AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE OF PAGES 1 66

2. CONTRACT (Proc. Inst. Ident.) NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
HSCETC-14-C-00002	See Block 20C	192114CIOPEO2CM2.2

5. ISSUED BY CODE ICE/TC/IT SERVICES	6. ADMINISTERED BY (If other than Item 5) CODE ICE/TC/IT SERVICES
ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW, (b)(6);(b)(7)(C) Washington DC 20536	ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW, (b)(6);(b)(7)(C) Attn: Bethany Stutler Washington DC 20536

7. NAME AND ADDRESS OF CONTRACTOR (No., Street, City, Country, State and ZIP Code)	8. DELIVERY ☐ FOB ORIGIN ☒ OTHER (See below) 9. DISCOUNT FOR PROMPT PAYMENT Net 30 10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN ▶ ITEM
PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853 CODE 9673917930000 FACILITY CODE	

11. SHIP TO/MARK FOR CODE ICE/CIO	12. PAYMENT WILL BE MADE BY CODE ICE-OCIO-TECS-CM-M
ICE Chief Information Officer Immigration and Customs Enforcement 801 I Street, NW (b)(6);(b)(7)(C) Washington DC 20536	DHS, ICE Burlington Finance Center P.O. Box 1620 Attn: ICE-OCIO-TECS-CM-M Williston VT 05495-1620

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
☐ 10 U.S.C. 2304 (c) ( ) ☐ 41 U.S.C. 253 (c) ( )	See Schedule

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

15G. TOTAL AMOUNT OF CONTRACT ▶ $12,472,821.20

16. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
X	A	SOLICITATION/CONTRACT FORM	1	X	I	CONTRACT CLAUSES	44
X	B	SUPPLIES OR SERVICES AND PRICES/COSTS	11			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
X	C	DESCRIPTION/SPECS./WORK STATEMENT	12	X	J	LIST OF ATTACHMENTS	66
X	D	PACKAGING AND MARKING	13			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
X	E	INSPECTION AND ACCEPTANCE	14		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE	15				
X	G	CONTRACT ADMINISTRATION DATA	18		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	22		M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. ☒ CONTRACTOR'S NEGOTIATED AGREEMENT (Contractor is required to sign this document and return 1 copies to issuing office.) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. (Attachments are listed herein.)	18. ☐ AWARD (Contractor is not required to sign this document.) Your offer on Solicitation Number HSCETC-14-R-00002 including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any condition sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.
19A. NAME AND TITLE OF SIGNER (Type or print)	20A. NAME OF CONTRACTING OFFICER (b)(6);(b)(7)(C)
19B. NAME OF CONTRACTOR BY (Signature of person authorized to sign)	19C. DATE SIGNED
20B. UNITED STATES OF AMERICA BY (Signature of the Contracting Officer)	20C. DATE SIGNED

NSN 7540-01-152-8069
PREVIOUS EDITION IS UNUSABLE

STANDARD FORM 26 (Rev. 4-85)
Prescribed by GSA
FAR (48 CFR) 53.214(a)

NAME OF OFFEROR OR CONTRACTOR

PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	DUNS Number: 825284321 This contract is to provide an Investigative Case Management System (ICMS) in accordance with Sections A-J and all attachments. The total value of the task order is (b)(4). The total obligated amount is (Requisition no. 192114CIOPEO2CM2.2) The Contract Specialist is (b)(6);(b)(7)(C) (b)(6);(b)(7)(C), 202-732-(b)(6);(The Contracting Officer is (b)(6);(b)(7)(C) (b)(6);(b)(7)(C), 202-732-(b)(6);(The Contracting Officer's Representative (COR) is (b)(6);(b)(7)(C) 202-732-(b)(6);(Exempt Action: Y FOB: Destination Period of Performance: 09/26/2014 to 09/24/2019				
0001	Proof of Concept (FFP) (FFP shall not exceed (b)(4) Base Period (2 months from date of contract award) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
0004	Travel Base Period (2 months from date of contract award) Not-to-Exceed (NTE) Amount: (b)(4) Obligated Amount: (b)(4) Accounting Info: TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4)				(b)(4)
1001	Labor for Transition-In (Two Months) and IOC FFP: (b)(4) SLIN 1001A: Completion of Transition-In: (b)(4) (5% of FFP) SLIN 1001B: Phase 1-Requirements Confirmation and Baseline Installation: (b)(4) (10% of FFP) SLIN 1001C: Phase 2-Baseline Gap Analysis: (b)(4) (10% of FFP) SLIN 1001D: Phase 3-Code Freeze for IOC: Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR

PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(4) (25% of FFP) SLIN 1001E: Phase 4-IOC Integration and Testing: (b)(4) (50% of FFP) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: TECS081-001 Y5 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4) Accounting Info: TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4)				
1002	ICM Software License: Enterprise License for 10,000 users and the scope of work described in the PWS. The Enterprise License is a perpetual license to (b)(4);(b)(7)(E) solution and 10 months of annual support and maintenance, which includes updates, patches, and Upgrades released during the term (Support and Maintenance). FFP: (b)(4) Option Period 1 (10 months) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: TECS081-001 Y5 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4)				(b)(4)
1003	Other Direct Costs (ODCs) NTE Amount (Cost-Reimbursable) Option Period 1 (10 months) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR

PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1004	Travel Option Period 1 (10 months) NTE Amount: (b)(4) Obligated Amount: (b)(4) Accounting Info: TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4)				(b)(4)
2002	ICM Software License: This annual FFP license cost includes renewal of one year of Product Support and Maintenance, which includes updates, patches, and Upgrades released in Option Period 2. FFP: (b)(4) Option Period 2 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2015 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
2003	Other Direct Costs (ODCs) NTE Amount (Cost-Reimbursable) Option Period 2 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2015 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
2004	Travel Option Period 2 (12 months) NTE Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2015				(b)(4)
2005	O&M (to include Tier 2 and Tier 3 Service Desk Support) Monthly FFP: $(b)(4) Total FFP: (b)(4) Option Period 2 (12 months) Amount: (b)(4) Option Line Item) 09/25/2015 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Continued ...	12	MO	(b)(4)	

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2006	Optional System Enhancements for FOC Option Period 2 (12 months) Labor-Hour (LH)/NTE Amount: (b)(4) NTE Number of Hours and Hourly Rate for each labor category as follows: Applications Developer (Associate)- NTE 4,800 Hours, (b)(4) /Hour Applications Developer (Intermediate)- NTE 7,680 Hours, (b)(4) /Hour Principal Software Development Manager- NTE 1,920 Hours, (b)(4) /Hour Configuration Management Specialist- NTE 960 Hours, (b)(4) /Hour Database Specialist (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Architect- NTE 1,920 Hours, (b)(4) /Hour Information Assurance (Associate)- NTE 960 Hours, (b)(4) /Hour Project Manager- NTE 1,920 Hours, (b)(4) /Hour Requirements Analyst (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Engineer- NTE 1,920 Hours, (b)(4) /Hour Technical Writer/Technical Editor- NTE 960 Hours, (b)(4) /Hour Test Engineer (Associate)- NTE 3,840 Hours, (b)(4) /Hour Test Engineer (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Amount: (b)(4) (Option Line Item) 09/25/2015 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
3002	ICM Software License: This annual FFP license cost includes renewal of one year of Product Support and Maintenance, which includes updates, patches, and Upgrades released in Option Period 3. FFP: (b)(4) Option Period 3 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR

PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
3003	Other Direct Costs (ODCs) NTE Amount (Cost-Reimbursable) Option Period 3 (12 months) Amount: (b)(4) Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
3004	Travel Option Period 3 (12 months) NTE Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2016				(b)(4)
3005	O&M (to include Tier 2 and Tier 3 Service Desk Support) Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 3 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE	12	MO	(b)(4)	
3006	Optional System Enhancements Option Period 3 (12 months) Labor-Hour (LH)/NTE Amount: (b)(4) Not-to-Exceed (NTE) Number of Hours and Hourly Rate for each labor category as follows: Applications Developer (Associate)- NTE 4,800 Hours, (b)(4) /Hour Applications Developer (Intermediate)- NTE 7,680 Hours, (b)(4) /Hour Principal Software Development Manager- NTE 1,920 Hours, (b)(4) /Hour Configuration Management Specialist- NTE 960 Hours, (b)(4) /Hour Database Specialist (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Architect- NTE 1,920 Hours, (b)(4) /Hour Information Assurance (Associate)- NTE 960 Hours, (b)(4) /Hour Project Manager- NTE 1,920 Hours, (b)(4) /Hour Requirements Analyst (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Engineer- NTE 1,920 Hours, Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(4) /Hour Technical Writer/Technical Editor- NTE 960 Hours, (b)(4) /Hour Test Engineer (Associate)- NTE 3,840 Hours, (b)(4) Hour Test Engineer (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				
4002	ICM Software License: This annual FFP license cost includes renewal of one year of Product Support and Maintenance, which includes updates, patches, and Upgrades released in Option Period 4. FFP: $(b)(4) Option Period 4 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
4003	Other Direct Costs (ODCs) NTE Amount (Cost-Reimbursable) Option Period 4 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
4004	Travel Option Period 4 (12 months) NTE Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2017				(b)(4)
4005	O&M (to include Tier 2 and Tier 3 Service Desk Support) Monthly FFP: (b)(4) Total FFP: $887,040.00 Option Period 4 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Continued ...	12	MO	(b)(4)	

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				
4006	Optional System Enhancements Option Period 4 (12 months) Labor-Hour (LH)/NTE Amount: (b)(4) Not-to-Exceed (NTE) Number of Hours and Hourly Rate for each labor category as follows: Applications Developer (Associate)-NTE 4,800 Hours, (b)(4) /Hour Applications Developer (Intermediate)- NTE 7,680 Hours, (b)(4) /Hour Principal Software Development Manager- NTE 1,920 Hours, (b)(4) /Hour Configuration Management Specialist- NTE 960 Hours, (b)(4) /Hour Database Specialist (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Architect- NTE 1,920 Hours, (b)(4) /Hour Information Assurance (Associate)- NTE 960 Hours, (b)(4) /Hour Project Manager- NTE 1,920 Hours, (b)(4) /Hour Requirements Analyst (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Engineer- NTE 1,920 Hours, (b)(4) /Hour Technical Writer/Technical Editor- NTE 960 Hours, (b)(4) /Hour Test Engineer (Associate)- NTE 3,840 Hours, (b)(4) /Hour Test Engineer (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
5001	Labor for two (2) month transition-out period Monthly FFP: (b)(4) Option Period 5 Amount: (b)(4) Option Line Item) 07/25/2019 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE	2	MO	(b)(4)	

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
5002	ICM Software License: This annual FFP license cost includes renewal of one year of Product Support and Maintenance, which includes updates, patches, and Upgrades released in Option Period 5. FFP: (b)(4) Option Period 5 (10 months) Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
5003	Other Direct Costs (ODCs) NTE Amount (Cost-Reimbursable) Option Period 5 (10 months) Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
5004	Travel Option Period 5 (10 months) NTE Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2018				(b)(4)
5005	O&M (to include Tier 2 and Tier 3 Service Desk Support) Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 5 (12 months) Amount: (b)(4) Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE	12	MO	(b)(4)	
5006	Optional System Enhancements Option Period 5 (10 months) Labor-Hour (LH)/NTE Amount: (b)(4) Not-to-Exceed (NTE) Number of Hours and Hourly Rate for each labor category as follows: Applications Developer (Associate)- NTE 4,800 Hours, (b)(4) /Hour Applications Developer (Intermediate)- NTE 7,680 Hours, (b)(4) /Hour Principal Software Development Manager- NTE 1,920 Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR

PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Hours, (b)(4) /Hour Configuration Management Specialist- NTE 960 Hours, (b)(4) /Hour Database Specialist (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Architect- NTE 1,920 Hours, (b)(4) /Hour Information Assurance (Associate)- NTE 960 Hours, (b)(4) /Hour Project Manager- NTE 1,920 Hours, (b)(4) /Hour Requirements Analyst (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Principal Systems Engineer- NTE 1,920 Hours, (b)(4) /Hour Technical Writer/Technical Editor- NTE 960 Hours, (b)(4) /Hour Test Engineer (Associate)- NTE 3,840 Hours, (b)(4) /Hour Test Engineer (Intermediate)- NTE 1,920 Hours, (b)(4) /Hour Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE The total amount of award: (b)(4) The obligation for this award is shown in box 15G.				

SECTION B – SUPPLIES/SERVICES AND PRICES/COSTS

B.1-TYPE OF CONTRACT

This contract is a hybrid firm-fixed price (FFP)/labor-hour (LH) contract with FFP, LH, and Cost Reimbursement (CR) CLINs; CR type CLINs will only be used for Other Direct Costs (ODCs) and Travel.

B.2-CLIN STRUCTURE

The Offeror 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 the work specified in Attachment 1-Performance Work Statement (PWS) for the ICE Investigative Case Management requirement.

B.3-TRAVEL

Travel is not expected under this contract. Any required travel will be reimbursed in accordance with the Federal Travel Regulations. Travel Not-to-Exceed (NTE) Amounts have been provided in Section A-Schedule and are set as follows:

CLIN 0004:	(b)(4)
CLIN 1004:	
CLIN 2004:	
CLIN 3004:	
CLIN 4004:	
CLIN 5004:	

Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the Contractor's usual accounting practices consistent with FAR 31.2.

Travel CLINs will be invoiced monthly. Travel requires pre-approval from the COR.

B.4-NAICS AND PSC

NAICS Code: 541512 Computer System Design Services, Size Standard: (b)(4)
PSC Code: D307 Automated Information Systems Design and Integration Services

SECTION C-PERFORMANCE WORK STATEMENT

See Section J, Attachment 1-Performance Work Statement

SECTION D-PACKAGING AND MARKING

This section is left intentionally blank.

SECTION E-INSPECTION AND ACCEPTANCE

E.1-INSPECTION OF SERVICES: CLAUSES INCORPORATED BY REFERENCE

Clause	Description	Date
52.246-3	Inspection of Supplies-Cost-Reimbursement	May 01
52.246-4	Inspection of Services-Fixed Price	Aug-96
52.246-6	Inspection-Time and Material and Labor-Hour	May-01

SECTION F-DELIVERIES AND PERFORMANCE

F.1- CLAUSES INCORPORATED BY REFERENCE

Clause	Description	Date
52.242-15	Stop-Work Order	Aug-89
52.242-17	Government Delay of Work	Apr-84

F.2-PLACE OF PERFORMANCE

Work, meetings, and briefings will be performed primarily at the Government sites located at 801 I St. NW, Washington, D.C and 500 12th St, SW, Washington, D.C.

Note: For the Base Period (Proof of Concept), the Contractor will perform work on the Contractor's site and on the Contractor's systems.

F.3-PERIOD OF PERFORMANCE

The PoP will consist of a base period and five (5) option periods as follows:
Base Period: September 26, 2014 to November 25, 2014 (Two (2) months from date of award*)
Option Period 1: November 26, 2014 to September 25, 2015 (ten (10) months)
Option Period 2: September 26, 2015 to September 25, 2016 (twelve (12) months)
Option Period 3: September 26, 2016 to September 25, 2017 (twelve (12) months)
Option Period 4: September 26, 2017 to September 25, 2018 (twelve (12) months)
Option Period 5: September 26,2018 to September 25, 2019 (twelve (12) months)

*The Base Period and Option Period 1will be exercised at the time of award.

F.4-DELIVERABLES

See Section J, Attachment 1-Performance Work Statement that includes all deliverables and work products. Note: All deliverables that are a "Major System Technical Data Deliverable" or "Major System Technical Data Work Product" in the following table (that are also listed in the PWS) are subject to FAR 52.227-21, Technical Data Declaration, Revision, and Withholding of Payment-Major Systems (DEC 07):

Work Product/Deliverable Title	Deliverable/Work Product
ICM System Proof of Concept COTS Suite Attachment 1-PWS, Deliverable 3.1.1	Major System Technical Data Deliverable
ICM System Proof of Concept COTS User Documentation Attachment 1-PWS, Deliverable 3.1.2	Major System Technical Data Deliverable
ICM System Requirements Verification Matrix Attachment 1-PWS, Deliverable 3.2.1	Major System Technical Data Deliverable
ICM System Baseline Gap Analysis Attachment 1-PWS, Deliverable 3.3.1	Major System Technical Data Deliverable

ICM System Data Migration Plan Attachment 1-PWS, Deliverable 3.3.3	Major System Technical Data Deliverable
ICM System Design Document (DD) Attachment 1-PWS, Deliverable 3.3.4	Major System Technical Data Deliverable
ICM System Design Review Presentation Attachment 1-PWS, Deliverable 3.3.5	Major System Technical Data Deliverable
Requirements Traceability Matrix Attachment 1-PWS, Deliverable 3.3.2	Major System Technical Data Work Product
ICM System Data Management Plan Attachment 1-PWS, Deliverable 3.4.1	Major System Technical Data Deliverable
ICM System Deployment Plan Attachment 1-PWS, Deliverable 3.4.2	Major System Technical Data Deliverable
ICM System Development Test Plan Attachment 1-PWS, Deliverable 3.4.3	Major System Technical Data Deliverable
ICM System Performance Analysis Plan Attachment 1-PWS, Deliverable 3.4.4	Major System Technical Data Deliverable
ICM System Training Plans and Materials Attachment 1-PWS, Deliverable 3.4.5	Major System Technical Data Deliverable
ICM System Version Description Document Attachment 1-PWS, Deliverable 3.4.6	Major System Technical Data Deliverable
ICM System Software Attachment 1-PWS, Deliverable 3.4.11	Major System Technical Data Deliverable
Contingency Plan (CP) Attachment 1-PWS, Deliverable 3.5.6	Major System Technical Data Deliverable
Contingency Plan (CP) Test Results Attachment 1-PWS, Deliverable 3.5.7	Major System Technical Data Deliverable
Development Test Analysis Report Attachment 1-PWS, Deliverable 3.5.8	Major System Technical Data Work Product
ICM System User Manuals/Guides Attachment 1-PWS, Deliverable 3.5.1	Major System Technical Data Deliverable
ICM System Maintenance Manual(s) Attachment 1-PWS, Deliverable 3.5.5	Major System Technical Data Deliverable
Software Documentation Attachment 1-PWS, Deliverable 3.5.4	Major System Technical Data Deliverable
ICM System Administration and Operations Manual Attachment 1-PWS, Deliverable 3.5.2	Major System Technical Data Deliverable
Information Assurance Plan Attachment 1-PWS, Deliverable 3.5.3	Major System Technical Data Deliverable
Transition Management Plan Attachment 1-PWS, Deliverable 3.9.1	Major System Technical Data Deliverable

Plan for Extraction of ICE Data in the ICM System Attachment 1-PWS, Deliverable 3.9.2	Major System Technical Data Deliverable
Final Updated ICM System Documentation Attachment 1-PWS, Deliverable 3.9.3	Major System Technical Data Deliverable

F.5-DELIVERY INSTRUCTIONS

All deliverables shall be submitted in electronic format no later than 4:00 PM on the deliverable's due date. All electronic versions of the deliverables shall be submitted in MS Office 2010 or compatible.

Electronic deliverables shall be submitted to the COR at the following e-mail address:
(b)(6),(b)(7)(C)

Items must be approved by the Program Manager (PM) and/or the appropriate Government authority to be considered "acceptable." The Government will provide written acceptance, comments, or change requests within ten (10) business days from receipt by the Government of all required Contract deliverables, with the exception of Software Versions and Releases.

Upon receipt of the Government comments, the Contractor shall schedule a collaborative session with the Government within five (5) business days to review any comments or change requests. After the collaborative session, the Contractor shall have ten (10) business days to incorporate the comments or changes, and resubmit the deliverable to the Government.

F.6-NOTICE REGARDING LATE DELIVERY

The Contractor shall notify the COR as soon as it becomes apparent to the Contractor that a scheduled deliverable will be late. The Contractor shall include in the notification the rationale for late delivery of the deliverable, the expected date for the deliverable, any consideration provided by the Contractor, and the impact of the late delivery of the deliverable on the project. The COR, Program Manager, and Contracting Officer will review the new schedule and the Contracting Officer will provide guidance to the Contractor.

SECTION G-CONTRACT ADMINISTRATION DATA

G.1-TECHNICAL DIRECTION AND SURVEILLANCE

a) Performance of the work under this contract shall be subject to the surveillance and written technical direction of the COR, who shall be specifically appointed by the Contracting Officer in writing. Technical direction is defined as a directive to the Contractor which approves approaches, solutions, designs, or refinements; fills in details or otherwise completes the general description of work of documentation items; shifts emphasis among work areas or tasks; or otherwise furnishes guidance to the Contractor. Technical direction includes the process of conducting inquiries, requesting studies, or transmitting information or advice by the COR, regarding matters within the general tasks and requirements in Section C of this CONTRACT.

b) The COR does not have the authority to, and shall not, issue any technical direction which:

1. Constitutes an assignment of additional work outside the PWS;
2. Constitutes a change as defined in the contract clause entitled "Changes";
3. In any manner causes an increase or decrease in the total price or the time required for contract performance;
4. Changes any of the expressed terms, conditions, or specifications of the contract; or
5. Interferes with the Contractor's right to perform the specifications of the contract.

c) All technical directions shall be issued in writing by the COR via e-mail. The Contractor shall proceed promptly with the performance of technical directions duly issued by the COR. Any instruction or direction by the COR which falls within one or more of the categories defined in (b)(1) through (5) above, shall follow the procedures in FAR 52.243-7.

G.2-CONTRACTING OFFICER'S REPRESENTATIVE

The COR for this contract is: (b)(6);(b)(7)(C)

Alternate COR for this contract is (b)(6);(b)(7)(C)

G.3-INVOICING AND PAYMENT PROCEDURES

Invoicing Instructions

Service Providers/Contractors shall use these procedures when submitting an invoice.

1. Invoice Submission: Invoices shall be submitted in a .pdf format in accordance with the contract terms and conditions via email to:

(b)(6);(b)(7)(C)

Each email shall contain only (1) invoice and the invoice number shall be indicated on the subject line of the email.

Alternative methods of invoice submission include United States Postal Service (USPS) mail or fax. The mailing address of DHS ICE Financial Operations is:

DHS, ICE
Financial Operations - Burlington
P.O. Box 1620
Williston, VT 05495-1620
ATTN: ICE/PEO/TECS

Note: the Contractor's Dunn and Bradstreet (D&B) DUNS Number must be registered in the System for Award Management (SAM) at https://www.sam.gov prior to award and shall be notated on every invoice submitted to ensure prompt payment provisions are met. The ICE Program Office identified in the award shall also be notated on every invoice.

The Contractors Data Universal Numbering System (DUNS) Number must be registered and active in the System for Award Management (SAM) at https://www.sam.gov prior to award and shall be notated on every invoice submitted to ensure prompt payment provisions are met. The ICE program office identified in the task order/contract shall also be notated on every invoice.

Alternate method of submission is fax. Invoices shall be submitted to:
(802)-288-7658 (include a cover sheet with point of contact & # of pages)

2. Content of Invoices: Each invoice submission shall contain the following information:
(i) Name and address of the Contractor. The name, address and DUNS number on the invoice MUST match the information in both the Contract/Agreement and the information in the SAM;
(ii) Dunn and Bradstreet (D&B) DUNS number;
(iii) Invoice date and invoice number;
(iv) Agreement/Contract number, contract line item number and, if applicable, the order number;
(v) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(vi) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vii) Terms of any discount for prompt payment offered;
(viii) Remit to Address;
(ix) Name, title, and phone number of person to notify in event of defective invoice;
(x) Whether the invoice is "Interim" or "Final" and
(xi) ICE program office designated on order/contract/agreement.

In accordance with Contract Clause, FAR 52.212-4(g)(1), Contract Terms and Conditions Commercial Items, or FAR 52.232-25(a)(3), Prompt Payment, as applicable, the information identified above is required with each invoice submission.

3. Payment Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at 1-877-491-6521 or by e-mail at OCFO.CustomerService@ice.dhs.gov

CLIN 1001-Firm-Fixed Price (FFP) shall be invoiced for based on the percentage of each Sub-Contract Line Item Number (SLIN). Once the deliverable for each SLIN is accepted by the Government, the Contractor shall submit an invoice for the percentage of FFP listed in the SLIN. The FFP percentage allocated to each SLIN is as follows:

SLIN No.	Deliverable/Phase	Amount
SLIN 1001A	Completion of Transition-In	(b)(4)
SLIN 1001B	Phase 1: Requirements Confirmation and Baseline Installation	(b)(4)
SLIN 1001C	Phase 2: Baseline Gap Analysis	(b)(4)
SLIN 1001D	Phase 3: Code Freeze for IOC	(b)(4)
SLIN 1001E	Phase 4: IOC Integration and Testing	(b)(4)

Labor Hour CLINs:
Materials on T&M Orders must comply with FAR 52.232-7 Payments Under Time-and-Materials and Labor Hour Contracts (Aug 2012).

Cost Reimbursable CLIN (Other Direct Costs) CLINs:
The contractor may invoice monthly on the basis of cost incurred for the Other Direct Cost (ODC) CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and name. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable in spreadsheet form:

Item purchased
Cost
Date expensed
Documentation of prior COR approval

All cost presentations provided by the Contractor shall also include applicable indirect cost.

Travel CLINs:
The contractor may invoice monthly on the basis of cost incurred. The invoice shall include the period of performance covered by the invoice and the CLIN number and name. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable in spreadsheet form:

Project Total Travel: This will identify all current and cumulative travel on the project.

The listing shall include separate columns and totals for the following, at a minimum:

Date Expensed
Authorized Travel Event Number
Days of Travel
Documentation of COR approval prior to travel

Travel shall be in accordance with the Federal Travel Regulations (FTR). The contractor shall be reimbursed for actual, allowable, and reasonable cost, not to exceed the amount shown in the schedule. Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the contractor's usual accounting practices consistent with FAR 31.2.

In order to ensure that an accurate invoice is submitted, the Contractor shall coordinate the invoice with the Contracting Officers Representative (COR) before sending the invoice to Financial Operations Burlington.

Payment Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at 1-877-491-6521 or by e-mail at OCFO.CustomerService@ice.dhs.gov

G.4-PAST PERFORMANCE EVALUATIONS

Interim past performance evaluations will be completed for this contract after the conclusion of each 12-month period. The Government will provide past performance evaluations in the Contractor Performance Assessment Reporting System (CPARS) within 90 days of the PoP of each 12-month period. CPARS is a web-enabled tool for the COR to evaluate the Contractor's performance and for the Contracting Officer and Contractor to review, comment on, and approve evaluations. The tool can be accessed at http://www.cpars.csd.disa.mil. The Contractor will be allowed thirty (30) calendar days to submit comments, rebut statements, or provide additional information. Comments, if any shall be retained as part of the evaluation record. The completed evaluation shall not be released to other than Government personnel and the Contractor whose performance is being evaluated during the period the information may be used to provide source selection information. Past performance information will not be retained for longer than three years after completion of a contract.

SECTION H-SPECIAL CONTRACT REQUIREMENTS

H.1-GOVERNMENT FURNISHED INFORMATION

The Government will provide the following documents as Government Furnished Information (GFI) during the contract:

Description of GFI	Date GFI Furnished	Date GFI Returned
PWS Constraint Documents including the following: • Exhibit A: ICE/HSI ICM System Requirements (LES) • Exhibit B: ICE/HSI Business Process Deep Dive Diagrams (LES) • Exhibit C: Target Data Model for Data Migration (LES) • Exhibit D: ICE TECS Modernization SELC Tailoring Plan • Exhibit E: ICE TECS Modernization ORD • Exhibit F: ICE/HSI RACI Chart (LES) • Exhibit G: ICE TECS Modernization TEMP	Provided with Request for Proposals (RFP) Updated versions of GFI, as versions are approved during the contract period of performance.	n/a
Finalized, Baseline Requirements	Provided to the Contractor at the beginning of each release.	n/a

H.2-GOVERNMENT FURNISHED PROPERTY

The Government will provide the following items as Government Furnished Property (GFP):
Note: The Government will not provide GFP during the Base Period: Proof of Concept

Description of GFP	Date GFP Furnished	Date GFP Returned
ICE Virtual Private Network (VPN) Tokens and Air Cards	Provided as Contractor is cleared for service and laptops are reimaged.	Returned once Contractor employee leaves the contract (via termination or reassignment) or the contract completion.
Personal Identification Verification (PIV) card	Provided as Contractor is cleared for service	Returned once Contractor employee leaves the contract or contract completion.
Direct-line access to the ICE Intranet and LAN/WAN access	Provided once the Contractor facility meets Government security requirements	Removed upon contract completion.
Blackberry Mobile devices (for personnel selected by the COR)	Provided at request of the COR	Returned at request of the COR.
Other GFP (thumb drives, iPads, etc)	Provided at request of the COR	Returned at request of the COR.
Desktop Computers/Laptops	Provided as Contractor is cleared for service	Returned upon contract completion.
Hardware/Software Proposed by the Contractor to be provided by OCIO Engineering (If required)	N/A	N/A

Note: The Contractor shall keep an accurate inventory of GFP, which shall be made available to the Government upon request.

H.3-TRAVEL

Frequent local travel in the greater D.C. area to Immigration and Customs Enforcement (ICE) Office of the Chief Information Officer (OCIO) offices located at 801 I Street NW, Washington, D.C., or 500 12th St SW, Washington, D.C., may be required. However, local travel (defined as within 50 miles of the greater Washington, D.C. area) will not be reimbursed.

Travel requires pre-approval from the COR. Travel shall be in accordance with the Federal Travel Regulations (FTR). The Contractor shall be reimbursed for actual, allowable, and reasonable costs, not to exceed the amount shown in the schedule. Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the Contractor's usual accounting practices consistent with FAR 31.2.

H.4-OTHER DIRECT COSTS (INCLUDING MATERIALS)

All ODCs require pre-approval from the COR. The Contractor shall be reimbursed for actual, allowable, and reasonable costs, not to exceed the amount shown in the schedule. Profit shall not

be applied to ODCs. Contractors may apply indirect costs to ODCs in accordance with the Contractor's usual accounting practices consistent with FAR 31.2.

H.5-REQUIRED APPROVALS FOR TRAVEL AND ODCs

All requests for Travel and Other Direct Costs must be approved in writing by the ICE COR and be appropriately funded prior to incurring costs. The Contractor shall not be reimbursed if the appropriate documentation is not provided with the invoice or approved in advance.

H.6- SECURITY REQUIREMENTS

H.6.1-SECURITY REQUIREMENTS FOR BASE PERIOD OF CONTRACT (PROOF OF CONCEPTS)

Contractors shall complete Attachment 5-BAR FORM and fingerprint cards for each individual providing services during the Base Period (Proof of Concepts) of the contract. These individuals will be screened (or re-screened if they were previously screened as part of Step 2 of the solicitation) to ensure they meet the requirements for performance during the Base Period (Proof of Concepts) of the contract to include access to LES Information. Offerors shall submit all completed BAR FORMS to the COR via e-mail no later than five (5) business days after award of the contract. If the Contractor needs fingerprint cards, the Contractor shall submit a request to the COR via e-mail within three (3) business days of contract award. Further instructions on how to submit the fingerprint cards will be provided at the time of contract award. ICE reserves the right and prerogative to deny and/or restrict access to sensitive and/or LES Government information or deny ability to perform on the contract to any individual whose actions are in conflict with the mission of ICE, or whom ICE determines to present a risk of compromising sensitive and/or LES Government information to which he or she would have access to under the Base Period (Proof of Concepts) of the contract. The Contractor will be notified if there are any personnel that shall be denied access to sensitive and/or LES information or denied ability to perform on the contract.

H.6.2-CONTRACTOR PERSONNEL REQUIRED SECURITY LANGUAGE FOR SENSITIVE /BUT UNCLASSIFED (SBU) CONTRACTS SECURITY REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in Contract **HSCETC-14-C-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.

PRELIMINARY DETERMINATION

ICE will 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. ICE may, as it deems appropriate, authorize and make a favorable expedited pre-employment determination based on preliminary security checks. The expedited pre-employment determination will allow the employees to

commence work temporarily prior to the completion of the full investigation. The granting of a favorable pre-employment determination shall not be considered as assurance that a favorable full employment determination will follow as a result thereof. The granting of a favorable pre-employment determination or a full employment determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the Contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary fitness determination or final fitness 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 pre-employment determination or full employment determination by the OPR-PSU. Contract employees are processed under the DHS Management Directive 6-8.0. The contractor shall comply with the pre-screening requirements specified in the DHS Special Security Requirement – Contractor Pre-Screening paragraph located in this contract, if HSAR clauses 3052.204-70, Security Requirements for Unclassified Information Technology (IT) Resources; and/or 3052.204-71, Contractor Employee Access are included in the Clause section of this contract.

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 shall submit the following completed forms to the Personnel Security Unit through the Contracting Offices Representative (COR), no less than 35 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) (Original and One Copy)

2. Three signed eQip Signature forms: Signature Page, Release of Information and Release of Medical Information (Originals and One Copy)

3. Two FD Form 258, "Fingerprint Card"

4. Foreign National Relatives or Associates Statement (Original and One Copy)

5. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" (Original and One Copy)

6. Optional Form 306 Declaration for Federal Employment (applies to contractors as well) (Original and One Copy)

Prospective Contractor employees who currently have an adequate current investigation and security clearance issued by the Department of Defense Central Adjudications Facility (DoD CAF) or by another Federal Agency may not be required to submit complete security packages, and the investigation will be accepted for adjudication under reciprocity.

An adequate and current investigation is one where the investigation is not more than five years old and the subject has not had a break in service of more than two years.

Required forms will be provided by ICE 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 DHS /ICE IT systems and the information contained therein, to include, the development and / or maintenance of DHS/ICE IT systems; or access to information contained in and / or derived from any DHS/ICE IT system.

TRANSFERS FROM OTHER DHS CONTRACTS:
Personnel may transfer from other DHS Contracts provided they have an adequate and current investigation (see above). If the prospective employee does not have an adequate and current investigation an eQip Worksheet will be submitted to the Intake Team to initiate a new investigation.

Transfers will be submitted on the COR Transfer Form which will be provided by the Dallas PSU Office along with other forms and instructions.

CONTINUED ELIGIBILITY
If a prospective employee is found to be ineligible for access to Government facilities or information, the COR 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 will conduct reinvestigations every 5 years, or when derogatory information is received, to evaluate continued eligibility.

ICE 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 ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

REQUIRED REPORTS:

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

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COR, as soon as possible. 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 Contractor will provide, through the COR a Quarterly Report containing the names of personnel who are active, pending hire, have departed within the quarter or have had a legal name change (Submitted with documentation) . The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

Submit reports to the email address (b)(6);(b)(7)(C)

EMPLOYMENT ELIGIBILITY

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

The E-Verify system, formerly known as the Basic Pilot/Employment Eligibility verification Program, is an Internet-based system operated by DHS USCIS, in partnership with the Social Security Administration (SSA) that allows participating employers to electronically verify the employment eligibility of their newly hired employees. E-Verify represents the best means currently available for employers to verify the work authorization of their employees.

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 COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COR 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 COR 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) U.S. Immigration and Customs Enforcement (ICE) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

INFORMATION TECHNOLOGY

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).

H.6.4-IT SECURITY REQUIREMENTS

General

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Subcontractors must adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE Information System Security Officer (ISSO) and Contracting Officer and detailed in the contract. Non-DHS Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Subcontractors.

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how Contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering Contractors specifically for all Contracts that require access to DHS facilities, IT resources, or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the Contractor except as specified in the Contract.

Interconnection Security Agreements

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 Interconnection Security Agreements. The Contractor shall work with the ICE OCIO Information Assurance Division (IAD) to complete the required documentation

Security Policy References
The following primary DHS/ICE IT Security documents are applicable to Contractor/Sub-contractor operations supporting Sensitive But Unclassified (SBU) based contracts. Additionally, ICE and its Contractors must conform to other DHS Management Directives (MD) (Note: these additional MD documents appear on DHS-Online in the MD Section. Volume 11000 "Security and Volume 4000 "IT Systems". All services provided under this Contract must be compliant with DHS 4300A, Sensitive Systems Policy Directive, DHS Information Security Policy for SBU Systems, and 4300A Sensitive Systems Handbook.

Contractor Information Systems Security Officer (ISSO) Point of Contact
The Contractor must appoint and submit name to ICE ISSO for approval, via the ICE COR, of a qualified individual to act as ISSO to interact with ICE personnel on all IT security matters.

Protection of Sensitive Information
The Contractor shall protect all DHS/ICE "sensitive information" to which the Contractor is granted physical or electronic access by adhering to the specific IT security requirements of this contract and the DHS/ICE security policies specified in the Reference Section above. The Contractor shall ensure that their systems containing DHS/ICE information and data be protected from unauthorized access, modification and denial of service. Further, the data must be protected in order to ensure the privacy of individual's personal information. All contractor employees must sign DHS 11000-6, Non-Disclosure Agreement, prior to accessing any sensitive information. The signed agreements must be provided to the COR.

Information Technology Security Program
If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall establish and maintain an IT Security Program. This program shall be consistent with the referenced DHS/ICE IT security policy documents and at a minimum contain and address the following elements:

- Handling of DHS/ICE sensitive information and IT resources to include media protection, access control, auditing, network security, and rules of behavior
- Certification and Accreditation and Federal Information Security Management Act (FISMA) compliance (C&A) of Systems containing, processing or transmitting of DHS/ICE data
- Training and Awareness for Contractor personnel
- Security Incident Reporting
- Contingency Planning
- Security Reviews
- Contract Closeout Actions

Handling of Sensitive Information and IT Resources
The Contractor shall protect DHS/ICE sensitive information and all government provided and Contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

- **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)

- **Access Control.** The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication and authorization (Roles and Rules based) mechanisms. Access control measures employed shall provide protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.

- **Auditing.** The Contractor shall ensure that it's Contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.

- **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between Contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its e-mail systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems

containing DHS/ICE sensitive information to identify security vulnerabilities. The results, of this information, will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.

- DHS employees and Contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.

- Rules of Behavior. The Contractor shall develop and enforce Rules of Behavior for Contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior must meet or exceed the DHS/ICE rules of behavior.

- The Contractor shall adhere to the policy and guidance contained in the DHS/ICE reference documents.

Training and Awareness

- The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS/ICE sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior. The Contractor must use the ICE-provided annual awareness training and submit to the COTR the certificates of training for each individual on the contract.

- The Contractor shall ensure that all Contractor personnel, including Sub-contractor personnel, with IT security responsibilities receive specialized DHS/ICE annual training tailored to their specific security responsibilities. The Contractor must use the ICE-provided special training and provide certificates of training to the COTR.

- Any Contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers may be required to attend and participate in the annual DHS Security Conference.

Certification and Accreditation (C&A) and FISMA Compliance

The Contractor shall ensure that any Contractor-owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements. Any work on developing, maintaining or modifying DHS/ICE systems must be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The Contractor must ensure that the necessary C&A and FISMA compliance requirements are being effectively met prior to the System or application's release into Production (this also includes pilots). The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

Security Incident Reporting
The Contractor shall establish and maintain a computer incident response capability that reports all incidents to the ICE Computer Security Incident Response Center (CSIRC) in accordance with the guidance and procedures contained in the referenced documents.

Contingency Planning
If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted. All Contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery.

Security Review and Reporting
- The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.
- 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/ICE, including the Office of Inspector General, ICE ISSO, and other Government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. 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/ICE data or the function of computer systems operated on behalf of DHS/ICE, and to preserve evidence of computer crime.

Use of Government Equipment
Contractors are not authorized to use Government office equipment of IT systems/computers for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, Contractors shall be governed by the limited personal use policies in the referenced documents.

Contract Closeout
At the expiration of this contract, the Contractor shall return all sensitive DHS/ICE information and IT resources provided during the life of this contract. The Contractor shall certify that all DHS/ICE information has been purged from any Contractor-owned system used to store or process DHS/ICE information. Electronic media must be sanitized (overwritten or degaussed) in accordance with the sanitation guidance and procedures contained in reference documents and with DHS/NIST/NSA approved hardware and software.

Personnel Security

- DHS/ICE does not permit the use of non U.S. Citizens in the performance of this contract or to access DHS/ICE systems or information
- All Contractor personnel (including Sub-contractor personnel) must have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.
- The Contractor shall ensure all Contractor personnel are properly submitted for appropriate clearances.
- The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have been issued. At the option of the Government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.
- The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.
- The Contractor shall ensure that its personnel comply with applicable Rules of Behavior (See Attachment 4-DHS 4300A Sensitive Systems Handbook, Rules of Behavior that is provided as reference only) for all DHS/ICE and Contractor-owned IT systems to which its personnel have been granted access privileges.
- The Contractor shall implement procedures to ensure that system access privileges are revoked for Contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.
- The Contractor shall conduct exit interviews to ensure that Contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

Physical Security

The Contractor shall ensure that access to Contractor buildings, rooms, work areas and spaces, and structures that house DHS/ICE sensitive information or IT systems through which DHS/ICE sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS/ICE sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the relevant ICE policies and guidance. The Contractor shall ensure that the development facilities are approved through the C&A for storing Government information.

H.7-PRIVACY CONTROL

1.0 Privacy Requirements for IT Security Plan

Personally Identifiable Information is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a United States citizen, legal permanent resident, or a visitor to the U.S.

Sensitive Personally Identifiable Information (PII) is a subset of PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any grouping of information that contains the individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last-4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer information
(5) Medical information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PINs)

The IT Security Plan must address how this information will be protected.
NOTE: Other PII may be "sensitive" depending upon its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or a public phone directory of agency employees contains PII but is not sensitive.

The work to be performed under this contract requires the handling of Sensitive PII in order to perform a contract with the Department of Homeland Security (DHS) or one of its components. The Contractor shall provide DHS or the DHS component access to and information regarding the Contractor's systems when requested by the Department in connection with its efforts to ensure compliance with all such security requirements, and shall otherwise cooperate with the Department in such efforts. DHS and DHS component access shall include independent validation testing of controls, system penetration testing by DHS or DHS component, FISMA data reviews, and access by the DHS Office of the Inspector General for its reviews.

For all systems handling Sensitive PII, the Contractor shall comply with all security requirements applicable to DHS systems described in DHS Sensitive System Publication 4300A or any replacement publication, and those of the DHS component for which the contract is being performed.

The use of Contractor-owned laptops or other media storage devices to process or store Sensitive PII is prohibited.

2.0 Handling of Personally Identifiable Information

The Contractor must limit access to the data covered by this clause to those employees who need the information to perform work under this contract. Contractor must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and ensure it is secured when in transit to prevent unauthorized access or loss. If the Contractor is e-mailing Sensitive PII within the DHS network (i.e. from a DHS e-mail account (dhs.gov) to another DHS e-mail account), the information can be sent unencrypted. If Sensitive PII is being sent outside of the DHS network (i.e. e-mailing it from a DHS e-mail address to a non-DHS e-mail address or vice versa), the information must be encrypted. If Sensitive PII is stored on a shared drives, access to it should be restricted to those with a need to know by permissions settings or passwords. The "Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security" provides additional guidance for the proper handling of Sensitive PII. Sensitive PII shall not be transported overseas without the prior written approval of the CO. When Sensitive PII is no longer needed and no longer required to be retained under applicable records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

Contractor may only use Sensitive PII obtained under this contract for purposes of the contract, and may not collect or use such information for any other purpose without the prior written approval of the CO. At the expiration of the contract, the Contractor shall turn over all Sensitive PII obtained under this contract that is still in its possession to DHS or DHS component.

3.0 Privacy Training and Awareness

The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) take the annual Culture of Privacy training.
The Contractor shall ensure that all Contractor personnel (including Sub-contractor personnel) take the annual Records Management training.

4.0 Breach Response

A breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users have access or potential access to personally identifiable information, whether physical or electronic, without an authorized purpose.

By acceptance of, or performance on, this contract, the Contractor agrees that in the event of any actual or suspected breach of Sensitive PII, the Contractor will immediately (and in no event later than within one hour of discovery) report the breach to the CO and contracting officer's technical representative (COR), and the DHS or DHS component information security response team. The Contractor is responsible for positively verifying that the notification is received and acknowledged.

If the data breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, the Contractor shall call the DHS or DHS component Computer Emergency Readiness Team within one hour of discovery of the breach. The Contractor shall also notify the CO as soon as possible during regular business hours.

5.0 Personally Identifiable Information Notification Requirement

The Contractor will certify that it has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached. The method and content of any notification by the Contractor shall be coordinated with, and be subject to the approval of, DHS or the DHS Component. Notification shall not proceed unless DHS or the DHS component has made a determination that notification is appropriate and would not impede a law enforcement investigation or jeopardize national security.

The method of notification may include letter sent via first class mail, electronic means, or general public notice, as approved by DHS or DHS component. As a minimum, the notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; and (5) who affected individuals should contact for more information.

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor shall, when directed by the CO and at no cost to the government, take action to correct or mitigate the violation, which may include providing notification or other identity protection services to affected individuals for a period not to exceed eighteen months from the discovery of the breach. The Contractor shall be responsible for the acts or omissions of its employees that contribute to a Sensitive PII breach when any such employee had access to such PII by virtue of his or her employment by the Contractor. All mitigation and corrective measures must be approved by the CO.

DHS or the DHS component may elect to provide and/or procure notification or identity protection services, in which case the Contractor will be responsible for reimbursing DHS or the DHS component for those costs.

The requirements set forth in this section apply to all subcontractors who perform work in connection with this contract. For each subcontractor, the Contractor must certify that it has required the subcontractor to adhere to all such requirements. Any breach by a subcontractor of any of the provisions set forth in this clause will be attributed to the Contractor.

H.8-ACCESSIBILITY REQUIREMENTS

Accessibility Requirements (Section 508)

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 (EIT), 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 EIT accessibility 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 1194.24 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.

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed 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.

Section 508 Applicable Accessibility Exceptions

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 1194.3(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.

Section 508 Compliance Requirements (Note to Offerors: The following is a requirement for the Government and is provided in the contract for informational purposes only)

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 that 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 authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools.

H.9-DHS AND ICE ENTERPRISE ARCHITECTURE COMPLIANCE

All solutions and services shall meet ICE and DHS Enterprise Architecture policies, standards, and procedures as it relates to the Performance Work Statement. The Contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the ICE and HLS EA.
- All IT hardware or software shall be compliant with the ICE and HLS EA 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.
- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

H.10 – LICENSING REQUIREMENTS

Identification and Assertion of Restrictions
The Contractor shall not deliver or otherwise provide to the Government any technical data or computer software with restrictive markings (or otherwise subject to restrictions on access, use, modification, reproduction, release, performance, display, or disclosure) unless the technical data or computer software are identified in accordance with the following requirements.

The contractor identified and asserted any restrictions for all commercial computer software, including Open Source Software (OSS), and commercial technical data, i.e., technical data pertaining to a commercial item, in the following table.

Commercial Technical Data/Computer Software Title and Version #*	If Open Source Software, Open Source License and Version #**	Name of Contractor Delivering Commercial Software***	Technical Use/ Implementing Approach****	If OSS, was OSS modified by contractor?*****	If OSS and OSS was modified, was OSS modified by incorporation into a third party's software? ******	Restriction
(b)(4)	N/A	Palantir USG, Inc.	Commercial software for ICM Solution	N/A	N/A	Per FAR 12.212 and subject to 52.227-19, use of this commercial software is subject to our LSA, which is provided as Attachment 3 to the Contract.
Atlassian software suite, including Jira products and Confluence	N/A	Atlassian	Palantir support/issue ticket tracking and documentation management tools	N/A	N/A	This will be utilized solely for use by Palantir during the support services term. This is not being offered or provided on a stand-alone basis.

Post-Award Updates to the Pre-Award Identification and Assertions: The Contractor may supplement or revise its pre-award identification and assertion of restrictions on computer software and technical data, if such software or technical data restrictions were not known at the time of award and its omission would not have materially affected the source selection.

Use of Open Source Software Without Delivery: The Government treats Open Source Software (OSS) as a category of commercial computer software. If the Contractor proposes to use OSS while performing under this contract, the Contractor shall follow the same rules prescribed in the Contract for commercial computer software. Additionally, the Contractor must ensure that its use thereof does not: (i) create, or purport to create, any Government distribution obligations with respect to the computer software deliverables; or (ii) grant, or purport to grant, to any third party any rights to or immunities under Government intellectual property or Government data rights to the Government computer software deliverables.

Contractor Use of Commercial Computer Software, Including Open Source Software
Contractor Use of Commercial Computer Software, including Open Source Software. Open source software is often licensed under terms that require a user to make user's modifications to the open source software or any software that the user combines with the open source software freely available in source code form pursuant to distribution obligations in the license.

In cases where the Contractor proposes to use open source software while performing under a Government contract, regardless of whether the open source software is delivered, the Contractor shall not create, or purport to create, any Government distribution obligation with respect to Government computer software deliverables.

Prior to using any commercial computer software, the Contractor shall additionally evaluate each license for commercial computer software, including open source software which is considered commercial computer software, and confirm that each of the following requirements is satisfied:

a) A license for a particular commercial computer software shall be compatible with all licenses for other commercial computer software that are or will be linked to, adapted to, integrated, combined or merged with the particular commercial computer software, including when the particular commercial computer software and the other commercial computer software are used with another computer program;

b) A license for commercial computer software shall not impose a future Government distribution obligation that is foreseeable by the Contractor;

c) A license for commercial computer software shall not be terminated by the Contractor's use of the commercial computer software in performing under the contract; and

d) Contractor's cost to comply with this requirement presents no additional cost to the Government.

The Contractor shall provide a written summary report to the Contracting Officer stating that the Contractor has evaluated the commercial computer software use and commercial computer software license, and made each determination identified above and clearly identifies the proposed use(s) of the commercial computer software proposed. The Contracting Officer shall give the Contractor permission for the proposed use of the software.

If the Contractor is unable to satisfy the requirements above for a particular commercial computer software license, then the Contractor may not use the commercial computer software covered by the particular license without prior approval by the Contracting Officer. If the Contractor wants to use the Commercial Computer Software for which the requirements of paragraphs a) – d) above, the Contractor shall request approval to use the otherwise prohibited subject commercial computer software from the Contracting Officer by providing a written notification addressing the following: (i) the name and version number of the software; (ii) the

name of the applicable license(s); (iii) a brief description of the technical use and implementing approach; (iv) a "yes/no" indication as to whether the Contractor has made, or will make, any modifications to the source code; (v) the software website; and in addition (vi) an identification of the reason(s) that the Contractor was unable to make the determinations in paragraphs a)-d) above. Commercial computer software is the same as defined in FAR 2.101.

Disclosure to Parties Outside of the Federal Government
Before any disclosure of technical data of computer software to ICE service support contractors and subcontractors, ICE service support contractors and subcontractors shall be required to sign DHS 11000-6.

License Users
Authorized users of any licensed software product shall include any government employee, Federal, State, or Local, and ICE's service support contractors and subcontractors. Should ICE transfer its license rights to a DHS component or agency, the authorized users of the licensed software product shall include the service support contractors and subcontractors of that DHS component or agency.

License Transfer
ICE shall have the right, without the prior written consent of the Software Publisher or its Authorized Resellers, to assign, reassign, or transfer software licenses or ICE's rights in the software to any other component or agency within DHS. Such authorization includes sublicensing, assignment or transfer among or between these users. If the Department or a DHS component or agency that has been transferred the license rights is reorganized or restructured such that its responsibilities and operations are transferred to another Department or DHS component or agency, the Department, component or agency shall have the right to assign the affected program licenses to a successor. The licensed agency and successor agency agree to be bound to the language in section H.

License Use
The license shall not restrict use of the software to a single computer, specific hardware, mobile devices, building or location.

Warranty
In addition to the completed Exhibit A-ICE/HSI Investigative Case Management System Requirements and the statement of affirmation from the Contractor regarding their understanding and intention to fulfill the full system requirements, the software shall be guaranteed to meet the requirements in the Performance Work Statement and all Exhibits of the contract after the completion of Phase 4: IOC Integration and Testing (See Schedule B: SLIN 1001D).

The software vendor warrants from the date of completion of Phase 4 on which the software specified in the contract is first used in production by ICE that the software will perform in all material respects to the functions described in ICE's ICM requirements specified in this contract. This warranty is effective for each year of the contract.

License Rights in Software Modifications
Any software modifications made to the system under this contract shall be provided to the government with unlimited rights. Unlimited rights means that the Government has unlimited rights to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so as defined in FAR 27.401. ICE shall also obtain unlimited rights in any other data first produced in performance of this contract, form fit, and function data and all other data delivered under the contract other than restricted rights in commercial computer software. The Contractor shall not incorporate any software modifications made specifically under this contract into the Contractor's Commercial Computer Software, including Open Source Software, or any third party software, without prior written approval from the ICE Contracting Officer IAW FAR 52.227-17.

Third Party Software
Contractor has obtained all necessary licenses for ICE to any Third Party Materials (including without limitation, all Open Source licenses) provided with each Product. Contractor complies with and shall continue to comply with all third party licenses (including, without limitation, all Open Source licenses) associated with any Third Party Materials provided with each Product. To the extent any Third Party Materials are provided with a Product, ICE's use of such Product as provided by the Contractor or Software Publisher and in accordance with contract issued hereunder will not be in conflict with any third party license requirements and will satisfy all conditions on use, modification or distribution of any such Third Party Materials without the need for any additional, unanticipated action or license fees on ICE's part; ICE does not and will not need to procure any rights or licenses to any patents or other third-party intellectual property rights to use as intended in this contract hereunder the Product delivered by Software Publisher or Contractor.

Audit
In lieu of any audit provisions in the license agreement, Licensee (ICE) may perform an internal audit and will use its best efforts to keep full and accurate accounts that may be used to properly ascertain and verify numbers of licenses in use.

Order of Precedence
The terms and conditions of set forth in section H take precedence over any conflicting Software Publisher license terms and conditions including those found in a Software Publisher or Third Party Software Click Wrap license, whether presented in writing or electronically; whether presented prior to or subsequent to executing this contract. ICE and its users shall not be bound by the terms of a Click Wrap license encountered during installation or at any time thereafter, notwithstanding ICE users clicking 'Accept' in order to continue using the Software.

SECTION I-CONTRACT CLAUSES

I.1-CLAUSES INCORPORATED BY REFERENCE

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 at these addresses:

https://www.acquisition.gov/far/index.html
https://www.acquisition.gov/gsam/gsam.html

(End of Clause)

Clause	Description	Date
52.202-1	Definitions	Nov-13
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	Jan-97
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Oct-10
52.203-13	Contractor Code of Business Ethics and Conduct	Apr-10
52.203-3	Gratuities	Apr-84
52.203-5	Covenant Against Contingent Fees	Apr-84
52.203-6	Restrictions on Subcontractor Sales to the Government	Sep-06
52.203-7	Anti-Kickback Procedures	Oct-10
52.203-8	Cancellation, Recession, and Recovery of Funds for Illegal or Improper Activity	Jan-97
52.203-17	Contractor Employee Whistleblower Rights and Requirements to Inform Employees of Whistleblower Rights.	Sep-13
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	May-11
52.204-9	Personal Identity Verification of Contractor Personnel	Jan-11
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	Jul-13
52.204-13	System for Award Management Maintenance	Jul-13
52.204-14	Service Contract Reporting Requirements	Jan-14
52.209-6	Protecting the Government's Interest when Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	Aug-13
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	July 13

52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	May-12
52.210-1	Market Research	Apr 11
52.215-2	Audit and Records-Negotiation	Oct 10
52.215-8	Order of Precedence-Uniform Contract Format	Oct-97
52.215-14	Integrity of Unit Prices	Oct 10
52.219-16	Liquidated Damages-Subcontracting Plan	Jan 99
52.219-28	Post-Award Small Business Program Representation	Jul-13
52.219-8	Utilization of Small Business Concerns	Jul-13
52.222-3	Convict Labor	Jun-03
52.222-17	Nondisplacement of Qualified Workers	Jan 13
52.222-21	Prohibition of Segregated Facilities	Feb-99
52.222-26	Equal Opportunity (Provision)	Mar-07
52.222-35	Equal Opportunity for Veterans	Sep-10
52.222-36	Affirmative Action for Workers with Disabilities	Oct-10
52.222-37	Employment Reports on Veterans	Sep-10
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	Dec-10
52.222-50	Combating Trafficking in Persons	Feb-09
52.223-5	Pollution Prevention and Right-to-Know Information	May-11
52.223-6	Drug-Free Workplace	May-01
52.223-18	Contractor Policies to Ban Text Messaging While Driving	Aug-11
52.224-1	Privacy Act Notification	Apr-84
52.224-2	Privacy Act	Apr-84
52.225-1	Buy American Act-Supplies	Feb-09
52.225-13	Restrictions on Certain Foreign Purchases	Jun-08
52.227-1	Authorization and Consent	Dec-07
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	Dec-07
52.227-3	Patent Indemnity	Apr-84
52.227-14	Rights in Data-General, Alt. III	Dec-07
52.227-16	Additional Data Requirements	June 87
52.227-17	Rights in Data-Special Works	Dec-07
52.227-19	Commercial Computer Software License	Dec-07
52.227-21	Technical Data Declaration, Revision, and Withholding of Payment-Major Systems	Dec 07
52.227-22	Major System-Minimum Rights	June 87
52.228-5	Insurance-Work on a Government Installation	Jan-97
52.229-3	Federal, State, and Local Taxes	Feb 13

52.232-1	Payments	Apr-84
52.232-7	Payments under Time-and-Materials and Labor-Hour Contracts	Aug 12
52.232-8	Discounts for Prompt Payment	Feb-02
52.232-11	Extras	Apr-84
52.232-17	Interest	Oct-10
52.232-23	Assignment of Claims	Jan-86
52.232-25	Prompt Payment	Jul-13
52.232-33	Payment by Electronic Funds Transfer-System for Award Management	Jul-13
52.232-39	Unenforceability of Unauthorized Obligations	Jun-13
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	Dec-13
52.233-1	Disputes, Alt. I	Dec 91
52.233-3	Protest after Award	Aug-96
52.233-4	Applicable Law for Breach of Contract Claim	Oct-04
52.239-1	Privacy or Security Safeguards	Aug-96
52.242-13	Bankruptcy	Jul-95
52.243-1	Changes-Fixed Price-Alt II	Apr-84
52.243-3	Changes-Time-and-Materials or Labor-Hours	Sept 00
52.243-7	Notification of Changes	April 84
52.244-6	Subcontracts for Commercial Items.	Dec 13
52.246-20	Warranty of Services	May 01
52.246-25	Limitation of Liability-Services	Feb 97
52.248-1	Value Engineering	Oct 10
52.249-2	Termination for Convenience of the Government (Fixed Price)	Apr-12
52.249-8	Default (Fixed-Price Supply and Service)	Apr-84

I.2-FAR CLAUSES IN FULL TEXT

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 six (6) months. The Contracting Officer may exercise the option by written notice to the Contractor at least 15 days before the contract 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 15 days of contract expiration; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years and six (6) months.

(End of Clause)

FAR 52.219-9 Small Business Subcontracting Plan, Alt. II (Oct. 01), DEVIATION 2013-O0014 (AUG 2013)

(a) This clause does not apply to small business concerns.

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

"Alaska Native Corporation (ANC)" means any Regional Corporation, Village Corporation, Urban Corporation, or Group Corporation organized under the laws of the State of Alaska in accordance with the Alaska Native Claims Settlement Act, as amended (43 U.S.C. 1601, *et seq.*) and which is considered a minority and economically disadvantaged concern under the criteria at 43 U.S.C. 1626(e)(1). This definition also includes ANC direct and indirect subsidiary corporations, joint ventures, and partnerships that meet the requirements of 43 U.S.C. 1626 (e)(2).

"Commercial item" means a product or service that satisfies the definition of commercial item in section 2.101 of the Federal Acquisition Regulation.

"Commercial plan" means a subcontracting plan (including goals) that covers the offeror's fiscal year and that applies to the entire production of commercial items sold by either the entire company or a portion thereof (*e.g.*, division, plant, or product line).

"Electronic Subcontracting Reporting System (eSRS)" means the Governmentwide, electronic, web-based system for small business subcontracting program reporting. The eSRS is located at http://www.esrs.gov.

"Indian tribe" means any Indian tribe, band, group, pueblo, or community, including native villages and native groups (including corporations organized by Kenai, Juneau, Sitka, and Kodiak) as defined in the Alaska Native Claims Settlement Act (43 U.S.C.A. 1601 *et seq.*), that is recognized by the Federal Government as eligible for services from the Bureau of Indian

Affairs in accordance with 25 U.S.C. 1452(c). This definition also includes Indian-owned economic enterprises that meet the requirements of 25 U.S.C. 1452(e).

"Individual contract plan" means a subcontracting plan that covers the entire contract period (including option periods), applies to a specific contract, and has goals that are based on the offeror's planned subcontracting in support of the specific contract except that indirect costs incurred for common or joint purposes may be allocated on a prorated basis to the contract.

"Master plan" means a subcontracting plan that contains all the required elements of an individual contract plan, except goals, and may be incorporated into individual contract plans, provided the master plan has been approved.

"Subcontract" means any agreement (other than one involving an employer-employee relationship) entered into by a Federal Government prime Contractor or subcontractor calling for supplies or services required for performance of the contract or subcontract.

(c) Proposals submitted in response to this solicitation shall include a subcontracting plan, that separately addresses subcontracting with small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns. If the offeror is submitting an individual contract plan, the plan must separately address subcontracting with small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns with a separate part for the basic contract and separate parts for each option (if any). The plan shall be included in and made a part of the resultant contract. The subcontracting plan shall be negotiated within the time specified by the Contracting Officer. Failure to submit and negotiate a subcontracting plan shall make the offeror ineligible for award of a contract.

(d) The offeror's subcontracting plan shall include the following:

(1) Goals, expressed in terms of percentages of total planned subcontracting dollars, for the use of small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns as subcontractors. The offeror shall include all subcontracts that contribute to contract performance, and may include a proportionate share of products and services that are normally allocated as indirect costs. In accordance with 43 U.S.C. 1626:

(i) Subcontracts awarded to an ANC or Indian tribe shall be counted towards the subcontracting goals for small business and small disadvantages business (SDB) concerns, regardless of the size or Small Business Administration certification status of the ANC or Indian tribe.

(ii) Where one or more subcontractors are in the subcontract tier between the prime contractor and the ANC or Indian tribe, the ANC or Indian tribe shall

designate the appropriate contractor(s) to count the subcontract towards its small business and small disadvantaged business subcontracting goals.

(A) In most cases, the appropriate Contractor is the Contractor that awarded the subcontract to the ANC or Indian tribe.

(B) If the ANC or Indian tribe designates more than one Contractor to count the subcontract toward its goals, the ANC or Indian tribe shall designate only a portion of the total subcontract award to each Contractor. The sum of the amounts designated to various Contractors cannot exceed the total value of the subcontract.

(C) The ANC or Indian tribe shall give a copy of the written designation to the Contracting Officer, the prime Contractor, and the subcontractors in between the prime Contractor and the ANC or Indian tribe within 30 days of the date of the subcontract award.

(D) If the Contracting Officer does not receive a copy of the ANC's or the Indian tribe's written designation within 30 days of the subcontract award, the Contractor that awarded the subcontract to the ANC or Indian tribe will be considered the designated Contractor.

(2) A statement of—

(i) Total dollars planned to be subcontracted for an individual contract plan; or the offeror's total projected sales, expressed in dollars, and the total value of projected subcontracts to support the sales for a commercial plan;

(ii) Total dollars planned to be subcontracted to small business concerns (including ANC and Indian tribes);

(iii) Total dollars planned to be subcontracted to veteran-owned small business concerns;

(iv) Total dollars planned to be subcontracted to service-disabled veteran-owned small business;

(v) Total dollars planned to be subcontracted to HUBZone small business concerns;

(vi) Total dollars planned to be subcontracted to small disadvantaged business concerns (including ANCs and Indian tribes); and

(vii) Total dollars planned to be subcontracted to women-owned small business concerns.

(3) A description of the principal types of supplies and services to be subcontracted, and an identification of the types planned for subcontracting to --

(i) Small business concerns,

(ii) Veteran-owned small business concerns;

(iii) Service-disabled veteran-owned small business concerns;

(iv) HUBZone small business concerns;
(v) Small disadvantaged business concerns, and
(vi) Women-owned small business concerns.

(4) A description of the method used to develop the subcontracting goals in paragraph (d)(1) of this clause.

(5) A description of the method used to identify potential sources for solicitation purposes (*e.g.*, existing company source lists, the System for Award Management (SAM), veterans service organizations, the National Minority Purchasing Council Vendor Information Service, the Research and Information Division of the Minority Business Development Agency in the Department of Commerce, or small, HUBZone, small disadvantaged, and women-owned small business trade associations). A firm may rely on the information contained in SAM as an accurate representation of a concern's size and ownership characteristics for the purposes of maintaining a small, veteran-owned small, service-disabled veteran-owned small, HUBZone small, small disadvantaged, and women-owned small business source list. Use of SAM as its source list does not relieve a firm of its responsibilities (*e.g.*, outreach, assistance, counseling, or publicizing subcontracting opportunities) in this clause.

(6) A statement as to whether or not the offeror included indirect costs in establishing subcontracting goals, and a description of the method used to determine the proportionate share of indirect costs to be incurred with --

(i) Small business concerns (including ANC and Indian tribes);

(ii) Veteran-owned small business concerns;

(iii) Service-disabled veteran-owned small business concerns;

(iv) HUBZone small business concerns;

(v) Small disadvantaged business concerns (including ANC and Indian tribes); and

(vi) Women-owned small business concerns.

(7) The name of the individual employed by the offeror who will administer the offeror's subcontracting program, and a description of the duties of the individual.

(8) A description of the efforts the offeror will make to assure that small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns have an equitable opportunity to compete for subcontracts.

(9) Assurances that the offeror will include the clause of this contract entitled "Utilization of Small Business Concerns" in all subcontracts that offer further subcontracting opportunities, and that the offeror will require all subcontractors (except small business concerns) that receive subcontracts in excess of $650,000 ($1.5 million for construction of any public facility with further subcontracting possibilities) to adopt a plan similar to the plan that complies with the requirements of this clause.

(10) Assurances that the offeror will --

(i) Cooperate in any studies or surveys as may be required;

(ii) Submit periodic reports so that the Government can determine the extent of compliance by the offeror with the subcontracting plan;

(iii) Submit the Individual Subcontracting Report (ISR) and/or the Summary Subcontract Report (SSR), in accordance with the paragraph (l) of this clause using the Electronic Subcontracting Reporting System (eSRS) at http://www.esrs.gov . The reports shall provide information on subcontract awards to small business concerns (including ANCs and Indian tribes that are not small businesses), veteran-owned small business concerns, service-disabled veteran-owned small business concerns, HUBZone small business concerns, small disadvantaged business concerns (including ANCs and Indian tribes that have not been certified by the Small Business Administration as small disadvantaged businesses), women-owned small business concerns, and Historically Black Colleges and Universities and Minority Institutions. Reporting shall be in accordance with this clause, or as provided in agency regulations;

(iv) Ensure that its subcontractors with subcontracting plans agree to submit the ISR and/or the SSR using eSRS;

(v) Provide its prime contract number, its DUNS number, and the e-mail address of the offeror's official responsible for acknowledging receipt of or rejecting the ISRs, to all first-tier subcontractors with subcontracting plans so they can enter this information into the eSRS when submitting their ISRs; and

(vi) Require that each subcontractor with a subcontracting plan provide the prime contract number, its own DUNS number, and the e-mail address of the

subcontractor's official responsible for acknowledging receipt of or rejecting the ISRs, to its subcontractors with subcontracting plans.

(11) A description of the types of records that will be maintained concerning procedures that have been adopted to comply with the requirements and goals in the plan, including establishing source lists; and a description of the offeror's efforts to locate small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns and award subcontracts to them. The records shall include at least the following (on a plant-wide or company-wide basis, unless otherwise indicated):

(i) Source lists (*e.g.*, SAM), guides, and other data that identify small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns.

(ii) Organizations contacted in an attempt to locate sources that are small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, or women-owned small business concerns.

(iii) Records on each subcontract solicitation resulting in an award of more than $150,000, indicating --

(A) Whether small business concerns were solicited and if not, why not;

(B) Whether veteran-owned small business concerns were solicited and, if not, why not;

(C) Whether service-disabled veteran-owned small business concerns were solicited and, if not, why not;

(D) Whether HUBZone small business concerns were solicited and, if not, why not;

(E) Whether small disadvantaged business concerns were solicited and if not, why not;

(F) Whether women-owned small business concerns were solicited and if not, why not; and

(G) If applicable, the reason award was not made to a small business concern.

(iv) Records of any outreach efforts to contact --

(A) Trade associations;

(B) Business development organizations;

(C) Conferences and trade fairs to locate small, HUBZone small, small disadvantaged, and women-owned small business sources; and

(D) Veterans service organizations.

(v) Records of internal guidance and encouragement provided to buyers through -

(A) Workshops, seminars, training, etc., and

(B) Monitoring performance to evaluate compliance with the program's requirements.

(vi) On a contract-by-contract basis, records to support award data submitted by the offeror to the Government, including the name, address, and business size of each subcontractor. Contractors having commercial plans need not comply with this requirement.

(e) In order to effectively implement this plan to the extent consistent with efficient contract performance, the Contractor shall perform the following functions:

(1) Assist small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns by arranging solicitations, time for the preparation of bids, quantities, specifications, and delivery schedules so as to facilitate the participation by such concerns. Where the Contractor's lists of potential small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business subcontractors are excessively long, reasonable effort shall be made to give all such small business concerns an opportunity to compete over a period of time.

(2) Provide adequate and timely consideration of the potentialities of small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business concerns in all "make-or-buy" decisions.

(3) Counsel and discuss subcontracting opportunities with representatives of small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business, small disadvantaged business, and women-owned small business firms.

(4) Confirm that a subcontractor representing itself as a HUBZone small business concern is identified as a certified HUBZone small business concern by accessing the SAM database or by contacting SBA.

(5) Provide notice to subcontractors concerning penalties and remedies for misrepresentations of business status as small, veteran-owned small business, HUBZone small, small disadvantaged or women-owned small business for the purpose of obtaining a subcontract that is to be included as part or all of a goal contained in the Contractor's subcontracting plan.

(6) For all competitive subcontracts over the simplified acquisition threshold in which a small business concern received a small business preference, upon determination of the successful subcontract offeror, the Contractor must inform each unsuccessful small business subcontract offeror in writing of the name and location of the apparent successful offeror prior to award of the contract.

(f) A master plan on a plant or division-wide basis that contains all the elements required by paragraph (d) of this clause, except goals, may be incorporated by reference as a part of the subcontracting plan required of the offeror by this clause; provided --

(1) The master plan has been approved;

(2) The offeror ensures that the master plan is updated as necessary and provides copies of the approved master plan, including evidence of its approval, to the Contracting Officer; and

(3) Goals and any deviations from the master plan deemed necessary by the Contracting Officer to satisfy the requirements of this contract are set forth in the individual subcontracting plan.

(g) A commercial plan is the preferred type of subcontracting plan for contractors furnishing commercial items. The commercial plan shall relate to the offeror's planned subcontracting generally, for both commercial and Government business, rather than solely to the Government contract. Once the Contractor's commercial plan has been approved, the Government will not require another subcontracting plan from the same Contractor while the plan remains in effect, as long as the product or service being provided by the Contractor continues to meet the definition of a commercial item. A contractor with a commercial plan shall comply with the reporting requirements stated in paragraph (d)(10) of this clause by submitting one SSR in eSRS for all contracts covered by its commercial plan. This report shall be acknowledged or rejected in eSRS by the Contracting Officer who approved the plan. This report shall be submitted within 30 days after the end of the Government's fiscal year.

(h) Prior compliance of the offeror with other such subcontracting plans under previous contracts will be considered by the Contracting Officer in determining the responsibility of the offeror for award of the contract.

(i) A contract may have no more than one plan. When a modification meets the criteria in 19.702 for a plan, or an option is exercised, the goals associated with the modification or option shall be added to those in the existing subcontract plan.

(j) Subcontracting plans are not required from subcontractors when the prime contract contains the clause at 52.212-5, Contract Terms and Conditions Required to Implement Statutes or Executive Orders—Commercial Items, or when the subcontractor provides a commercial item subject to the clause at 52.244-6, Subcontracts for Commercial Items, under a prime contract.

(k) The failure of the Contractor or subcontractor to comply in good faith with—

(1) The clause of this contract entitled "Utilization Of Small Business Concerns;" or

(2) An approved plan required by this clause, shall be a material breach of the contract.

(l) The Contractor shall submit ISRs and SSRs using the web-based eSRS at http://www.esrs.gov. Purchases from a corporation, company, or subdivision that is an affiliate of the prime Contractor or subcontractor are not included in these reports. Subcontract award data reported by prime Contractors and subcontractors shall be limited to awards made to their immediate next-tier subcontractors. Credit cannot be taken for awards made to lower tier subcontractors unless the Contractor or subcontractor has been designated to receive a small business or small disadvantaged business credit from an ANC or Indian tribe. Only subcontracts involving performance in the United States or its outlying areas should be included in these reports with the exception of subcontracts under a contract awarded by the State Department or any other agency that has statutory or regulatory authority to require subcontracting plans for subcontracts performed outside the United States and its outlying areas.

(1) *ISR*. This report is not required for commercial plans. The report is required for each contract containing an individual subcontract plan.

(i) The report shall be submitted semi-annually during contract performance for the periods ending March 31 and September 30. A report is also required for each contract within 30 days of contract completion. Reports are due 30 days after the close of each reporting period, unless otherwise directed by the Contracting Officer. Reports are required when due, regardless of whether there has been any subcontracting activity since the inception of the contract or the previous reporting period.

(ii) When a subcontracting plan contains separate goals for the basic contract and each option, as prescribed by FAR 19.704(c), the dollar goal inserted on this report shall be the sum of the base period through the current option; for example, for a report submitted after the second option is exercised, the dollar goal would be the sum of the goals for the basic contract, the first option, and the second option.

(iii) The authority to acknowledge receipt or reject the ISR resides—

(A) In the case of the prime Contractor, with the Contracting Officer; and

(B) In the case of a subcontract with a subcontracting plan, with the entity that awarded the subcontract.

(2) *SSR.*

(i) Reports submitted under individual contract plans—

(A) This report encompasses all subcontracting under prime contracts and subcontracts with the awarding agency, regardless of the dollar value of the subcontracts.

(B) The report may be submitted on a corporate, company or subdivision (*e.g.* plant or division operating as a separate profit center) basis, unless otherwise directed by the agency.

(C) If a prime contractor and/or subcontractor is performing work for more than one executive agency, a separate report shall be submitted to each executive agency covering only that agency's contracts, provided at least one of that agency's contracts is over $650,000 (over $1.5 million for construction of a public facility) and contains a subcontracting plan. For DoD, a consolidated report shall be submitted for all contracts awarded by military departments/agencies and/or subcontracts awarded by DoD prime Contractors.

(D) The consolidated SSR shall be submitted annually for the twelve month period ending September 30. The report is due 30 days after the close of the reporting period.

(E) Subcontract awards that are related to work for more than one executive agency shall be appropriately allocated.

(F) The authority to acknowledge or reject SSRs in eSRS, including SSRs submitted by subcontractors with subcontracting plans, resides with the Government agency awarding the prime contracts unless stated otherwise in the contract.

(ii) Reports submitted under a commercial plan—

(A) The report shall include all subcontract awards under the commercial plan in effect during the Government's fiscal year.

(B) The report shall be submitted annually, within thirty days after the end of the Government's fiscal year.

(C) If a Contractor has a commercial plan and is performing work for more than one executive agency, the Contractor shall specify the percentage of dollars attributable to each agency from which contracts for commercial items were received.

(D) The authority to acknowledge or reject SSRs for commercial plans resides with the Contracting Officer who approved the commercial plan.

(iii) All reports submitted at the close of each fiscal year (both individual and commercial plans) shall include a Year-End Supplementary Report for Small Disadvantaged Businesses. The report shall include subcontract awards, in whole dollars, to small disadvantaged business concerns by North American Industry Classification System (NAICS) Industry Subsector. If the data are not available when the year-end SSR is submitted, the prime Contractor and/or subcontractor shall submit the Year-End Supplementary Report for Small Disadvantaged Businesses within 90 days of submitting the year-end SSR. For a commercial plan, the Contractor may obtain from each of its subcontractors a predominant NAICS Industry Subsector and report all awards to that subcontractor under its predominant NAICS Industry Subsector.

(End of Clause)

I.3-APPLICABLE HSAM CLAUSES INCORPORATED BY REFERENCE

Clause	Description	Date
3052.203-70	Instructions for Contractor Disclosure of Violations	Sep-12
3052.205-70, ALT 1	Advertisements, Publicizing Awards, and Release	Sep-12
3052.215-70	Key Personnel or Facilities	Dec-03
3052.219-70	Small Business Subcontracting Plan Reporting	Jun-06
3052.219-71	DHS Mentor-Protégé Program	Jun-06
3052.228-70	Insurance	Dec-03
3052.242-72	Contracting Officer's Technical Representative	Dec-03

I.4-APPLICABLE HSAM CLAUSES IN FULL TEXT

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) Within15 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 (SEP 2012), ALT I

(a) *Sensitive Information,* as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, 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, Public Law 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) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and

(2) 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)

HSAM 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 an acquisition described in section 835(b)(1) 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]:

XX it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, 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 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(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 clause)

HSAR 3052.209-73-LIMITATION OF FUTURE CONTRACTING (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict is any contractor providing services under the ICM contract may have access to information that would prohibit them from assisting in preparing proposals for future related acquisitions.

(c) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

ADDITIONAL INFORMATION REGARDING ORGANIZATIONAL CONFLICT OF INTEREST

The following paragraphs in this section clarify the responsibilities of the Contractor regarding organizational conflict of interest.

The contractor agrees that if an actual or potential organizational conflict of interest is discovered after award, the contractor will make a full disclosure in writing to the Contracting Officer no later than three working days after discovery. This disclosure shall include a description of actions which the contractor has taken or proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or neutralize the actual or potential conflict.

The Government may terminate this contract for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If the contractor was aware, or should have been aware, of a potential organizational conflict of interest prior to award, or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for default, debar the contractor from Government contracting, or pursue such other remedies as may be permitted by law or this contract.

The contractor further agrees to insert provisions which shall conform substantially to the language of this clause, including this paragraph, in any subcontract or consultant agreement hereunder.

SECTION J-LIST OF ATTACHMENTS

Attachment 1-Performance Work Statement

- *Exhibit A: ICE/HSI Investigative Case Management System Requirements-Law Enforcement Sensitive (FINAL AFFIRMATION OF REQUIREMENTS)**

Attachment 2-Quality Assurance Surveillance Plan

Attachment 3-Software License Agreement and Related Material

Attachment 4-Palantir's Response to High Level Capabilities Matrix and Gap Analysis

Attachment 5-BAR FORM

Attachment 6-DHS Form 11000-6

Attachment 7-DHS 4300A Sensitive Systems Handbook Rules of Behavior

Note: Exhibit is Law Enforcement Sensitive

Note: Attachments 1 (including the affirmation of the requirements in Exhibit A), 2, 3, and 4 are part of Palantir's Proposal submitted in response to HSCETC-14-R-00002 and are hereby incorporated by reference. The following applies to Attachments 1, 2, 3, and 4: INCORPORATION OF PROPOSAL PAGES WITH PROPRIETARY MARKINGS: The contractor agrees that the government may duplicate, use and/or disclose inside the government, the pages of its proposal which have been incorporated into this contract as necessary to implement and administer this contract. Such pages shall retain any proprietary markings placed thereon by the contractor, and the data which is marked proprietary shall not be disclosed outside the government unless (a) required by law, (b) agreed to by the contractor, or (c) disclosed to a government support contractor who has signed an appropriate non-disclosure agreement and has agreed to adequately protect such data."

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 8

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. (If applicable)
P00002	See Block 16C	192115CIOSDD10003.1	

6. ISSUED BY	CODE	7. ADMINISTERED BY (If other than Item 6)	CODE
ICE/Information Technology Division Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW, (b)(6);(b)(7)(C) Washington DC 20536	ICE/ITD		

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)		9A. AMENDMENT OF SOLICITATION NO.
PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853	(x)	9B. DATED (SEE ITEM 11)
	X	10A. MODIFICATION OF CONTRACT/ORDER NO. HSCETC-14-C-00002
		10B. DATED (SEE ITEM 13) 09/25/2014

CODE 9673917930000	FACILITY CODE

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

Net Increase: (b)(4)

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.
	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:
X	D. OTHER (Specify type of modification and authority) FAR 52.243-1: Changes-Fixed Price-Alt II (APR-84)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

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

DUNS Number: 825284321
The purpose of this modification is to:

1. Add CLINs XX07, XX08, XX09, and XX10 to Option Years 1-5 for the Amazon Web Services (AWS) hosting solution;

2. Incorporate the revised Performance Work Statement and the revised Sections A-J;

3. Incorporate the attached ICE Cloud Addendum (to include Exhibit A-License and Services Agreement, dated 26 Sept. 2014 and the AWS Terms and Conditions and Federal Access Policy) into the contract; and

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)	15C. DATE SIGNED	16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	16C. DATE SIGNED
(b)(6);(b)(7)(C)	4/15/20	(b)(6);(b)(7)(C)	4/16/2015

NSN 7540-01-152-8070
Previous edition unusable

ARD FORM 30 (REV. 10-83)
ed by GSA
CFR) 53.243

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	4. Decrease the total amounts for CLINs 1001, 2005, 3005, 4005, and 5005 (see individual CLINs for specific amounts). As a result, the total obligated amount is increased from (b)(4) to (b)(4) The total amount is increased from (b)(4) to (b)(4) All other terms and conditions remain the same. Exempt Action: Y Discount Terms: Net 30 FOB: Destination Period of Performance: 09/26/2014 to 09/24/2019 Change Item 1001 to read as follows(amount shown is the obligated amount):				
1001	P00002: Decrease amount from (b)(4) by (b)(4) and re-align (b)(4) to CLIN 1007. Labor for Transition-In (Two Months) and IOC FFP: (b)(4) SLIN 1001A: Completion of Transition-In: (b)(4) (5% of FFP) SLIN 1001B: Phase 1-Requirements Confirmation and Baseline Installation: (b)(4) (10% of FFP) SLIN 1001C: Phase 2-Baseline Gap Analysis: (b)(4) (10% of FFP) SLIN 1001D: Phase 3-Code Freeze for IOC: (b)(4) (25% of FFP) SLIN 1001E: Phase 4-IOC Integration and Testing: (b)(4) (50% of FFP) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: TECS081-001 Y5 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4) Accounting Info: TECS081-001 Y6 80-99-00-000 Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 000000 Funded: (b)(4)				
	Add Item 1007 as follows:				
1007	Combined GovCloud Instances (252 Servers) Not-to-Exceed Amount: (b)(4) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 QC0000 Funded: (b)(4) Accounting Info: TECS081-001 Y5 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00- ------ --- QC0000 Funded: (b)(4)				(b)(4)
	Add Item 1008 as follows:				
1008	Networking and Data Transfer-FFP Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: (b)(4);(b)(7)(E)				(b)(4)
	Add Item 1009 as follows:				
1009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: Continued ...				(b)(4)

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 QC0000 Funded: (b)(4) Accounting Info: TECS081-001 Y5 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00-000000 00-00-0000-00-00-00-00 000000-000000-000000-000000 QC0000 Funded: (b)(4) Add Item 1010 as follows:				
1010	Software as a Service (b)(4) Not-to-Exceed Amount: (b)(4) Obligated Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Accounting Info: TECS081-001 Y6 80-99-00-000 23-02-0200-00-00-00-00 GE-31-15-00- ------ --- QC0000 Funded: (b)(4) Change Item 2005 to read as follows(amount shown is the obligated amount):				(b)(4)
2005	P00002: Decrease amount from (b)(4) by (b)(4) Support to include Tier 2 and Tier 3 Service Desk Support as referenced in Exhibit A, Section 2. Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 2 (12 months) Amount: (b)(4) Option Line Item) 09/25/2015 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 2007 as follows:				(b)(4)
2007	Combined GovCloud Instances (252 Servers) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) Option Line Item) 09/26/2016 Continued ...				(b)(4)

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 2008 as follows:				
2008	Networking and Data Transfer-FFP Amount: (b)(4) (Option Line Item) 09/26/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 2009 as follows:				(b)(4)
2009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Amount: (b)(4) Option Line Item) 09/26/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 2010 as follows:				(b)(4)
2010	Software as a Service (b)(4) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) Option Line Item) 09/26/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Change Item 3005 to read as follows(amount shown is the obligated amount):				(b)(4)
3005	P00002: Decrease amount from (b)(4) by (b)(4) Support to include Tier 2 and Tier 3 Service Desk Support as referenced in Exhibit A, Section 2 Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 3 (12 months) Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Add Item 3007 as follows:				
3007	Combined GovCloud Instances (252 Servers) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Add Item 3008 as follows:				
3008	Networking and Data Transfer-FFP Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Add Item 3009 as follows:				
3009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Amount: (b)(4) Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Add Item 3010 as follows:				
3010	Software as a Service (b)(4) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2016 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Change Item 4005 to read as follows(amount shown is the obligated amount):				
4005	P00002: Decrease total amount from (b)(4) by (b)(4) Support to include Tier 2 and Tier 3 Service Desk Support as referenced in Exhibit A, Section 2 Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 4 (12 months) Continued ...				(b)(4)

ITEM NO (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 4007 as follows:				
4007	Combined GovCloud Instances (252 Servers) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 4008 as follows:				(b)(4)
4008	Networking and Data Transfer-FFP Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 4009 as follows:				(b)(4)
4009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 4010 as follows:				(b)(4)
4010	Software as a Service (b)(4) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2017 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Change Item 5005 to read as follows(amount shown is the obligated amount):				(b)(4)
5005	P00002: Decrease total amount from (b)(4) by (b)(4) Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Support to include Tier 2 and Tier 3 Service Desk Support as referenced in Exhibit A, Section 2. Monthly FFP: (b)(4) Total FFP: (b)(4) Option Period 5 (12 months) Amount: (b)(4) Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 5007 as follows:				
5007	Combined GovCloud Instances (252 Servers) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 5008 as follows:				(b)(4)
5008	Networking and Data Transfer-FFP Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 5009 as follows:				(b)(4)
5009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE Add Item 5010 as follows:				(b)(4)
5010	Software as a Service (b)(4) Not-to-Exceed Amount: (b)(4) Amount: (b)(4) (Option Line Item) 09/25/2018 Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)

(b)(4);(b)(5);(b)(7)(E) **ADDENDUM TO LICENSE AND SERVICES AGREEMENT**

(b)(4);(b)(5);(b)(7 Addendum ("Addendum") is hereby appended to the License and Services Agreement ("Agreement") effective September 26, 2014, attached as Exhibit A, entered into pursuant to Contract HSCETC-14-C-00002, by and between Contractor ("**Palantir**") and U.S. Department of Homeland Security, Immigration and Customs Enforcement ("**ICE**" or "**Customer**" and, collectively with Palantir, the "**Parties**").

(b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

15. Certain Definitions. (b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

16.2 Authorized User Accounts. (b)(4);(b)(5);(b)(

(b)(4);(b)(5);(b)(7)(E)

16. (b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

17. AWS Terms and Conditions. (b)(4);(b)(5);(b)(

(b)(4);(b)(5);(b)(7)(E)

18. (b)(4);(b)(5);(b)(7)(E)

(b)(4);(b)(5);(b)(7)(E)

19. Customer Representations and Warranties.

(b)(4);(b)(5);(b)(7)(E)

EXHIBIT A

License and Services Agreement, dated 26 Sep 2014 (to be attached)

EXHIBIT B

AWS Federal Access Policy, GovCloud Addendum and GovCloud Affirmation of Compliance (to be attached) (collectively, "AWS Terms").

For avoidance of doubt, this contract, including any AWS Terms, will be governed by and interpreted and enforced in accordance with the laws of the United States of America without reference to conflict of laws.

AWS Access Policy - Federal
(v.1-4-2013)

This AWS Access Policy ("**Access Policy**") governs your access to and use of the Services (as defined below) of Amazon Web Services, Inc. ("**AWS**") provided to you by your systems integrator, reseller, or services provider ("**Provider**"). It sets out the additional rules, conditions and restrictions that apply to you or the entity you represent ("**you**") for use of the Services. In this Access Policy, "**we**", "**us**", or "**our**" means AWS and any of its affiliates. Please see Section 8 for definitions of capitalized terms.

1. Use of the Services.

1.1 Generally. You are provided access to the Services by your Provider. Your use of and access to the Services are governed by the agreement between you and Provider. This Access Policy supplements the terms of such agreement and may be updated by us from time to time. AWS Service Level Agreements apply to your use of the Services. Your continued access to and use of the Services is conditioned on your compliance with all laws, rules, regulations, policies and instructions applicable to your use of the Services, including the Policies.

1.2 Account Keys. Provider may provide you with AWS account keys which will allow you to directly access the Services via Provider's account(s). We are not responsible for any activities that occur under these account keys, regardless of whether the activities are undertaken by you, Provider or a third party (including your employees, contractors or agents) and we are also not responsible for unauthorized access to the account.

1.3 Third Party Materials. Through the use of Provider's AWS account(s), you may have access to Third Party Materials, such as software applications provided by third parties, which are made available directly to you by other companies or individuals under separate terms and conditions, including separate fees and charges. Your use of any Third Party Materials is at your sole risk.

2. Your Responsibilities

2.1 Your Materials. You are solely responsible for the development, content, operation, maintenance, and use of Your Materials with the Services. For example, you are solely responsible for:

(a) the technical operation of Your Materials, including ensuring that calls you make to any Service are compatible with then-current application program interfaces for that Service;

(b) compliance of Your Materials with the Acceptable Use Policy, the other Policies, and the law;

(c) any claims relating to Your Materials;

(d) properly handling and processing notices sent to you (or any of your affiliates) by any person claiming that Your Materials violate such person's rights, including notices pursuant to the Digital Millennium Copyright Act;

(e) any action that you permit, assist or facilitate any person or entity to take related to this Access Policy, Your Materials or use of the Services; and

(f) End Users' use of Your Materials and the Services and ensuring that End Users comply with your obligations under this Access Policy and that the terms of your agreement with each End User are consistent with this Access Policy.

2.2 Other Security and Backup. You or Provider are solely responsible for properly configuring and using the Services and taking steps to maintain appropriate security, protection and backup of Your Materials, including using encryption technology to protect Your Materials from unauthorized access and routinely archiving Your Materials.

2.3 End User Violations. If you become aware of any violation of your obligations under this Access Policy by an End User, you will immediately terminate such End User's access to Your Materials and the Services.

3. Service Interruption.

3.1 General. We may suspend the AWS account(s) through which you access the Services immediately if we determine your or an End User's use of the Services (i) violates the terms of this Access Policy (including the Acceptable Use Policy or Service Terms); (ii) poses a security risk to the Services or any other AWS customer, (iii) may harm our systems or the systems or Materials of any other AWS customer; or (iv) may subject us to liability as a result of any of the foregoing. We will provide notice of any suspension as soon as practicable to Provider, who is solely responsible for providing any notices to you under your agreement with them.

3.2 Scope of Interruption. To the extent practicable, we will (i) suspend your right to access or use only those instances, data, or portions of the Services that caused the suspension, and (ii) limit the suspension to those accounts that caused the suspension. If commercially feasible, access to the Services will be restored once the conditions or circumstances giving rise to the suspension have been removed or corrected. Nothing in this Section 3 will operate to limit your rights or remedies otherwise available to you against Provider under your agreement with them or applicable law.

4. Proprietary Rights

4.1 Services. As between you and us, we or our licensors own and reserve all right, title, and interest in and to the Services. You have the right to use the Services solely as a licensee of Provider in accordance with this Access Policy and the agreement between you and Provider. We have no obligation to provide the Service to you under this Access Policy, so you must look exclusively to Provider and your agreement with Provider regarding such obligation. Except as expressly provided in this Section 4, you obtain no rights to the Services, the AWS Materials or any Third Party Materials.

4.2 Materials. As a part of the Services, you may have access to AWS Materials and Third Party Materials, which may be subject to additional terms and conditions (including the Terms of Use and Apache Software License). By using those materials, you are subject to such additional terms. You are solely responsible for securing any necessary approvals for the download and use of such materials.

4.3 Restrictions. Neither you nor any End User may use the Services in any manner or for any purpose other than as expressly permitted by this Access Policy and the agreement between you and Provider. Neither you nor any End User may, or may attempt to, (a) modify, alter, tamper with, repair, or otherwise create derivative works of any software included in the Services (except to the extent software included in the Services are provided to you under a separate license that expressly permits the creation of derivative works), (b) reverse engineer, disassemble, or decompile the software included in the Services or apply any other process or procedure to derive the source code of any software included in the Services, or (c) access or use the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas. All rights and access granted to you with respect to the Services are conditioned on your continued compliance with this Access Policy, and you will immediately discontinue your use of the Services if you cannot comply with this Access Policy.

4.4 Suggestions. If you provide any Suggestions to us when using the Services, you hereby grant to AWS and its affiliates a perpetual, irrevocable, non-exclusive, worldwide, royalty-free right and license to reproduce, distribute, make derivative works based upon, publicly display, publicly perform, make, have made, use, sell, offer for sale, and import the Suggestions, including the right to sublicense such rights through multiple tiers, alone or in combination.

4.5 U.S. Government Rights. In accordance with Federal Acquisition Regulation (FAR) Sections 12.211 and 12.212, and Defense Federal Acquisition Regulation Supplement (DFARS) Sections 227.7202-1 and 227.7202-3, the Services are provided (as applicable) to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software

documentation," and "technical data" with the same rights and restrictions generally applicable to the Services. If you are using the Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, you will immediately discontinue your use of the Services (including any AWS Materials).

5. Representations and Warranties. You represent and warrant that (a) you and your End Users' use of the Services (including any use by your employees and personnel) will not violate this Access Policy; (b) you or your licensors own all right, title, and interest in and to Your Materials; (c) Your Materials (including the use, development, design, production, advertising, or marketing of your Materials) or the combination of your Materials with other applications, content or processes, do not and will not violate any applicable laws or infringe or misappropriate any third-party rights; and (d) your use of the Services will not cause harm to any End User.

6. Disclaimers. WE PROVIDE THE SERVICES ON AN "AS IS" BASIS TO PROVIDER. WE AND OUR LICENSORS MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND TO YOU, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICES OR ANY THIRD PARTY MATERIALS, INCLUDING ANY WARRANTY THAT THE SERVICES OR THIRD PARTY MATERIALS WILL BE UNINTERRUPTED, ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY MATERIALS, INCLUDING YOUR MATERIALS OR THE THIRD PARTY MATERIALS, WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. EXCEPT TO THE EXTENT PROHIBITED BY LAW, WE AND OUR LICENSORS DISCLAIM ALL WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE.

7. Limitations of Liability. YOU MUST LOOK SOLELY TO PROVIDER AND YOUR AGREEMENT WITH THEM REGARDING ANY CLAIMS OR DAMAGES RELATED TO THE SERVICES. WE AND OUR AFFILIATES OR LICENSORS WILL NOT BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA), EVEN IF A PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NEITHER WE NOR ANY OF OUR LICENSORS WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) YOUR INABILITY TO USE THE SERVICES, INCLUDING AS A RESULT OF ANY (I) SUSPENSION OF YOUR USE OF OR ACCESS TO THE SERVICES, (II) OUR DISCONTINUATION OF ANY OR ALL OF THE SERVICES, OR, (III) ANY UNANTICIPATED OR UNSCHEDULED DOWNTIME OF ALL OR A PORTION OF THE SERVICES FOR ANY REASON; OR (B) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR MATERIALS OR OTHER DATA THAT YOU OR ANY END USER SUBMITS OR USES IN CONNECTION WITH THE SERVICES (INCLUDING AS A RESULT OF YOUR OR ANY END USERS' ERRORS, ACTS OR OMISSIONS).

8. Definitions.

"Acceptable Use Policy" means the policy currently available at http://aws.amazon.com/aup, as it may updated by us from time to time.

"AWS Materials" means Materials we make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Materials does not include the Services.

"AWS Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time.

"AWS Site" means http://aws.amazon.com and any successor or related site designated by us.

"Documentation" means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals, instructions and specifications for the Services currently located at http://aws.amazon.com/documentation, as such documentation may be updated

by us from time to time.

"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Materials; or (b) otherwise accesses or uses the Services through you.

"Materials" means software (including machine images), data, text, audio, video, images or other content.

"Policies" means the Acceptable Use Policy, the Terms of Use, the Service Terms, all restrictions described in the AWS Materials and on the AWS Site, and any other policy or terms referenced in or incorporated into this Access Policy.

"Services" means, collectively or individually (as applicable), the web services made commercially available by us to Provider for use under this Access Policy, including (as applicable) those web services described in the Service Terms.

"Service Terms" means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms, as they may be updated by us from time to time.

"Suggestions" means all suggested improvements to the Services or AWS Materials that you provide to us.

"Terms of Use" means the terms of use located at http://aws.amazon.com/terms/, as they may be updated by us from time to time.

"Third Party Materials" means Materials made available to you by any third party on the AWS Site or in conjunction with the Services.

"Your Materials" means Materials you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services or otherwise transfer, process, use or store in connection with the Services.

GovCloud Addendum to AWS Customer License Terms

The terms of the AWS Access Policy – Federal v.1-4-2013 (the "Agreement") are hereby modified as set forth in this GovCloud Addendum to the AWS Customer License Terms (the "Addendum"). The Addendum also amends the GovCloud Affirmation of Compliance (the "Agreement and Notification") as updated from time to time. Unless otherwise defined in this Addendum, all capitalized terms used in this Addendum will have the meanings ascribed to them in the Agreement. The parties agree as follows:

1. AWS Security.

Without limiting Section 6 or Customer's obligations under Section 2.2, in accordance with the AWS Security Standards AWS will implement reasonable and appropriate measures for the AWS Network designed to: (i) help Customer secure Your Content against accidental or unlawful loss, access or disclosure; (ii) implement the in-scope baseline National Institute of Standards and Technology ("NIST") Special Publication 800-53 Rev 3 controls for a Federal Information Security Management Act ("FISMA") Moderate level system for the AWS Services identified by AWS as FISMA compliant (currently EC2, S3, EBS and VPC); and (iii) for the AWS GovCloud (US) region, maintain physical and logical access controls to limit access to the AWS Network by AWS personnel, including employees and contractors, to U.S. persons, as defined by 22 CFR part 120.15 ("U.S. Persons") ((i), (ii) and (iii) collectively the "Security Objectives").

2. U.S. Persons Restricted Access.

2.1 The AWS GovCloud (US) region is the only AWS region that has physical and logical access controls that limit access to the AWS Network by AWS Personnel to U.S. Persons. Customer represents and warrants that it will only access the AWS GovCloud (US) region if:

(i) Customer is a U.S. Person;

(ii) Customer, if required by the International Traffic In Arms Regulations ("ITAR"), has and will maintain a valid Directorate of Defense Trade Controls registration;

(iii) Customer is not subject to export restrictions under U.S. export control laws and regulations (e.g. Customer is not a denied or debarred party or otherwise subject to sanctions); and

(iv) Customer maintains an effective compliance program to ensure compliance with applicable U.S. export control laws and regulations, including the ITAR. If requested by AWS, Customer agrees to provide AWS with additional documentation and cooperation to verify the accuracy of the representations and warranties set forth in this Section.

2.2 Customer Responsibilities.

Customer is responsible for all physical and logical access controls beyond the AWS Network including, but not limited to, Customer account access, data transmission, encryption, and appropriate storage and processing of data within the AWS GovCloud (US) region. Customer is responsible for verifying that all End Users accessing Your Content in the AWS GovCloud (US) region are eligible to gain access to Your Content. AWS Services may not be used to process or store classified data. If Customer introduces classified data into the AWS Network, Customer will be responsible for all sanitization costs incurred by AWS. Customer's liability under this provision is exempt from any limitations of liability.

3. Definitions.

"AWS Security Standards" means the security standards attached to this Agreement as Attachment B.

"AWS Network" means AWS' data center facilities, servers, networking equipment, and host software systems (e.g., virtual firewalls) that are within AWS' control and are used to provide the Services.

The definition of "End User" is deleted in its entirety and replaced with the following:

"End User" means any entity, person, or United States Federal, State or Local Government agency that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under a Customer account. The term "End User" does not include individuals or entities when they are accessing or using the Services or any Content under their own account, rather than a Customer account.

4. Nondisclosure.
Customer agrees that the existence and details of this Addendum are not publicly known and constitute AWS Confidential Information under the Agreement.

5. Entire Agreement; Conflict. Except as amended by this Addendum, the Agreement will remain in full force and effect. This Addendum, together with the Agreement as amended by this Addendum: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof. If there is a conflict between the Agreement, this Addendum or any other Addendum or addendum to the Agreement or this Addendum, the document later in time will prevail.

[Remainder of Page Intentionally Left Blank.]

ATTACHMENT B
AWS Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the applicable Master Definition List.

1. Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) satisfy the Security Objectives, (b) identify reasonably foreseeable internal risks to security and unauthorized access to the AWS Network, and (c) minimize security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. The information security program for the AWS Services indicated as FISMA compliant will include the in-scope baseline security controls outlined in the NIST Special Publication ("SP") 800-53 Rev 3 for a FISMA Moderate system. The information security program for the AWS GovCloud (US) region will include internal policies, procedures and training that implement physical and logical access controls limiting access to the AWS Network for that region to U.S. Persons only. The information security program for all AWS Services will meet the following measures:

1.1 Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incidence response plans to respond to potential security threats.

1.1.1 Network Security for AWS GovCloud (US). In addition to the security standards set forth in Section 1.1, AWS will not replicate or transmit Your Content hosted, processed, and/or stored in the AWS GovCloud (US) region outside of the United States. AWS limits logical access to AWS's Network for the AWS GovCloud (US) region to authorized U.S. Persons by controlling access credentials, segregating the AWS GovCloud (US) region from other AWS systems, and prohibiting access to the AWS GovCloud (US) region by AWS personnel from points outside of the United States.

1.2 Physical Security

1.2.1 Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

1.2.2 Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access privileges are promptly

revoked, even if the employee or contractor continues to be an employee of AWS or its affiliates.

1.2.3 Physical Security Protections. All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorized access to the Facilities, including monitoring points of vulnerability with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.

1.2.4 Pre-Employment Screening. AWS conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees and contractors commensurate with the employee's or contractor's position and level of access to the Facilities. AWS will not permit an employee or contractor to have access to the non-public Your Content or perform material aspects of the Services if such employee or contractor has failed to pass such background check.

1.2.5 AWS GovCloud (US) Physical Access Controls. All AWS GovCloud (US) region servers are located in the United States. Access to these machines is limited to U.S. Persons. Foreign nationals, as defined by 22 CFR part 120.16, including employees, contractors, and visitors, are not permitted in controlled areas unless properly escorted at all times.

2. Continued Evaluation. For the AWS Services identified as FISMA compliant, AWS in conjunction with 3rd party independent auditors will conduct annual reviews of the security of its AWS Network and adequacy of its information security program as measured against the NIST SP 800-53 security controls. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program applicable to all AWS Services as measured against industry security standards as determined by AWS and its policies and procedures. AWS will conduct periodic audits of the physical and logical access controls for the AWS GovCloud (US) region to verify the adequacy of its information security program for the region. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

3. Security Breach Notification. If AWS has actual knowledge of a confirmed breach of the security measures described in these AWS Security Standards that affects the security of any of Your Content that is subject to applicable data breach notification law, AWS will (a) promptly notify the Customer, as required by applicable law, and (b) take commercially reasonable measures to address the breach in a timely manner. The term "breach of security" means the unauthorized access to or acquisition of any record containing Your Content in a manner that renders misuse of the information reasonably possible.

Attachment C
Master Definition List

"Acceptable Use Policy" means the policy currently available at http://aws.amazon.com/aup, as it may be updated by us from time to time.

"API" means an application program interface.

"AWS Confidential Information" means all nonpublic information disclosed by us, our affiliates, business partners or our or their respective employees, contractors or agents that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential. AWS Confidential Information includes: (a) nonpublic information relating to our or our affiliates or business partners' technology, customers, business plans, promotional and marketing activities, finances and other business affairs; (b) third-party information that we are obligated to keep confidential; and (c) the nature, content and existence of any discussions or negotiations between you and us or our affiliates. AWS Confidential Information does not include any information that: (i) is or becomes publicly available without breach of this Agreement; (ii) can be shown by documentation to have been known to you at the time of your receipt from us; (iii) is received from a third party who did not acquire or disclose the same by a wrongful or tortious act; or (iv) can be shown by documentation to have been independently developed by you without reference to the AWS Confidential Information.

"AWS Marks" means any trademarks, service marks, service or trade names, logos, and other designations of AWS and its affiliates that we may make available to you in connection with this Agreement.

"AWS Content" means Content we or any of its affiliates make available in connection with the Services or on the AWS Site to allow access to and use of the Services, including WSDLs; Documentation; sample code; software libraries; command line tools; and other related technology. AWS Content does not include the Services.

"AWS Premium Support Guidelines" means the guidelines currently available at http://aws.amazon.com/premiumsupport/guidelines, as they may be updated by us from time to time.

"AWS Site" means http://aws.amazon.com and any successor or related site designated by us.

"Content" means software (including machine images), data, text, audio, video, images or other content.

"Documentation" means the developer guides, getting started guides, user guides, quick reference guides, and other technical and operations manuals and specifications for the Services located at http://aws.amazon.com/documentation, as such documentation may be updated by us from time to time.

"End User" means any individual or entity that directly or indirectly through another user: (a) accesses or uses Your Content; or (b) otherwise accesses or uses the Service Offerings under your account. The term "End User" does not include individuals or entities when they are accessing or using the Services or any Content under their own AWS account, rather than your account.

"Notice and Procedure for Making Claims of Copyright Infringement" means the procedures currently located at http://aws.amazon.com/terms#notice-and-procedure-for-making-claims-of-copyright-infringement, as they may be updated by us from time to time.

"Policies" means the Acceptable Use Policy, the Site Terms, the Service Terms, the Trademark Use Guidelines, all restrictions described in the AWS Content and on the AWS Site, and any other policy or terms referenced in or incorporated into this Agreement. Policies does not include whitepapers or other marketing materials referenced on the AWS Site.

"Privacy Policy" means the privacy policy currently referenced at http://aws.amazon.com/privacy, as it may be updated by us from time to time.
"Service" means each of the web services made available by us or our affiliates, including those web services described in the Service Terms.
"Service Level Agreement" means all service level agreements that we offer with respect to the Services and post on the AWS Site, as they may be updated by us from time to time. The service level agreements we currently offer with respect to the Services are located at http://aws.amazon.com/ec2-sla/, http://aws.amazon.com/s3-sla/, and http://aws.amazon.com/cloudfront/sla.
"Service Offerings" means the Services (including associated APIs), the AWS Content, the AWS Marks, the AWS Site, and any other product or service provided by us under this Agreement. Service Offerings do not include Third Party Content.
"Service Terms" means the rights and restrictions for particular Services located at http://aws.amazon.com/serviceterms, as they may be updated by us from time to time.
"Site Terms" means the terms of use located at http://aws.amazon.com/terms/, as they may be updated by us from time to time.
"Suggestions" means all suggested improvements to the Service Offerings that you provide to us.
"Trademark Use Guidelines" means the guidelines and license located at http://aws.amazon.com/trademarkguidelines/, as they may be updated by us from time to time.
"Term" means the term of this Agreement described in Section 7.1.
"Third Party Content" means Content made available to you by any third party on the AWS Site or in conjunction with the Services.
"Your Content" means Content you or any End User (a) run on the Services, (b) cause to interface with the Services, or (c) upload to the Services under your account or otherwise transfer, process, use or store in connection with your account.
"Your Submissions" means Content that you post or otherwise submit to developer forums, sample code repositories, public data repositories, or similar community-focused areas of the AWS Site or the Services.

SECTION B – SUPPLIES/SERVICES AND PRICES/COSTS

B.1-TYPE OF CONTRACT

This contract is a hybrid firm-fixed price (FFP)/labor-hour (LH)/time and material (T&M) contract with FFP, LH, T&M and Cost Reimbursement (CR) CLINs; CR type CLINs will only be used for Other Direct Costs (ODCs) and Travel.

B.2-CLIN STRUCTURE

The Contractor~~Offeror~~ 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 the work specified in Attachment 1-Performance Work Statement (PWS) for the ICE Investigative Case Management requirement.

B.3-TRAVEL

Travel is not expected under this contract. Any required travel will be reimbursed in accordance with the Federal Travel Regulations. Travel Not-to-Exceed (NTE) Amounts have been provided in Section A-Schedule and are set as follows:

CLIN 0004:
CLIN 1004:
CLIN 2004:
CLIN 3004:
CLIN 4004:
CLIN 5004:
(b)(4)

Profit shall not be applied to travel costs. Contractors may apply indirect costs to travel in accordance with the Contractor's usual accounting practices consistent with FAR 31.2.

Travel CLINs will be invoiced monthly. Travel requires pre-approval from the COR.

B.4-NAICS AND PSC

NAICS Code: 541512 Computer System Design Services, Size Standard: (b)(4)
PSC Code: D307 Automated Information Systems Design and Integration Services

Page 3261

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3262

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3263

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3264

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3265

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Plan for Extraction of ICE Data in the ICM System Attachment 1-PWS, Deliverable 3.9.2	Major System Technical Data Deliverable
Final Updated ICM System Documentation Attachment 1-PWS, Deliverable 3.9.3	Major System Technical Data Deliverable

F.5-DELIVERY INSTRUCTIONS

All deliverables shall be submitted in electronic format no later than 4:00 PM on the deliverable's due date. All electronic versions of the deliverables shall be submitted in MS Office 2010 or compatible.

Electronic deliverables shall be submitted to the COR at the following e-mail address:
(b)(6),(b)(7)(C)

Items must be approved by the Program Manager (PM) and/or the appropriate Government authority to be considered "acceptable." The Government will provide written acceptance, comments, or change requests within ten (10) business days from receipt by the Government of all required Contract deliverables, with the exception of Software Versions and Releases.

Upon receipt of the Government comments, the Contractor shall schedule a collaborative session with the Government within five (5) business days to review any comments or change requests. After the collaborative session, the Contractor shall have ten (10) business days to incorporate the comments or changes, and resubmit the deliverable to the Government.

F.6-NOTICE REGARDING LATE DELIVERY

The Contractor shall notify the COR as soon as it becomes apparent to the Contractor that a scheduled deliverable will be late. The Contractor shall include in the notification the rationale for late delivery of the deliverable, the expected date for the deliverable, any consideration provided by the Contractor, and the impact of the late delivery of the deliverable on the project. The COR, Program Manager, and Contracting Officer will review the new schedule and the Contracting Officer will provide guidance to the Contractor.

SECTION G-CONTRACT ADMINISTRATION DATA

G.1-TECHNICAL DIRECTION AND SURVEILLANCE

a) Performance of the work under this contract shall be subject to the surveillance and written technical direction of the COR, who shall be specifically appointed by the Contracting Officer in writing. Technical direction is defined as a directive to the Contractor which approves approaches, solutions, designs, or refinements; fills in details or otherwise completes the general description of work of documentation items; shifts emphasis among work areas or tasks; or otherwise furnishes guidance to the Contractor. Technical direction includes the process of conducting inquiries, requesting studies, or transmitting information or advice by the COR, regarding matters within the general tasks and requirements in Section C of this CONTRACT.

b) The COR does not have the authority to, and shall not, issue any technical direction which:

1. Constitutes an assignment of additional work outside the PWS;
2. Constitutes a change as defined in the contract clause entitled "Changes";
3. In any manner causes an increase or decrease in the total price or the time required for contract performance;
4. Changes any of the expressed terms, conditions, or specifications of the contract; or
5. Interferes with the Contractor's right to perform the specifications of the contract.

c) All technical directions shall be issued in writing by the COR via e-mail. The Contractor shall proceed promptly with the performance of technical directions duly issued by the COR. Any instruction or direction by the COR which falls within one or more of the categories defined in (b)(1) through (5) above, shall follow the procedures in FAR 52.243-7.

G.2-CONTRACTING OFFICER'S REPRESENTATIVE

The COR for this contract is: (b)(6);(b)(7)(C)

Alternate COR for this contract is (b)(6);(b)(7)(C)

G.3-INVOICING AND PAYMENT PROCEDURES

Invoicing Instructions

Service Providers/Contractors shall use these procedures when submitting an invoice.

1. Invoice Submission: Invoices shall be submitted in a .pdf format in accordance with the contract terms and conditions via email to:

Invoice.Consolidation@ice.dhs.gov

Page 3268

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

3. Payment Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at 1-877-491-6521 or by e-mail at OCFO.CustomerService@ice.dhs.gov

CLIN 1001-Firm-Fixed Price (FFP) shall be invoiced for based on the percentage of each Sub-Contract Line Item Number (SLIN). Once the deliverable for each SLIN is accepted by the Government, the Contractor shall submit an invoice for the percentage of FFP listed in the SLIN. The FFP percentage allocated to each SLIN is as follows:

SLIN No.	Deliverable/Phase	Amount
SLIN 1001A	Completion of Transition-In	(b)(4)
SLIN 1001B	Phase 1: Requirements Confirmation and Baseline Installation	
SLIN 1001C	Phase 2: Baseline Gap Analysis	
SLIN 1001D	Phase 3: Code Freeze for IOC	
SLIN 1001E	Phase 4: IOC Integration and Testing	

Labor Hour CLINs:
Materials on T&M Orders must comply with FAR 52.232-7 Payments Under Time-and-Materials and Labor Hour Contracts (Aug 2012).

Cost Reimbursable CLIN (Other Direct Costs) CLINs:
The contractor may invoice monthly on the basis of cost incurred for the Other Direct Cost (ODC) CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and name. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable in spreadsheet form:

Item purchased
Cost
Date expensed
Documentation of prior COR approval

All cost presentations provided by the Contractor shall also include applicable indirect cost.

Page 3270

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3271

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3272

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3273

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3274

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3275

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3276

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3277

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3278

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3279

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3260

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3281

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3262

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3283

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3284

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3255

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3286

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3267

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3288

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3269

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3290

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3291

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3292

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3293

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3294

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3295

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3296

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3297

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3298

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3299

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3300

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3301

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3302

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3303

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3304

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3305

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3306

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3307

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3308

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3309

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3310

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3311

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3312

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3313

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3314

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3315

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3316

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3317

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3318

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3319

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3320

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3321

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3322

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3323

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3324

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3325

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3326

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3327

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3328

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

unlimited rights to all software modifications as defined above and shall have the same rights in the GOTS solution as the Government previously acquired when the GOTS software was developed.

ICE shall retain ownership of any training plans and manuals, all data input in the system, and all outputs of the system including all investigative reports created by a User of the system. Outputs of the system include both the data and formatting of the outputs. The Offeror shall not attach any unauthorized or restricted markings on this material. This material shall be delivered IAW FAR 52.227-17.

Implementation and Management

The overall ICE TECS Modernization program will follow structured DHS-approved lifecycle implementation processes as outlined in the ICE System Lifecycle Management (SLM) Handbook and will refer to the ICE Technical Reference Model (TRM) for commercial products already approved by ICE. The ICE TRM is provided as Exhibit I to the RFP. The Contractor shall conduct an implementation strategy, in collaboration with the Government that aligns with the ICE SLM Handbook and industry best practices for managing programs and projects. During ICM system implementation and management, the Contractor shall collaborate closely with the Government and other developers on the ICE TECS Modernization program. In particular, the Contractor shall provide the Government with complete visibility and transparency into all phases of their implementation and management work on the ICE TECS Modernization program, including working co-located with the Government, conducting daily collaboration with Government counterparts, both technical and functional, sharing of status on a real-time basis via joint Contractor/Government teams. Such collaboration will enable the Government to determine acceptance (or not) of the technology and functionality being development efficiently and effectively.

Development, Test, and Deployment Approach

(b)(5)(b)(7)(E) The hosting environments are described in the table under **Hosting Environments** to support development, test, and deployment activities for all ICE TECS Modernization system components, including the ICM system.

The Contractor shall use these hosting environments for development, configuration, integration, and testing of their solution. The Contractor shall participate in all levels of integration and testing as the overall ICE TECS Modernization system progresses to IOC. Specifically, the Contractor shall assist in analyzing problems discovered during all levels of integration and testing. The Contractor shall correct errors and shortfalls (example of shortfall is not meeting performance requirements) in the ICM system during all levels of integration and testing.

Software code changes applied to the Contractor's system to support the ICM system requirements shall be developed to be compatible with, and shall not prevent the ability to apply, future software maintenance upgrades to the Contractor's product that are made generally available. In general, the Government would prefer that functional extensions or enhancements and error corrections developed for the ICM system during all development, test, and maintenance activities be incorporated into the code base for the ICM system so that future

Palantir

(b)(4);(b)(5);(b)(7)(E)

Deliverables for this Task are:

Deliverable #	Deliverable Title	Deliverable Due Date
(b)(4);(b)(5);(b)(7)(E)		

(b)(5),(b)(7)(E)

Environment	Purpose	ICM Hosting Location
(b)(5),(b)(7)(E)		

Exhibit 25: (b)(5),(b)(7)(E)

Key Performance Parameters and Maintainability

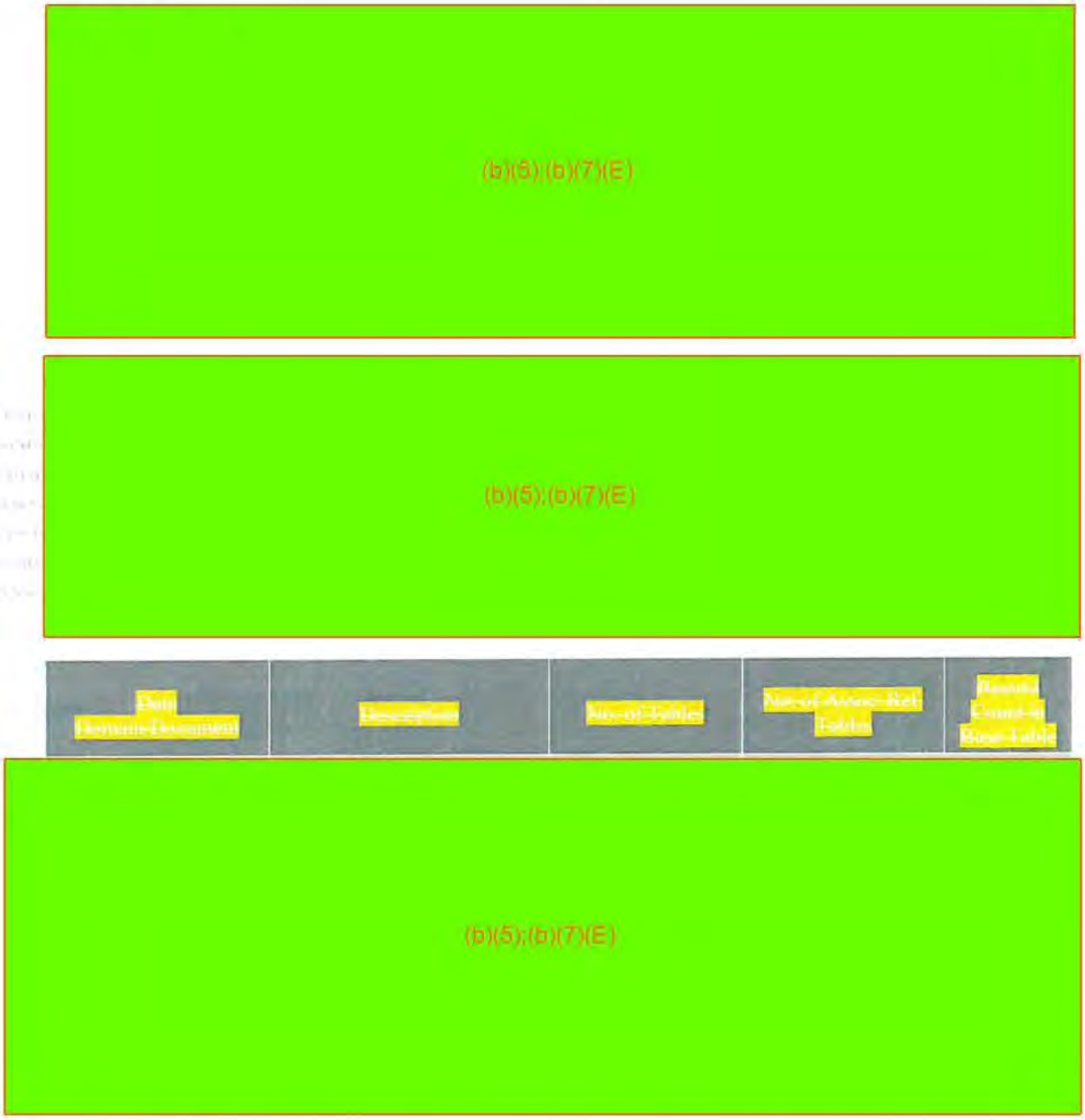
Key performance parameters (KPPs) are specified for the ICE TECS Modernization system in the ICE TECS Modernization System Operational Requirements Document (ORD), which was provided as Exhibit E to the RFP. These KPPs are shown in the table below. As the overall ICE TECS Modernization system includes several components, the ICM Contractor shall meet the performance requirements relevant to their solution and its key role in the overall ICE TECS Modernization system.

In addition to the KPPs found in Table 3, there are other performance requirements (e.g., related to maintainability) in the detailed requirements in **Exhibit 26**. The availability KPP below shall drive the ICM system maintainability requirements in terms of mean time to restore service (average time to restore service after a failure), mean downtime (time that the ICM system is not operational due to service incident or preventive maintenance including logistic and

ReceiveEventNotification	Allows ICM to be made aware of *subscribed* law enforcement events and information related to cases and/or investigative subjects, such as seizures, arrests, border crossings, and other information.	Inbound (from the ICE Interface Hub)	ICM system

Exhibit 28: *ICE TECS Modernization System Interfaces.*

Data Migration



(b)(5);(b)(7)(E)

(b)(5);(b)(7)(E) The ICE Data Warehouse will retrieve legacy data (e.g., cases and ROIs) as well as new data created by the ICM system, and return results back in an XML file. The ICE Data Warehouse will have mechanisms to enforce access control and will only return results to which requesting users have access. The ICM system shall render the results from the ICE Data Warehouse in MS-Word, PDF, or similar formats.

Security and Privacy

The system shall be compliant with all relevant security controls outlined in the Federal Information Processing Standard (FIPS) and the Federal Information Security Management Act (FISMA) to include, but not limited to, the ability of the federal government to perform a security certification and accreditation process to obtain an authorization to operate that will be signed by the federal principal without delay to system deployment. Specific security and privacy requirements for the ICM system are specified in the detailed ICM system requirements provided as Exhibit A to the RFP.

DHS/ICE has determined that all contractors/subcontractor(s) performing work under the ICE TECS Modernization contract will have access to sensitive but unclassified (SBU) DHS and ICE information, which requires DHS Suitability Clearance (b)(5);(b)(7)(E) position of public trust adjudication.

has spawned any new risks. The Risk Register will be available on-demand in our JIRA portal, and we will regularly provide ICE stakeholders with a risk matrix illustrating any change in risk probability or severity.

We will communicate frequently and openly with ICE stakeholders and within our project team to ensure that we capture and leverage lessons learned—including those from other deployments—and that we anticipate risks, proactively take action to avoid or mitigate them, and systematically manage the risks that we cannot fully prevent.

13.0 Risk Mitigation and Avoidance Strategies

(b)(5);(b)(7)(E)

#	Risk	Mitigation Strategies	Residual Probability After Mitigation
1	(b)(5);(b)(7)(C)	(b)(5);(b)(7)(E)	(b)(5);(b)(7)(
2	(b)(5);(b)(7)(E)	(b)(5);(b)(7)(E)	(b)(5);(