

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE		PAGE OF PAGES 1 3	
2. AMENDMENT/MODIFICATION NO. P00006		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO.	
5. PROJECT NO. (If applicable)		6. ISSUED BY CODE ICE/ITD		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					
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853		(x)		9A. AMENDMENT OF SOLICITATION NO.	
				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					
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended. <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required) See Schedule					
13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.				
	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				
E. IMPORTANT: Contractor <input checked="" type="checkbox"/> is not. <input type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) DUNS Number: 967391793 The purpose of this modification (P00006) is to reduce the total price of this contract by (b)(4) as a result of changing from Labor Hour-type to Firm Fixed Price-type the following CLINs:					
1) CLIN 3006 - Decrease by (b)(4) and change to Firm Fixed-Price for new total (b)(4) 2) CLIN 4006 - Decrease by (b)(4) and change to Firm Fixed-Price for new total (b)(4) 3) CLIN 5006 - Decrease by (b)(4) and change to Firm Fixed-Price for new total (b)(4)					
Continued ...					
Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)			
		(b)(6);(b)(7)(C)			
15B. CONTRACTOR/OFFEROR		15C. DATE SIGNED		16C. DATE SIGNED	
(Signature of person authorized to sign)		(Signature of Contracting Officer)			

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00006PAGE OF
2 3NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Exempt Action: Y Discount Terms: Net 30 FOB: Destination Period of Performance: 09/26/2014 to 09/24/2019 Change Item 3006 to read as follows (amount shown is the obligated amount):				
3006	Optional System Enhancements Option Period 3 (12 months) Firm Fixed-Price: (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 Change Item 4006 to read as follows (amount shown is the obligated amount):				(b)(4)
4006	Optional System Enhancements Option Period 4 (12 months) Firm Fixed-Price: (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 5006 to read as follows (amount shown is the obligated amount):				(b)(4)
5006	Optional System Enhancements Option Period 5 (12 months) Firm Fixed-Price: (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 Points of Contact Contracting Officer - (b)(6);(b)(7)(C) Phone - 202.732.(b)(6) (temp) Email - (b)(6);(b)(7)(C) Contracting Officer's Representative (COR) - (b)(6);(b)(7)(C) Phone - (b)(6);(b)(7)(C) Continued ...				(b)(4)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00006

PAGE OF
3 3

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Email - (b)(6),(b)(7)(C)				
	Vendor POC - (b)(6),(b)(7)(C)				
	Phone - 678.523. (b)(6),(b)(7)(C)				
	Email - (b)(6),(b)(7)(C)				

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE		PAGE OF PAGES 1 112	
2. AMENDMENT/MODIFICATION NO. P00011		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO.	
5. PROJECT NO. (If applicable)		6. ISSUED BY ICE/Information Technology Division Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW, (b)(6)(b)(7)(C) Washington DC 20536		7. ADMINISTERED BY (If other than Item 6) CODE	
8. NAME AND ADDRESS OF CONTRACTOR (No. street, county, State and ZIP Code) PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853		(x) 9A. AMENDMENT OF SOLICITATION NO.		9B. DATED (SEE ITEM 11)	
CODE 9673917930000		FACILITY CODE		10A. MODIFICATION OF CONTRACT/ORDER NO. HSCETC-14-C-00002	
				10B. DATED (SEE ITEM 13) 09/25/2014	

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

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

12. ACCOUNTING AND APPROPRIATION DATA (If required)

See Schedule

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

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

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

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

DUNS Number: 967391793

The purpose of this modification is to incorporate the following changes:

1) Replace (b)(6)(b)(7)(C) with (b)(6)(b)(7)(C) in the key personnel position of Principal Systems Engineer.

Exempt Action: Y Sensitive Award: LAW ENFORCEMENT

Period of Performance: 09/26/2014 to 09/24/2019

Continued ...

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) (b)(6)(b)(7)(C)	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16C. DATE SIGNED 2/14/16	

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>The total obligated value of this contract does not change, remaining (b)(4)</p> <p>The total contract value of this contract does not change, remaining (b)(4)</p> <p>Points of Contact</p> <p>Contracting Officer - (b)(6),(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)(b)(7)(C)</p> <p>Email - (b)(6),(b)(7)(C)</p> <p>Contracting Officer's Representative (COR) - (b)(6),(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6),(b)(7)(C)</p> <p>Alternate Contracting Officer's Representative (ACOR) - (b)(6),(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6),(b)(7)(C)</p> <p>Vendor POC - (b)(6),(b)(7)(C)</p> <p>Phone - 703-270-(b)(6)</p> <p>Email - (b)(6),(b)(7)(C)</p> <p>The total value of this contract value decreases from (b)(4) to (b)(4)</p>				

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE		PAGE OF PAGES 1 2	
2. AMENDMENT/MODIFICATION NO. P00012		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO.	
5. PROJECT NO. (If applicable)		6. ISSUED BY CODE ICE/ITD		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					
8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853		(x)		9A. AMENDMENT OF SOLICITATION NO.	
				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					
<input type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers <input type="checkbox"/> is extended. <input type="checkbox"/> is not extended. Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods: (a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGEMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required) See Schedule					
13. THIS ITEM ONLY APPLIES TO MODIFICATION OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
CHECK ONE					
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.					
X B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).					
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF					
D. OTHER (Specify type of modification and authority)					
E. IMPORTANT: Contractor <input checked="" type="checkbox"/> is not, <input type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) DUNS Number: 967391793 The purpose of this modification is to incorporate the following changes: 1) Replace (b)(6);(b)(7)(C) as the Alternative Contracting Officer's Representative (ACOR) for this contract. Exempt Action: Y Sensitive Award: LAW ENFORCEMENT Period of Performance: 09/26/2014 to 09/24/2019 The total obligated value of this contract does not change, remaining (b)(4) The total contract value of this contract does not change, remaining \$ Continued ... Except as provided herein, all terms and conditions of the document referenced in Item 9 A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or print)		15B. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)			
		(b)(6);(b)(7)(C)			
15B. CONTRACTOR/OFFEROR		15C. DATE SIGNED		15C. DATE SIGNED 3/7/17	
(Signature of person authorized to sign)		(Signature of person authorized to sign)			
NSN 7540-01-152-8070 Previous edition unusable		STANDARD FORM 30 (REV. 10-83) Prescribed by GSA FAR (48 CFR) 53.243			

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00012PAGE OF
2 2NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Points of Contact</p> <p>Contracting Officer - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Contracting Officer's Representative (COR) - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Alternate Contracting Officer's Representative (ACOR) - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Vendor POC - (b)(6);(b)(7)(C)</p> <p>Phone - 703-270-(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p>				

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT		1. CONTRACT ID CODE		PAGE OF PAGES 1 73	
2. AMENDMENT/MODIFICATION NO. P00010		3. EFFECTIVE DATE See Block 16C		4. REQUISITION/PURCHASE REQ. NO. 192117CIOSDD10012	
5. PROJECT NO. (If applicable)		6. ISSUED BY ICE/Information Technology Division Immigration and Customs Enforcement Office of Acquisition Management 801 I Street NW, (b)(6);(b)(7)(C) Washington DC 20536		7. ADMINISTERED BY (If other than Item 6) CODE	
8. NAME AND ADDRESS OF CONTRACTOR (No, street, county, State and ZIP Code) PALANTIR USG 1660 INTERNATIONAL DR STE 800 MCLEAN VA 221024853		(X)		9A. AMENDMENT OF SOLICITATION NO.	
				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 Decrease: -\$423,242.12

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
	D. OTHER (Specify type of modification and authority)
X	By Mutual Agreement of Both Parties

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: 967391793

The purpose of this modification (P00010) is to incorporate the following changes:

- 1) Update the Sections B-J of the Contract.
 - 2) Update the Performance Work Statement (Attachment 1);
 - 3) Update the license agreement for AWS Cloud hosting services (part of Attachment 3 - Software License Agreement and Related Material) removing DLT as a subcontractor;
 - 4) Add Attachment 8 - Palantir AWS Cloud Pricing Sheet.
- Note: all prices for services performed for CLINs 3007, 3009, 3010, 4007, 4009, 4010, 5007, 5009, and 5010 shall be based on the prices established in Attachment 8 - Palantir AWS Cloud Pricing Sheet

Continued ...

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

15A. NAME AND TITLE OF SIGNER (Type or print) (b)(6);(b)(7)(C)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) (b)(6);(b)(7)(C)	
15B.	15C. DATE SIGNED 2017.01.12	A	16C. DATE SIGNED 1/12/17

NSN 7540-01-152-8070
Previous edition unusable

STANDARD FORM 30 (REV. 10-83)
Prescribed by GSA
FAR (48 CFR) 53.243

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00010PAGE OF
2 73NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Cloud Pricing Sheet</p> <p>As a result of this modification the following CLINs and CLIN amounts are revised as follows:</p> <p>CLIN 3007: Deobligate (b)(4) decreasing the CLIN total to (b)(4)</p> <p>CLIN 3009: Transfer (b)(4) to CLIN 3010 and deobligate the remaining (b)(4) decreasing the CLIN total to (b)(4)</p> <p>CLIN 3010: Obligate (b)(4) from CLIN 3009, increasing the CLIN total to (b)(4)</p> <p>CLIN 4007: Total value of this CLIN is reduced to (b)(4)</p> <p>CLIN 4009: Total value of this CLIN is reduced to (b)(4)</p> <p>CLIN 4010: Total value of this CLIN is increased to (b)(4)</p> <p>CLIN 5007: Total value of this CLIN is reduced to (b)(4)</p> <p>CLIN 5009: Total value of this CLIN is reduced to (b)(4)</p> <p>CLIN 5010: Total value of this CLIN is increased to (b)(4)</p> <p>Exempt Action: Y</p> <p>Discount Terms:</p> <p>Net 30</p> <p>Delivery Location Code: ICE/CIO</p> <p>ICE Chief Information Officer</p> <p>Immigration and Customs Enforcement</p> <p>801 I Street, NW</p> <p>(b)(6) (b)(7)(C)</p> <p>Washington DC 20536</p> <p>(b)(4),(b)(7)(E)</p> <p>FOB: Destination</p> <p>Period of Performance: 09/26/2014 to 09/24/2019</p> <p>Change Item 3007 to read as follows (amount shown is the obligated amount):</p> <p>3007 Combined GovCloud Instances (252 Servers)</p> <p>Not-to-Exceed Amount: (b)(4)</p> <p>Product/Service Code: D307</p> <p>Continued ...</p>				(b)(4)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00010PAGE OF
3 73NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

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				
	Change Item 3009 to read as follows (amount shown is the obligated amount):				
3009	AWS Standard Support Package Not-to-Exceed Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Change Item 3010 to read as follows (amount shown is the obligated amount):				
3010	Software as a Service (SaaS)-Palantir Cloud Not-to-Exceed Amount: (b)(4) Product/Service Code: D307 Product/Service Description: IT AND TELECOM- IT STRATEGY AND ARCHITECTURE				(b)(4)
	Change Item 4007 to read as follows (amount shown is the obligated amount):				
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				(b)(4)
	Change Item 4009 to read as follows (amount shown is the obligated amount):				
4009	AWS Standard Support Package Not-to-Exceed Amount: \$0 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)
	Change Item 4010 to read as follows (amount shown is the obligated amount):				
4010	Software as a Service (SaaS)-Palantir Cloud Continued ...				(b)(4)

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00010PAGE OF
4 73NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	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 5007 to read as follows (amount shown is the obligated amount):				
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 Change Item 5009 to read as follows (amount shown is the obligated amount):				(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 Change Item 5010 to read as follows (amount shown is the obligated amount):				(b)(4)
5010	Software as a Service (SaaS)-Palantir Cloud 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 The total obligated value of this contract decreases from (b)(4) to (b)(4) The total contract value of this contract decreases from (b)(4) to (b)(4) Points of Contact Continued ...				0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
HSCETC-14-C-00002/P00010

PAGE OF
5 73

NAME OF OFFEROR OR CONTRACTOR
PALANTIR USG

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	<p>Contracting Officer - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Contracting Officer's Representative (COR) - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Alternate Contracting Officer's Representative (ACOR) - (b)(6);(b)(7)(C)</p> <p>Phone - 202.732.(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>Vendor POC - (b)(6);(b)(7)(C)</p> <p>Phone - 703-270-(b)(6)</p> <p>Email - (b)(6);(b)(7)(C)</p> <p>The total value of this contract value decreases from (b)(4) to (b)(4)</p>				

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 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 1 will 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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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:
Andrew.Fox@ice.dhs.gov

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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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.

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

3. Payment Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at 1-877-491-6521 or by e-mail at (b)(6),(b)(7)(C)

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

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
<p>PWS Constraint Documents including the following:</p> <ul style="list-style-type: none">• 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	<p>Provided with Request for Proposals (RFP)</p> <p>Updated versions of GFI, as versions are approved during the contract period of performance.</p>	<p>Returned or purged by Contractor once Contractor employee leaves the contract (via termination or reassignment) or the contract completion.</p>
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 UNCLASSIFIED (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.

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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.6.3-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 surplus, 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.
- DHS employees and Contractors shall follow DHS 4300 guidelines in Section 5.4.6 Email Security specifically the policy stated in 5.4.6.i which states "*Auto-forwarding or redirecting of DHS email to any address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risks or consequences are minimal.*"
- **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. Please see Section 9 of the Performance Work Statement for list of references.

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).

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. Please see Section 9 of the Performance Work Statement for list of references.

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 and non-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 (to include subcontractor 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 7 - DHS 4300A Sensitive Systems Handbook, Rules of Behavior that is provided as reference) 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)

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

- (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 and the Rules of Behavior that the Contractor develops 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-PRIV 1.4: Separation Checklist for Contractor Employees

Contractors shall enact a protocol to use a separation checklist before its employees, sub-Contractor employees, or independent Contractors terminate working on the contract. The separation check list must cover areas such as: (1) return of any government-furnished equipment; (2) return or proper disposal of Sensitive PII (paper or electronic) in the custody of the Contractor/sub-Contractor employee or independent Contractor, including the wiping of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access Sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee, sub-Contractor employee, or independent Contractor, the Contractor shall notify the COR within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of the employment or work on the contract.

(End of clause)

H.9-PRIV 1.6: Prohibition on Performing Work Outside A Government

Facility/Network/Equipment: As mutually agreed between the Parties, the Contractor shall perform all tasks described in this document at Contractor's facilities or at authorized government facilities. Except as otherwise authorized by the Government to perform the tasks described in this document, Government information shall remain within the confines of authorized government facilities and/or networks at all times.

H.10- PRIV 1.7: Privacy Act Information

In accordance with FAR 52.224-1, PRIVACY ACT NOTIFICATION (APR 1984), and FAR 52.224-2, PRIVACY ACT (APR 1984), this contract requires Contractor personnel to have access to information protected by the Privacy Act of 1974. The agency advises that the relevant system of records notices (SORNs) applicable to this Privacy Act information are as follows:

DHS / ICE 009 – External Investigations System of Records
DHS/ALL-020 - Internal Affairs System of Records

These SORNs may be updated at any time and the most current versions are publicly available at www.dhs.gov/privacy.

H.11- PRIV 2.1: Restriction on Testing Using Real Data Containing PII

Except as required to fulfill contract requirements, the use of real data containing Sensitive PII, from any source, for testing purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system testing be approved by the ICE Privacy Officer and Chief Information Security Officer in advance. In the event performance of the contract requires or necessitates the use of real data for system testing purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation.

(End of clause)

H.12- PRIV 2.2: Restriction on Training Using Real Data Containing PII

Except as required to fulfill contract requirements, the use of real data containing Sensitive PII, from any source, for training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for training whenever feasible. ICE policy requires that any proposal to use real data or de-identified data for IT system training be approved by the ICE Privacy Officer and Chief Information Security Officer in advance. In the event performance of the contract requires or necessitates the use of real data for training purposes, the Contractor in coordination with the CO or COR and government program manager shall obtain approval from OCIO and the ICE Privacy Office and complete any required documentation.

(End of clause)

H.13-Records Management Language for Contracts

(Adapted from: <http://www.archives.gov/records-mgmt/handbook/records-mgmt-language.html>)

H.13.1 RECORDS 1.1: Except as stated in the Performance Work Statement, Terms and Conditions (Sections B-J), and the Contractor's Commercial License Agreement, the Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the express permission of the Contracting Officer or Contracting Officer's representative. The Government Agency owns the rights to all data/records produced as part of this contract.

(End of clause)

H.13.2 RECORDS 1.2: The Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records. The Contractor shall not create or maintain any records containing any Government Agency data that are not specifically tied to or authorized by the contract.

(End of clause)

H.13.3 RECORDS 1.3: Except as stated in the Performance Work Statement, Terms and Conditions (Sections B-J), and the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation created as part of this contract. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(End of clause)

H.13.4 RECORDS 1.4: The Contractor agrees to comply with Federal and Agency records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format, mode of transmission, or state of completion.

(End of clause)

H.13.5 RECORDS 1.5: No disposition of documents will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

(End of clause)

H.13.6 REC 1.6: No disposition of Federal Records will be allowed without the prior written consent of the Contracting Officer. The Agency and its contractors are responsible for preventing the alienation or unauthorized destruction of Federal records, including all forms of mutilation.

Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. Federal Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

(End of clause)

H.13.7 RECORDS 1.7: The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-contractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(End of clause)

H.14-ADDITIONAL KEY PERSONNEL-PRIVACY LEAD

The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Office, the Office of the Chief Information Officer, and the Records Management Branch to ensure that the privacy documentation are kept on schedule, that the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

- Candidate must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and to synthesize information together from a variety of sources.
- Candidate must have excellent verbal communication and organizational skills.
- Candidate must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Candidate must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Candidate must be able to work well with others.

H.15-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:

Section 508 Applicable EIT Accessibility Standards

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 1194.31 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 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 COR 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

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. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

H.17-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.18-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.

HSCETC-14-C-00002
 INVESTIGATIVE CASE MANAGEMENT SYSTEM
 PALANTIR

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
Palantir Gotham with Case Management (CM-PG 3.12)	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.

H.19-CLAUSES FOR CLINs XX07, XX09, and XX10

The following clause applies to CLINs XX07 and XX09.

The unit pricing for this CLIN shall be in accordance with the discount provided by Palantir's enterprise AWS account.

(End of clause)

H.20-CLAUSES FOR CLINs XX07, XX09, and XX10

The following clause applies to CLINs XX07, XX09, and XX10.

Once the Investigative Case Management System reaches post-production, the Government reserves the right to re-negotiate CLINs XX07, XX09, and XX10. Currently, these CLINs are priced on a 'Not-to-Exceed' basis. However, once post-production is achieved and usage becomes more static, firm-fixed priced CLINs may be more appropriate. Prior to exercising these CLINs, the type (NTE vs. Firm-Fixed Price) and amount of the CLINs will be re-evaluated and if necessary, revised via a bilateral modification.

(End of clause)

H.21-CLAUSES FOR CLINs XX07, XX09, and XX10

The following clause applies to CLINs XX07, XX09, and XX10.

The Contractor agrees to perform the work specified for CLINs XX07, XX09, and XX10 within the funding obligated to each CLIN. The Contractor shall notify the Contracting Officer in writing whenever it has reason to believe that the costs it expects to incur under CLINs XX07, XX09, and XX10 in the next 90 days, when added to all costs previously incurred under each of the CLINs, will exceed 75 percent of the total amount so far allotted to each of the CLINs by the Government. The notice shall state the estimated amount of additional funds required to continue performance for the remainder of the CLIN's period of performance.

The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount allotted by the Government to CLINs XX07, XX09, and XX10. The Contractor is not obligated to continue performance under these CLINs or otherwise incur costs in excess of the amount allotted to the CLINs by the Government.

(End of clause)

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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

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

1.2-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 2013-00014 (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 disadvantaged 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.

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

(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 --

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

- (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;

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

(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.

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

(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 HSAR 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 HSAR CLAUSES IN FULL TEXT

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of this clause in all subcontracts.

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

“Personally Identifiable Information (PII)” means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as 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.

“Sensitive Information Incident” is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

“Sensitive Personally Identifiable Information (SPII)” 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. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

- (1) Truncated SSN (such as last 4 digits)
- (2) Date of birth (month, day, and year)
- (3) Citizenship or immigration status
- (4) Ethnic or religious affiliation
- (5) Sexual orientation
- (6) Criminal History
- (7) Medical Information
- (8) System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>, or available upon request from the Contracting Officer, including but not limited to:

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments

- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year)
- (8) DHS Privacy Incident Handling Guidance
- (9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>
- (10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>
- (11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA)*, as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones.

Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, 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 Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to

take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting*, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);

- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

- (i) Inspections,
- (ii) Investigations,
- (iii) Forensic reviews, and
- (iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless

the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- (i) A brief description of the incident;
- (ii) A description of the types of PII and SPII involved;
- (iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
- (iv) Steps individuals may take to protect themselves;
- (v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
- (vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements.* In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

- (i) Triple credit bureau monitoring;
- (ii) Daily customer service;
- (iii) Alerts provided to the individual for changes and fraud; and
- (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

- (i) A dedicated telephone number to contact customer service within a fixed period;
- (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
- (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
- (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

- (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
- (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(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

HSCETC-14-C-00002
INVESTIGATIVE CASE MANAGEMENT SYSTEM
PALANTIR

(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)

INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

(a) *Applicability.* This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The

Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(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

Attachment 8-Palantir AWS Cloud Pricing Sheet

**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."

Page 3548

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3549

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3550

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3551

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3552

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3553

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3554

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3555

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3556

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3557

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3558

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3559.

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3560

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3561

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3562

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3563

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3564

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3565

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3566

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3567

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3566

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3569

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3570

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3571

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3572

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3573

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3574

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3575

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3576

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3577

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3578

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3579

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3580

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3581

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3552

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3583

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3584

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3585

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3586

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3587

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3585

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3589

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3590

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3591

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3592

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3593

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3594

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3595

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3596

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3597

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3598

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3599

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3600

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3601

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3602

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3603

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3604

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3605

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3606

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3607

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3608

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3609

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3610

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3611

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3612

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3613

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3614

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3615

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3616

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3617

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3618

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3619

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3620

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3621

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3622

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3623

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3624

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3625

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3626

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3627

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3626

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3629

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3630

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3631

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3632

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3633

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3634

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3635

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3636

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3637

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3636

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3639

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3640

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3641

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3642

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3643

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3644

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3645

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3646

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 3647

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3646

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3649

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3650

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3651

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3652

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3653

Withheld pursuant to exemption

(b)(7)

of the Freedom of Information and Privacy Act.

Page 3654

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3655

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act.

Page 3656

Withheld pursuant to exemption

(b)(7)

of the Freedom of Information and Privacy Act.