduled stops due to weather or mechanical difficulties.

Loading-Offloading Operations

Preparation - It is the responsibility of each field office to ensure that the ground security personnel are staged at least 30 minutes prior to the scheduled arrival time of JPATS aircraft.

Alien Exchange Vehicles - When the aircraft comes to a complete stop and the engines have been shut down, the GOIC and the SOIC will coordinate the positioning of all alien exchange vehicles. Consideration is to be given to visibility and perimeter control and a minimum 50-foot distance must be maintained from the loading stairs of the aircraft. Ground vehicles must not be parked directly towards or away from the aircraft for safety reasons. The preferred method of parking is bumper-to-bumper to ensure a secure perimeter around the aircraft. When possible, vehicles should be turned off in order to avoid potentially dangerous situations.

Security Procedures - The SOIC and PIC will determine a safe distance from the aircraft for ICE vehicles during landings and take offs. The SOIC will give the order to disembark crewmembers for ground security. The alien exchange process will not begin until a secure perimeter is established. When CONUS, armed personnel will challenge and identify all persons approaching the alien exchange location and will prohibit entry by unauthorized personnel or vehicles into the area. In the event of an escape attempt,

security personnel must use extreme caution in preventing the escape. Weapons must not be discharged toward the aircraft or in the direction of the secured perimeter. All use of force actions will be according to ICE policy and procedures. Armed personnel will not participate in any alien exchange operation inside the secured perimeter. Failure to comply will result in the cessation of prisoner/alien exchanges. Ground security personnel will not depart from the alien exchange location until the JPATS-owned or leased aircraft is airborne. No one is to board the aircraft without clearance from the PIC and the SOIC. Authorization to depart early must be obtained from the SOIC.

Boarding Requirements

- **Searches:** All detainees will be thoroughly searched prior to being brought to the prisoner/alien exchange location. Security personnel will pat down search the detainees before they are accepted for boarding.
- **Carry-on Items:** Unless specified differently in this document, items such as cash, books, valuables, religious items, and legal material will generally be placed with the detainee's property to be shipped on the aircraft. Detainees with carry-on coats, jackets, or sweaters will have those items returned to the delivering agency, office or ICE facilities for disposition. During inclement weather, each field office will be responsible for providing an adequate supply of coats and/or blankets for use during detainee exchanges.
- **Clothing:** Detainees are limited to one set of clothing on their body.
- **Footwear:** All persons boarding the aircraft are required to wear footwear. For safety reasons, high-heeled boots and shoes are not acceptable on the aircraft.
- **Jewelry:** Detainees will be permitted to wear a plain wedding band. All other jewelry, including religious medallions, must be packaged with the detainee's property. All ICE detainees departing the country the same day are permitted to keep money and jewelry on their person.
- **Eyeglasses:** Two pairs of prescription eyeglasses and one soft eyeglass case (without metal inserts) or hard paper case will be permitted if carried on-person.
- **Contact Lenses:** All contact lens cases in the possession of the detainees will be turned over to PHS medical personnel or the SOIC and placed in personal property.
- **Hair:** No detainee will be permitted to board with his/her hair bound with any object (rubber bands, ponytail holders, string, bobby pins, beads, etc.). No hair decorations are permitted. Wigs will be permitted for a valid medical reason (hair loss due to chemotherapy, etc.). Only disposable religious headgear is permitted in transit.
- **Accessories:** Belts, suspenders, bootstraps, chains, neckties, scarves, hats, caps, or gloves are not permitted.

- **Removal of Pierced Items From Detainees:** Neither JPATS security personnel nor U.S. Public Health Service (PHS) flight nurses will remove any foreign bodies jewelry, studs, metal pieces, etc. implanted in the skin or body of a detainee. All foreign bodies implanted in the skin or bodies of detainees scheduled to travel via JPATS must be removed at a medical facility and/or by trained medical personnel prior to travel.
- The removal of such items can potentially cause infection and/or injury to the detainee and must never be attempted outside a proper medical setting. The sending office is responsible for ensuring that any detainee moved via JPATS has no medically unnecessary foreign bodies implanted in his/her skin or body. The SOIC will make the final decision for rejection/acceptance of detainees with foreign bodies implanted in their skin or bodies that might be used as a potential weapon or an escape device.

Documentation Required for All ICE DRO JPATS Movements

- All movements must be authorized and coordinated by ATU, and the ICE DRO sending and receiving field offices.
- Six (6) copies of Form I-216, Record of Persons and Property Transferred shall accompany all movements on JPATS.
- An I-770, Notice of Rights and Request for Disposition, shall accompany all juveniles.
- A medical summary prepared by the sending facility's medical staff must accompany each detainee. This requirement may be waived by ATU in certain circumstances where the alien has been apprehended within 72 hours prior to the date of the flight and has not been processed through an ICE DRO facility.
- The JPATS flight nurse will conduct a visual screening consistent with current JPATS policy and procedure on those detainees lacking Tuberculosis (TB) documents who are delivered to the aircraft. Any ICE detainee who fails to pass screening by a flight nurse and is suspected of having active TB will be denied boarding and will be referred to a facility for screening. For those detainees for whom TB testing has been completed, USM Form 553, Medical Summary of Federal Prisoner/Alien in Transfer, or equivalent, will be required.
- Facility medical staff must clear the transfer of detainees with special medical needs or psychiatric conditions.
- In all movements, all aliens must have a completed I-213, Record of Deportable/Inadmissible Alien, with a clear and current photo. In the case of a Bureau of Prisons (BOP) flight, four photos and two sets of fingerprints are required.
- In all movements aliens must be entered into ENFORCE/IDENT before being transported. This must be noted and the FINS numbers entered on the I-216.
- In all movements, aliens possessing property are limited to one bag, suitcase or box weighing no more than 40 pounds. There must be a completed I-77, Baggage Check, for the item. The I-77 number must be noted on the I-216.

- For removal flights departing foreign from the staging location, the I-205s, Warrant of Removal/Deportation, and I-296s, Notice to Alien Ordered Removed/Departure Verification, will be completed by the DRO officers verifying departure of the aircraft from the staging location. Field Offices are to ensure an envelope with the Docket Control Office's address is provided to the Field Office verifying departure/removal.
- All ICE personnel conducting JPATS operations will wear the approved class of ICE uniform as set by the local Field Office Director. Hats or caps will not be worn on JPATS flights for safety reasons. Exceptions to the uniform requirements may be made for personnel who will be meeting with foreign officials to conduct negotiations or liaison activities. These personnel will dress, at a minimum, in business casual attire or as appropriate for the occasion.

Additional information, to include a checklist of required items prior to transferring detainees, may be found in the ICE Detention Standard, "Detainee Transfer" in the *Detention Operations Manual*.

Additional Documentary Requirements According to Type of Movement

Aliens Scheduled to Depart the United States Foreign:

- This includes Administrative Voluntary Returns (VR) to Mexico, Expedited Removals (ER), and other Aliens Subject to an Administratively Final Order of Removal/Deportation.
- Completed I-205/I-296, as applicable, with clear and current photo and clear right index fingerprint. It is recommended that the office address be stamped on the I-205/I-296 to facilitate the return of the executed document.
- Original travel document with photo, as required. Travel document may not be required for *special removal* cases pre-arranged by HQDRO (i.e. Haiti, Cambodia, etc.).
- Individuals leaving the United States the same day as the JPATS movement must retain possession of money and valuables/jewelry.
- For aliens transferred for staging for a later scheduled repatriation mission (Removal other than same day of movement via JPATS):
 - Money and jewelry are to be placed into separate plastic seal-a-meal with G-589, Property Receipt, for each. Money must be fanned out and stapled for visual verification of amount. Coins should be taped and fanned out using a clear tape for visual verification.
- Mexican VRs must also have an I-94, Arrival/Departure Record.

Aliens Being Transferred From One ICE Office to Another (Not yet ready for removal):

- This includes new Notice to Appear (NTA) cases, ER cases pending court, Final Order cases pending travel documents, Change of Venue, and Room and Board (R&B) cases.
- The sending field office will comply with the ICE Detention Standards regarding Detainee Transfer.
- Appropriate documents, such as NTAs (I-862), must be properly served on the alien by the sending office.
- The detainee's A-file must accompany the alien. For R&B cases, only a work folder with applicable case specific documentation is required.
- Money and jewelry are to be placed into separate plastic *seal-a-meal* (or similar packaged see-through bag) with a completed G-589, Property Receipt, for each. Money must be fanned out and stapled for visual verification of amount. Coins should be taped and fanned out using a clear tape for visual verification.

Aliens transferred on the USMS/BOP airlift:

- Refer to the above requirements depending on the type of case.
- Property is limited to BOP standards of 40 lbs in a 14"x14"x19" size box per person.
- Aliens are permitted to have a check in any amount and/or cash not to exceed \$50.00 United States Dollars. The alien number must be on the check.
- Copy of travel document, if applicable.
- I-217, Information for Travel Document or Passport.
- Four sets of photos and two sets of fingerprints.
- Criminal history, judgment and commitment records.

Waiver of Documentary Requirements

Waiver of documentary or informational requirements may be obtained only from ATU. The requesting office must articulate the reason(s) for which such waiver may be warranted. Examples warranting a waiver may include urgent operational requirements to transport large numbers of newly apprehended aliens, natural disasters requiring emergent movements, or the inoperability of computer databases such as IDENT. The requesting office must obtain concurrence from the receiving field office before submitting the request to the ATU.

The concurrence must be documented on all I-216s related to the specific movement. Information must include the name of the officer at the receiving office who approved the request. In all instances, officer-safety and medical information must be provided to ATU officers in Kansas City so that it may be timely relayed to JPATS crews. In those instances where medical documentation is unavailable, the sending office must submit a statement that the detainee is not exhibiting any medical symptoms and does not pose any health risk to officers who take custody of the detainee.

Special Interest Cases:

Field offices must ensure compliance with HQDRO memoranda, *Pre-Removal/Release Record Checks and Related Procedures* (July 18, 2006) and *Headquarters Detention and Removal Operations Special Interest Cases* (November 6, 2006).

Fugitives and/or Cases of Special Interest

If an alien is a special interest case or a fugitive in his home country appropriate annotation must be made in the "Status" column of the I-216. If a warrant of arrest has been confirmed through INTERPOL or through other law enforcement agencies, the field office shall obtain a copy of the warrant and fax that copy to the ATU in Washington, DC and Kansas City. This will ensure that appropriate notifications are made to receiving governments. If no warrant is available, then copies of documentation received by the field from overseas entities confirming the alien is wanted must be sent. The alien's file must have a cover sheet that clearly identifies it as a special case that requires special handling. Country clearance cables must be sent at least five business days in advance. Information relating to any international arrest warrants should be made known to the ATU at least five business days prior to the mission.

Violent and Escape Risk Aliens

Advance notification must be provided to the ATU in the "Afflicted/Dangerous" column of the I-216 for those individuals being transported by JPATS who have exhibited or threatened violence and for whom special custody conditions are required, and for those aliens who have gang affiliation. Available supplemental information must also be provided to ATU.

Field offices are to ensure a summary of the case is forwarded timely to appropriate HQDRO units, including ATU, Custody Determination Unit, and Travel Document Unit prior to scheduling.

Medical Cases

Psychological Issues: Those cases requiring psychological care should be identified on the I-216 as 'special handling' cases in the "Afflicted/Dangerous" column. ATU Kansas City must be made aware of these cases so that proper notifications can be made to receiving countries. Detainees who are taking prescribed psychotropic medications must be transferred with their medications and sufficient documentation to allow proper monitoring and treatment of their conditions. Detainees on active suicide watch will be refused boarding unless prior approval has been obtained from the Prisoner Transportation Nurse, and the ICE SOIC.

Pregnant Detainees: Pregnant detainees who are in the first two trimesters of pregnancy may travel via JPATS providing there have been no complications with the pregnancy. Those individuals in their third trimester may travel only if the detainee has a written statement from an ICE-contracted physician or PHS official authorizing travel by aircraft and the alien is not experiencing any medical problems at the time of boarding. The statement must be dated within 72 hours of the scheduled movement.

Tuberculosis (TB) Screening/Testing: Detainees presented for boarding on a JPATS aircraft must have a full TB screening documented in USM Form 553 or ICE equivalent. All standard JPATS policy and procedure will be followed as applicable. In accordance with the ICE National Standards (referencing the *Detention Operations Manual* "Medical Care" and "Detainee Transfers" sections located at <http://www.ice.gov/partners/dro/opsmanual/index.htm>) aliens/detainees will be screened for TB by a tuberculin skin test (PPD) or chest x-ray (CXR) upon admission to all Service Processing Centers (SPCs), all ICE Contract Detention Facilities (CDFs), and all Intergovernmental Service Agreements facilities (IGSAs – state or local government facilities that hold ICE aliens/detainees for greater than 72 hours). Results must be documented on USM-553 or equivalent. DRO detainee(s) whom have not been processed and/or newly arrested detainees might not have completed TB screening; therefore, a USM-553 might not be available. Detainees who *have been screened* by PPD or CXR must have results documented on USM-553. The flight nurse will check for evidence of a positive PPD on those whom *have* had skin tests placed but not yet evaluated; and will symptom screen those whom *have not* had the screening process initiated. Detainees with a positive PPD skin test will be required to have a normal CXR for clearance to fly. Those with a positive (abnormal) CXR will be required to have three separate negative AFB Smear (sputa) reports for clearance to fly. Any Alien/Detainee who fails to pass symptom screening by a flight nurse will be declined boarding and be referred back to the originating facility for further medical evaluation.

The flight nurse will be the primary individual to determine suitability of a detainee's health status to board a JPATS aircraft; discrepancies are to be discussed with the Aero-Medical Branch Chief or designee. Policies, procedures, and directives are subject to review and revision to ensure applicability of current national guidelines, standards of care, and mission needs.

Prescription Medication: *Any detainee needing prescribed medication will be medicated prior to acceptance by PHS flight nurse or the SOIC.* Prescribed medication must be delivered to the PHS flight nurse. Detainees requiring medication must have at least a 7-day supply in appropriate dosages prior to boarding. When possible, carded medicines should be stapled with the form USM-553 medical form, and I-216. Detainees are permitted two respiratory inhalers and one bottle of nitroglycerin tablets on their person.

Narcotics and Controlled Substances: The PHS flight nurse will account for and secure all Drug Enforcement Agency (DEA) Schedule II, III, and IV drugs in his/her custody. Change of custody of narcotics and controlled substances requires a written transfer as follows:

- The PHS flight nurse and the officer delivering the detainees to the airlift will note the amount of the transferred dosage on form USM-553, (Section II- Medication Required for Care En Route). Information included will be the name of the detainee, alien number, name and dosage of the drug, and the quantity of the drug transferred to the custody of the PHS flight nurse.
- The PHS flight nurse will document any drugs administered during flight on the medical form.
- The PHS flight nurse and the receiving officer will count the number or quantity of each controlled substance being transferred and will document the amount on the USM-553 form upon arrival of the detainee at the final destination. Both the PHS flight nurse and the receiving officer will print and sign their names on the USM-553.
- The PHS flight nurse (or the SOIC on flights without PHS) will retain the original copy of the finalized form, giving one copy to the delivering officer, and one copy to the receiving officer.

Special Medical Treatment: Detainees requiring special medical treatment (self-catheter, colostomy care) will not be boarded unless the detainee can perform the necessary care or treatment on himself/herself, and the necessary equipment is intact and accompanies the detainee.

Decreased Mobility: Detainees who are unable to board the aircraft under their own power will not be boarded on the aircraft for safety without advance authorization of one of the following, the Prisoner Transportation Nurse Practitioner; the Chief, Aero-Medical Branch; the Chief PHS Officer, or the ICE SOIC. Transport chairs are available for detainees with decreased mobility or paralysis. Officers will not carry detainees without using the chair. The SOIC will make the final determination regarding boarding.

Medical Conditions Requiring Evaluation: Detainees with the conditions such as the following will be refused boarding unless prior approval has been obtained from either the Prisoner Transportation Nurse Practitioner or the SIOC coordinator: infectious (contagious) disease; respiratory condition; gastrointestinal problem (bleeding); uncontrolled seizure disorder; uncontrollable psychiatric behavior; sickle cell disease; kidney failure requiring dialysis; head injury; cardiac condition (history of angina or heart attack); thrombophlebitis of the lower extremities; and dental appliance or wire restricting opening of the mouth that cannot be clipped by PHS personnel.

Female Detainees: Unless instructed otherwise by the Assistant Director, JPATS, or JPATS Security, male and female detainees may be transported together on JPATS flights. When possible, female detainees will be under the visible surveillance of a female officer.

Exceptions to Medical Provisions: Unless otherwise noted, the only individuals authorized to grant exceptions to any provision in this section are the Prisoner Transportation Nurse Practitioner or the ICE SOIC.

Restraint Requirements

Detainees transported by JPATS will be fully restrained by the use of handcuffs, waist chain and leg irons during CONUS flights. Detainees will not be delivered to the airlift in any type of restraint that necessitates removal prior to the alien boarding the aircraft. JPATS security personnel will restrain any individual aboard a JPATS flight who poses a threat to the safety of the mission. JPATS-approved handcuffs and leg irons (Hiatt, S&W, Peerless, etc.) will be applied according to JPATS policy and procedures. Series 400 Peerless are not to be used. All cuffs should have the correct right and left side in their construction. Many least expensive cuffs simply have two right side cuffs attached with a chain, but there should be a mirror image relationship. All restraints will be applied with double bars and locking pins up and keyholes forward. The SOIC will have final decision as to restraints.

Escort Category 1: Aliens will not be restrained for deportation outside the United States.

Escort Category 2 and 3: Aliens who are being removed from the United States will be restrained.

Types of Restraints: All detainees for CONUS flights must be restrained with USMS-approved handcuffs, waist chains, and leg irons unless accompanied by supporting medical documents exempting the use of particular types of restraints. Aliens medically unable to wear hand/leg restraints will require approval by PHS medical personnel and the SOIC prior to boarding.

Exchanging Restraints: Delivering ICE Field Offices will exchange restraints on a one-for-one basis during the alien exchange process. Crewmembers are not authorized to exchange working restraints for damaged or defective restraints.

Application of Restraints: Connect handcuffs to the waist chain in a manner that restricts the alien's ability to touch his/her chin while standing erect, but so that he/she can accomplish such tasks as eating and using the lavatory. Detainees whose wrists are too large to permit the use of standard handcuffs may be restrained with modified leg irons (Big-Boy Cuffs), or leg irons with chain shortened to approximately the length of the handcuff chain using a flexible type cuff. Detainees wearing a cast or brace on their arm may be restrained by securing the arm to the waist chain using flexible cuffs. Restrain the uninjured arm properly with handcuffs.

Waist chains are not to be passed through the belt loops on detainee clothing as it inhibits the use of the lavatory on aircraft. For this reason, detainees wearing jumpsuits is discouraged. A maximum-security box with padlock will be applied to detainees identified as extremely dangerous or escape risks on the manifest. Leg irons will not be inserted through bootstraps or over the boots; boots will be turned down to enable leg irons to be properly applied around the detainee's leg. The SOIC will determine the proper application of restraints in the cases of a detainee whose legs are too large to permit the use of leg irons, and who do not have documented medical exceptions for leg irons.

Removal of Restraints: Restraints will not be removed for any reason unless approved by the SOIC.

Special Restraints: The SOIC has the authority to authorize the type of restraints used on detainee with special needs such as bite masks, mittens, leg braces, cargo straps, etc.

Meals

Ready To Eat Meals provided by JPATS will include one sandwich, one granola bar (or acceptable substitute), and one juice package or bottled water. Fruit or condiments (mustard, ketchup, mayonnaise, etc.) are not allowed.

Detainee Meals and Incidentals: Designated ICE offices meeting the aircraft will provide detainee meals as indicated on the official flight manifest. This should include food items, diapers for infants/toddlers, and sanitary supplies for females.

Property

Detainee Property and Money: Detainees transferred to the custody of the BOP will be subject to BOP property policies. BOP policy allows detainees to retain: a wedding band (no stones), prescribed medical device, legal material for an ongoing case, cigarettes (2 unopened packs), photographs (10 non-Polaroid's), tennis shoes (1 pair), currency or negotiable instrument, religious medal or medallion, watch (under \$100 dollars) prescription glasses and personal letters (5 maximum). If applicable, property not permitted on the body of a detainee for boarding purposes may be sealed with their other property. All excess alien property must be shipped by ICE/DRO in property boxes tagged with an I-77. Property information must also be listed on the I-216.

Confiscated and Refused Property: Property refused by the SOIC will be returned to the delivering agency at the airlift detainee exchange location for disposition/forwarding. Any item the SOIC determines could be used as a possible weapon will be taken from the alien and returned to the delivering ICE official for disposition.

Discrepancies: All discrepancies regarding the contents of the transported sealed detainee property container/box will be resolved between the sending and receiving ICE office.

Detainee Money: Cash is the accepted vehicle for money transfer to foreign soil; however, checks may also be allowed in special circumstances. The sending office must coordinate such cases with ATU. The detainee's alien number must be on any check.

Emergency Movements:

Emergency air movements will be based on unforeseen circumstances such as disturbances and/or riots in ICE/DRO facilities, urgent evacuations due to natural phenomena, or other urgent operational reasons. Emergency air movements may also occur due to urgent enforcement operational requirements. All emergency air movements must be authorized by HQDRO and JPATS.

Access to JPATS Flights

Only persons assigned to JPATS flight operations or air operations security will be transported via JPATS aircraft unless otherwise approved by the Assistant Director for Management of DRO or the Assistant Director for JPATS. Approval for requests for access to JPATS aircraft or flight operations will be coordinated through the DRO ATU.

Requests for Access to JPATS Flights

Requests to board JPATS flights (by accredited media, congressional staff or consular officials) or requests to access JPATS operations (without boarding the aircraft) must be submitted for consideration to the appropriate DRO Deputy Assistant Director. If approved, the request will be forwarded to the appropriate HQ ICE components and the ATU for coordination with JPATS, as well as with the respective field offices involved. Such requests must be in writing and be submitted at least five business days in advance of the requested date of access. The request must include the reason for the request, as well as the name, date of birth, place of birth, and social security number for each individual requesting access. If the mission is traveling OCONUS, passport/visa information will also be required. Officers and other U.S. Government employees requesting access to JPATS operations shall include their name, agency affiliation, and dates of requested access. Exceptions to the above procedures due to special circumstances may be authorized only by HQDRO.