

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS <i>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30</i>				1. REQUISITION NUMBER 192118VHQUCOP0005		PAGE OF 1 31			
2. CONTRACT NO.		3. AWARD/EFFECTIVE DATE		4. ORDER NUMBER 70CMSD18P00000145		5. SOLICITATION NUMBER		6. SOLICITATION ISSUE DATE	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME (b)(6); (b)(7)(C)		b. TELEPHONE NUMBER (No collect calls) 214-905-(b)(6); (b)(7)(C)		8. OFFER DUE DATE/LOCAL TIME			
9. ISSUED BY Investigations Ops Support Dallas Immigration and Customs Enforcement Office of Acquisition Management 7701 N. Stemmons Freeway, Suite 300 Dallas TX 75247				10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A) NAICS: 518210 SIZE STANDARD: \$32.5					
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS (b)(4)		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700) <input type="checkbox"/>		13b. RATING			
15. DELIVER TO ICE Hmlnd Sec Inv HQ Div. 4 Immigration and Customs Enforcement 11320 Random Hills Road Suite (b)(6); (b)(7)(C) Fairfax VA 22030				16. ADMINISTERED BY Investigations Ops Support Dallas Immigration and Customs Enforcement Office of Acquisition Management 7701 N. Stemmons Freeway, Suite (b)(6); (b)(7)(C) Attn: (b)(6); (b)(7)(C) Dallas TX 75247				14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP	
17a. CONTRACTOR/OFFEROR THOMSON REUTERS SPECIAL SERVICES LLC 1410 SPRING HILL ROAD SUITE 140 MCLEAN VA 221023058		17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER <input type="checkbox"/>		18a. PAYMENT WILL BE MADE BY DHS, ICE Burlington Finance Center P.O. Box 1620 Attn: ICE-HSI-HQ-DIV 4 Williston VT 05495-1620		18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM			
19. ITEM NO.		20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT		
		DUNS Number: 827821757 Obligation POC: (b)(6); (b)(7)(C) 703-877-(b)(6); (b)(7)(C) @ice.dhs.gov Alternate Obligation POC (b)(6); (b)(7)(C) 703-877-(b)(6); (b)(7)(C) @ice.dhs.gov Technical POC (b)(6); (b)(7)(C) (b)(6); (b)(7)(C) is authorized to communicate with Thomson Reuters Special Services LLC concerning this purchase order. However, Thomson Reuters (Use Reverse and/or Attach Additional Sheets as Necessary)							
25. ACCOUNTING AND APPROPRIATION DATA See schedule						26. TOTAL AWARD AMOUNT (For Govt. Use Only) \$753,898.20			
27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA				27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4, FAR 52.212-5 IS ATTACHED. ADDENDA					
<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.				<input checked="" type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED.					
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.				29. AWARD OF CONTRACT: <u>Quote</u> OFFER DATED <u>09/12/2018</u> YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:					
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) (b)(6); (b)(7)(C)					
30b. NAME AND TITLE OF SIGNER (Type or print)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (Type or print) (b)(6); (b)(7)(C)		31c. DATE SIGNED September 20, 2018			

Page 073

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 074

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 075

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 076

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 077

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 078

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 079

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 080

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 081

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 082

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 083

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 084

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 085

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 086

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 087

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 088

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 089

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 090

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 091

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 092

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 093

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 094

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 095

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 096

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 097

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 098

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 099

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 100

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 101

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 102

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 103

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 104

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 105

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 106

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 107

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

1. REQUISITION NUMBER: 192117OAS00000031
 PAGE OF: 1 27
 2. CONTRACT NO.
 3. AWARD EFFECTIVE DATE: HSCSMD-17-P-00082
 4. ORDER NUMBER
 5. SOLICITATION NUMBER
 6. SOLICITATION ISSUE DATE

7. FOR SOLICITATION INFORMATION CALL: (b)(6); (b)(7)(C)
 b. TELEPHONE NUMBER: 214-905-(b)(6);
 c. OFFER DUE DATE/LOCAL TIME

8. ISSUED BY: ICE/IOSD
 Investigations Ops Support Dallas
 Immigration and Customs Enforcement
 Office of Acquisition Management
 7701 N. Stemmons Freeway, Suite (b)(6);
 Dallas TX 75247
 9. THIS ACQUISITION IS: UNRESTRICTED CP SET ASIDE
 SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS
 HUBZONE SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAME: 518210
 SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS EDWOSB 8(a) SIZE STANDARD: \$32.5

11. DELIVERY FOR FOR DESTINATION (UNLESS BLOCK IS MARKED) SEE SCHEDULE
 12. DISCOUNT TERMS: Net 30
 13. THIS CONTRACT IS A RATED ORDER UNDER DFARS (15.609)
 13b. RATING
 14. METHOD OF SOLICITATION: CFPQ IFB RFP

15. DELIVER TO: ICE/AS
 ICE Assistant Secretary
 Immigration and Customs Enforcement
 500 13th Street SW
 Washington DC 20536
 16. ADMINISTERED BY: ICE/IOSD
 Investigations Ops Support Dallas
 Immigration and Customs Enforcement
 Office of Acquisition Management
 7701 N. Stemmons Freeway, Suite (b)(6);
 Attn: (b)(6); (b)(7)(C)
 Dallas TX 75247

17a. CONTRACT/ORDER OFFEROR CODE: 8278217570000 FACILITY CODE:
 17b. PAYMENT WILL BE MADE BY: ICE-AS

THOMSON REUTERS SPECIAL SERVICES LLC
 ATTN: (b)(6); (b)(7)(C)
 1410 SPRING HILL ROAD
 MCLEAN VA 221023058
 DHS, ICE
 Burlington Finance Center
 P.O. Box 1620
 Attn: ICE-AS
 Ref: HSCSMD-17-P-00082
 Williston VT 05495-1620

TELEPHONE NO.: 5712058004
 17c. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER
 16. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 16a UNLESS BLOCK BELOW IS CHECKED SEE ADDENDUM

18. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DONS Number: 827821757 Obligation POC: (b)(6); (b)(7)(C) 202-732-(b)(6); (b)(7)(C) @ice.dhs.gov Alternate Obligation POC: (b)(6); (b)(7)(C) 202-732-(b)(6); (b)(7)(C) @ice.dhs.gov Technical POC: Unit Chief (b)(6); (b)(6); (b)(7)(C) 202-732 (b)(6); Exempt Action: Y Sensitive Award: LAW ENFORCEMENT Continued ... (Use Reverse and/or Attach Additional Sheets as Necessary)				

25. ACCOUNTING AND APPROPRIATION DATA: See schedule
 26. TOTAL AWARD AMOUNT (For Good Use Only): \$42,000.00

27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-2, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ARE ARE NOT ATTACHED
 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-6 IS ATTACHED. ADDENDA ARE ARE NOT ATTACHED

28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.
 29. AWARD OF CONTRACT QUOTE OFFER
 DATED 08/18/2017 YOUR OFFER ON SOLICITATION (BLOCK 9), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS

30. SIGNATURE OF CONTRACTOR: (b)(6); (b)(7)(C)
 31. DATE SIGNED: 8/18/17
 32. SIGNATURE OF CONTRACTOR: (b)(6); (b)(7)(C)
 33. DATE SIGNED: 18 Aug 2017

Page 109

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 110

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 111

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 112

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 113

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 114

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 115

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 116

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 118

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 119

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 120

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 121

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 122

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 123

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 124

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 125

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 126

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 127

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 128

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 129

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 130

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act



U.S. Immigration
and Customs
Enforcement

Terms and Conditions

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 prior to expiration of the contract term; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 15 days before the contract expires. The preliminary notice does not commit the Government to an extension.
- (b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
- (c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 5 years.

(End of Clause)

FAR 52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)

(a) Except as stated in paragraph (b) of this clause, when any supply or service acquired under this contract is subject to any End User License Agreement (EULA), Terms of Service (TOS), or similar legal instrument or agreement, that includes any clause requiring the Government to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

- (1) Any such clause is unenforceable against the Government.
- (2) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the EULA, TOS, or similar legal instrument or agreement. If the EULA, TOS, or similar legal instrument or agreement is invoked through an "I agree" click box or other comparable mechanism (e.g., "click-wrap" or "browse-wrap" agreements), execution does not bind the Government or any Government authorized end user to such clause.
- (3) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.

(b) Paragraph (a) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulation and procedures.

(End of clause)

HSAR 3052.70 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]:

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)

DHS HSAR 3052.212-70 CONTRACT TERMS AND CONDITIONS APPLICABLE TO DHS ACQUISITION OF COMMERCIAL ITEMS (SEP 2012)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference:

(a) Provisions.

___ 3052.209-72 Organizational Conflicts of Interest.

___ 3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

___ 3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

(b) Clauses.

___ 3052.203-70 Instructions for Contractor Disclosure of Violations.

___ 3052.204-70 Security Requirements for Unclassified Information Technology Resources.

___ 3052.204-71 Contractor Employee Access.

___ Alternate I

X 3052.205-70 Advertisement, Publicizing Awards, and Releases.

___ 3052.209-73 Limitation on Future Contracting.

___ 3052.215-70 Key Personnel or Facilities.

___ 3052.216-71 Determination of Award Fee.

___ 3052.216-72 Performance Evaluation Plan.

___ 3052.216-73 Distribution of Award Fee.

___ 3052.217-91 Performance. (USCG)

___ 3052.217-92 Inspection and Manner of Doing Work. (USCG)

___ 3052.217-93 Subcontracts. (USCG)

___ 3052.217-94 Lay Days. (USCG)

___ 3052.217-95 Liability and Insurance. (USCG)

___ 3052.217-96 Title. (USCG)

___ 3052.217-97 Discharge of Liens. (USCG)

___ 3052.217-98 Delays. (USCG)

___ 3052.217-99 Department of Labor Safety and Health Regulations for Ship Repair. (USCG)

___ 3052.217-100 Guarantee. (USCG)

- 3052.219-70 Small Business Subcontracting Plan Reporting.
- 3052.219-71 DHS Mentor Protégé Program.
- 3052.228-70 Insurance.
- 3052.228-90 Notification of Miller Act Payment Bond Protection. (USCG)
- 3052.228-91 Loss of or Damage to Leased Aircraft. (USCG)
- 3052.228-92 Fair Market Value of Aircraft. (USCG)
- 3052.228-93 Risk and Indemnities. (USCG)
- 3052.236-70 Special Provisions for Work at Operating Airports.
- 3052.242-72 Contracting Officer's Technical Representative.
- 3052.247-70 F.o.B. Origin Information.
- Alternate I
- Alternate II
- 3052.247-71 F.o.B. Origin Only.
- 3052.247-72 F.o.B. Destination Only.

(End of clause)

Section 508 Compliance:

29 U.S.C. Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998, 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 access to and use of information and services that is comparable to the access and use available to non-disabled federal employees and members of the public. All EIT will comply with the applicable technical and functional performance criteria of Section 508, unless exempt.

Software Maintenance Agreement

The Quoter shall notify the Government, at least, 30 days prior to the expiration of any software licensing/maintenance agreement. The Government will not be obligated to pay the Quoter any amount in excess of the firm-fixed price amount covering the effective period of performance in the order, and the Quoter shall not continue performance unless and until the Contracting Officer notifies the Quoter verbally or by written modification that a new period of performance has been established and approved.

ICE Information Governance and Privacy Requirements Clause (JUL 2017)

Guidance: In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following IGP clause must be included in its entirety in all contracts. No section of this clause may be read as self-deleting unless the terms of the contract meet the requirements for self-deletion as specified in this clause.

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) 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 Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization 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 to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and

passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self-deleting.

(1) Required Security and Privacy Training for Contractors

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. 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) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.

2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:
 - a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
 - b. Date, time, and location of the incident.
 - c. Type of information lost or compromised.
 - d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
 - e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
 - f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
 - g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
 - h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.
4. 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.
5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

- (a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) 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.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, 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 and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. 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.

D. Data Privacy and Oversight

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three 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 adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under "Key Personnel." 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 is 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. The Privacy Lead:

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

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

(End of Clause)

Invoicing Instructions

Invoice Instructions:

ICE – NON-ERO Contracts

Service Providers/Contractors shall follow these procedures when submitting invoices.

Advance payments are not authorized.

Invoices for services shall be submitted monthly or quarterly in arrears.

1. Invoice Submission: Invoices shall be submitted in a “.pdf” format in accordance with the contract terms and conditions via email, United States Postal Service (USPS) or facsimile as follows:

a. Email:

- (b)(6); (b)(7)(C)@ice.dhs.gov
- Contracting Officer Representative (COR) or Government Point of Contact (GPOC)
- Contract Specialist/Contracting Officer

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

b. USPS:

DHS, ICE
Financial Operations - Burlington
P.O. Box (b)(6);
Williston, VT 05495-1620

ATTN: ICE-OIA

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.

c. Facsimile:

Alternative Invoices shall be submitted to: (802)-288-(b)(6);
(b)(7)(C)

Submissions by facsimile shall include a cover sheet, point of contact and the number of total pages.

Submissions by facsimile shall include a cover sheet, point of contact and the number of total pages.

Note: the Service Providers or Contractors 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 task order/contract shall also be notated on every invoice.

2. Content of Invoices: Each invoice shall contain the following information in accordance with 52.212-4 (g), as applicable:

(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 unique invoice number;
- (iv) Agreement/Contract number, , if applicable, the order number;
- (v) Contract Line Item Number(s) (CLIN); Description; quantity; unit of measure; unit price and extended price of the items delivered, period of performance (each CLIN shall be identified separately on the invoice);
- (vi) If applicable, 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 an improper invoice;
- (x) ICE program office designated on order/contract/agreement and
- (xi) Mark invoice as “Interim” (Ongoing performance and additional billing expected) and “Final” (performance complete and no additional billing)
- (xii) Electronic Funds Transfer (EFT) banking information in accordance with 52.232-33 Payment by Electronic Funds Transfer – System for Award Management or 52-232-34, Payment by Electronic Funds Transfer – Other than System for Award Management.

3. Invoice Inquiries: Questions regarding invoice submission or payment, please contact ICE Financial Operations at 1-877-491-(b)(6); or by e-mail at (b)(6); (b)(7)(C)@ice.dhs.gov

52.212-4 Contract Terms and Conditions - Commercial Items. (Oct 2018)**52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (May 2019)**

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

- (1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).
- (2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).
- (3) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)
- (4) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).
- (5) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

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

[Contracting Officer check as appropriate.]

- (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).
- (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).
- (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).
- (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).
- (5) [Reserved]
- (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government' Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

_ (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

_ (10) [Reserved]

_ (11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

_ (ii) Alternate I (Nov 2011) of 52.219-3.

_ (12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

_ (ii) Alternate I (Jan 2011) of 52.219-4.

_ (13) [Reserved]

X (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

_ (ii) Alternate I (Nov 2011).

_ (iii) Alternate II (Nov 2011).

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

_ (ii) Alternate I (Oct 1995) of 52.219-7.

_ (iii) Alternate II (Mar 2004) of 52.219-7.

_ (16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

_ (17) (i) 52.219-9, Small Business Subcontracting Plan (Oct 2018) (15 U.S.C. 637 (d)(4))

_ (ii) Alternate I (Nov 2016) of 52.219-9.

_ (iii) Alternate II (Nov 2016) of 52.219-9.

_ (iv) Alternate III (Nov 2016) of 52.219-9.

_ (v) Alternate IV (Aug 2018) of 52.219-9.

- X (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).
- X (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).
- _ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).
- _ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).
- X (22) 52.219-28, Post Award Small Business Program Rerepresentation (Jul 2013) (15 U.S.C. 632(a)(2)).
- _ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).
- _ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).
- X (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).
- X (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).
- X (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- X (28) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
- X (29) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
- X (30) 52.222-36, Affirmative Action for Workers with Disabilities (July 2014) (29 U.S.C. 793).
- X (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
- X (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- X (33) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
- _ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).
- _ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

_ (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

_ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

X (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

X (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

_ (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Oct 2015) of 52.223-13.

_ (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

_ (ii) Alternate I (Jun 2014) of 52.223-14.

_ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

_ (41) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514)

_ (ii) Alternate I (Jun 2014) of 52.223-16.

X (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).

X (43) 52.223.20, Aerosols (Jun 2016) (E.O. 13693).

X (44) 52.223.21, Foams (Jun 2016) (E.O. 13696).

X (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

_ (ii) Alternate I (Jan 2017) of 52.224-3.

_ (46) 52.225-1, Buy American Act--Supplies (May 2014) (41 U.S.C. chapter 83).

X (47) (i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

- _ (ii) Alternate I (May 2014) of 52.225-3.
- _ (iii) Alternate II (May 2014) of 52.225-3.
- _ (iv) Alternate III (May 2014) of 52.225-3.
- _ (48) 52.225-5, Trade Agreements (Aug 2018) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).
- X (49) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).
- _ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2303 Note).
- _ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).
- _ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).
- _ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- _ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).
- X (55) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Oct 2018) (31 U.S.C. 3332).
- _ (56) 52.232-34, Payment by Electronic Funds Transfer— Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).
- _ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).
- X (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).
- _ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).
- _ (60) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).
- _ (ii) Alternate I (Apr 2003) of 52.247-64.

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

[Contracting Officer check as appropriate.]

- _ (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)
- _ (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67).
- _ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
- _ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).
- _ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).
- _ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).
- _ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).
- _ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015)
- _ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).
- _ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

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

- (1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.
- (2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the

records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

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

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

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(v) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

FAR 52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within *30 days* ; 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 3 years.

(End of clause)

ICE Information Governance and Privacy Requirements Clause (JUL 2017)

Guidance: In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following IGP clause must be included in its entirety in all contracts. No section of this clause may be read as self-deleting unless the terms of the contract meet the requirements for self-deletion as specified in this clause.

A. Limiting Access to Privacy Act and Other Sensitive Information*(1) Privacy Act Information*

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) 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 Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization 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 to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self-deleting.

(1) Required Security and Privacy Training for Contractors

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. 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) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.
2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-(b)(6)
(b)(7)(C)), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:
 - a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
 - b. Date, time, and location of the incident.
 - c. Type of information lost or compromised.
 - d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
 - e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
 - f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
 - g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
 - h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. 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.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) 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.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, 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 and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered

federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(c) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. 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.

D. Data Privacy and Oversight

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three 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 adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under “Key Personnel.” 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 is 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. The Privacy Lead:

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

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

(End of Clause)

Incorporated Provisions and Clauses:

FAR and HSAR provisions and clauses can be accessed at <http://farsite.hill.af.mil/>

CLAUSES AND PROVISIONS INCORPORATED BY REFERENCE:

FAR 52.203-17 -- Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights (Apr 2014)

FAR 52.212-4 -- Contract Terms and Conditions -- Commercial Items (Oct 2018)

FAR 52.217-5 -- Evaluation of Options (Jul 1990)

FAR 52.224-1 -- Privacy Act Notification (APR 1984)

FAR 52.224-2 -- Privacy Act (APR 1984)

FAR 52.232-39 -- Unenforceability of Unauthorized Obligations (Jun 2013)

HSAR 3052.205-70 -- Advertisements, Publicizing Awards, and Releases (Sep 2012)

CLAUSES INCORPORATED IN FULL TEXT:

FAR 52.202-1 – Definitions (Nov 2013)

When a solicitation provision or contract clause uses a word or term that is defined in the Federal Acquisition Regulation (FAR), the word or term has the same meaning as the definition in FAR 2.101 in effect at the time the solicitation was issued, unless--

- (a) The solicitation, or amended solicitation, provides a different definition;
- (b) The contracting parties agree to a different definition;
- (c) The part, subpart, or section of the FAR where the provision or clause is prescribed provides a different meaning; or
- (d) The word or term is defined in FAR Part 31, for use in the cost principles and procedures.

(End of Clause)

FAR 52.203-3 – Gratuities (Apr 1984)

(a) The right of the Contractor to proceed may be terminated by written notice if, after notice and hearing, the agency head or a designee determines that the Contractor, its agent, or another representative --

- (1) Offered or gave a gratuity (e.g., an entertainment or gift) to an officer, official, or employee of the Government; and
- (2) Intended, by the gratuity, to obtain a contract or favorable treatment under a contract.

(b) The facts supporting this determination may be reviewed by any court having lawful jurisdiction.

(c) If this contract is terminated under paragraph (a) of this clause, the Government is entitled --

(1) To pursue the same remedies as in a breach of the contract; and

(2) In addition to any other damages provided by law, to exemplary damages of not less than 3 nor more than 10 times the cost incurred by the Contractor in giving gratuities to the person concerned, as determined by the agency head or a designee. (This subparagraph (c)(2) is applicable only if this contract uses money appropriated to the Department of Defense.)

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

(End of Clause)

FAR 52.203-5 – Covenant Against Contingent Fees (May 2014)

(a) The Contractor warrants that no person or agency has been employed or retained to solicit or obtain this contract upon an agreement or understanding for a contingent fee, except a bona fide employee or agency. For breach or violation of this warranty, the Government shall have the right to annul this contract without liability or to deduct from the contract price or consideration, or otherwise recover, the full amount of the contingent fee.

(b) “Bona fide agency,” as used in this clause, means an established commercial or selling agency, maintained by a contractor for the purpose of securing business, that neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds itself out as being able to obtain any Government contract or contracts through improper influence.

“Bona fide employee,” as used in this clause, means a person, employed by a contractor and subject to the contractor’s supervision and control as to time, place, and manner of performance, who neither exerts nor proposes to exert improper influence to solicit or obtain Government contracts nor holds out as being able to obtain any Government contract or contracts through improper influence.

“Contingent fee,” as used in this clause, means any commission, percentage, brokerage, or other fee that is contingent upon the success that a person or concern has in securing a Government contract.

“Improper influence,” as used in this clause, means any influence that induces or tends to induce a Government employee or officer to give consideration or to act regarding a Government contract on any basis other than the merits of the matter.

(End of Clause)

FAR 52.203-7 – Anti-Kickback Procedures (May 2014)

(a) Definitions.

“Kickback,” as used in this clause, means any money, fee, commission, credit, gift, gratuity, thing of value, or compensation of any kind which is provided to any prime Contractor, prime Contractor employee, subcontractor, or subcontractor employee for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contract or in connection with a subcontract relating to a prime contract.

“Person,” as used in this clause, means a corporation, partnership, business association of any kind, trust, joint-stock company, or individual.

“Prime contract,” as used in this clause, means a contract or contractual action entered into by the United States for the purpose of obtaining supplies, materials, equipment, or services of any kind.

“Prime Contractor” as used in this clause, means a person who has entered into a prime contract with the United States.

“Prime Contractor employee,” as used in this clause, means any officer, partner, employee, or agent of a prime Contractor.

“Subcontract,” as used in this clause, means a contract or contractual action entered into by a prime Contractor or subcontractor for the purpose of obtaining supplies, materials, equipment, or services of any kind under a prime contract.

“Subcontractor,” as used in this clause,

(1) means any person, other than the prime Contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract, and

(2) includes any person who offers to furnish or furnishes general supplies to the prime Contractor or a higher tier subcontractor.

“Subcontractor employee,” as used in this clause, means any officer, partner, employee, or agent of a subcontractor.

(b) The 41 U.S.C. chapter 87, Kickbacks, prohibits any person from --

(1) Providing or attempting to provide or offering to provide any kickback;

(2) Soliciting, accepting, or attempting to accept any kickback; or

(3) Including, directly or indirectly, the amount of any kickback in the contract price charged by a prime Contractor to the United States or in the contract price charged by a subcontractor to a prime Contractor or higher tier subcontractor.

(c)

(1) The Contractor shall have in place and follow reasonable procedures designed to prevent and detect possible violations described in paragraph (b) of this clause in its own operations and direct business relationships.

(2) When the Contractor has reasonable grounds to believe that a violation described in paragraph (b) of this clause may have occurred, the Contractor shall promptly report in writing the possible violation. Such reports shall be made to the inspector general of the contracting agency, the head of the contracting agency if the agency does not have an inspector general, or the Attorney General.

(3) The Contractor shall cooperate fully with any Federal agency investigating a possible violation described in paragraph (b) of this clause.

(4) The Contracting Officer may

(i) offset the amount of the kickback against any monies owed by the United States under the prime contract and/or

(ii) direct that the Prime Contractor withhold from sums owed a subcontractor under the prime contract the amount of the kickback. The Contracting Officer may order that monies withheld under subdivision (c)(4)(ii) of this clause be paid over to the Government unless the Government has already offset those monies under subdivision (c)(4)(i) of this clause. In either case, the Prime Contractor shall notify the Contracting Officer when the monies are withheld.

(5) The Contractor agrees to incorporate the substance of this clause, including subparagraph (c)(5) but excepting subparagraph (c)(1), in all subcontracts under this contract which exceed \$150,000.

(End of Clause)

FAR 52.203-12 – Limitation on Payments to Influence Certain Federal Transactions (Oct 2010)

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

“Agency” means executive agency as defined in Federal Acquisition Regulation (FAR) 2.101.

“Covered Federal action” means any of the following Federal actions:

- (1) Awarding any Federal contract.
- (2) Making any Federal grant.
- (3) Making any Federal loan.
- (4) Entering into any cooperative agreement.

(5) Extending, continuing, renewing, amending, or modifying any Federal contract, grant, loan, or cooperative agreement.

“Indian tribe” and “tribal organization” have the meaning provided in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C.450B) and include Alaskan Natives.

“Influencing or attempting to influence” means making, with the intent to influence, any communication to or appearance before an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal action.

“Local government” means a unit of government in a State and, if chartered, established, or otherwise recognized by a State for the performance of a governmental duty, including a local public authority, a special district, an intrastate district, a council of governments, a sponsor group representative organization, and any other instrumentality of a local government.

“Officer or employee of an agency” includes the following individuals who are employed by an agency:

(1) An individual who is appointed to a position in the Government under Title 5, United States Code, including a position under a temporary appointment.

(2) A member of the uniformed services, as defined in subsection 101(3), Title 37, United States Code.

(3) A special Government employee, as defined in section 202, Title 18, United States Code.

(4) An individual who is a member of a Federal advisory committee, as defined by the Federal Advisory Committee Act, Title 5, United States Code, appendix 2.

“Person” means an individual, corporation, company, association, authority, firm, partnership, society, State, and local government, regardless of whether such entity is operated for profit, or not for profit. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and are permitted by other Federal law.

“Reasonable compensation” means, with respect to a regularly employed officer or employee of any person, compensation that is consistent with the normal compensation for such officer or employee for work that is not furnished to, not funded by, or not furnished in cooperation with the Federal Government.

“Reasonable payment” means, with respect to professional and other technical services, a payment in an amount that is consistent with the amount normally paid for such services in the private sector.

“Recipient” includes the Contractor and all subcontractors. This term excludes an Indian tribe, tribal organization, or any other Indian organization eligible to receive Federal contracts, grants, cooperative agreements, or loans from an agency, but only with respect to expenditures by such tribe or organization that are made for purposes specified in paragraph (b) of this clause and *are* permitted by other Federal law.

“Regularly employed” means, with respect to an officer or employee of a person requesting or receiving a Federal contract, an officer or employee who is employed by such person for at least 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person for receipt of such contract. An officer or employee who is employed by such person for less than 130 working days within 1 year immediately preceding the date of the submission that initiates agency consideration of such person shall be considered to be regularly employed as soon as he or she is employed by such person for 130 working days.

“State” means a State of the United States, the District of Columbia, or an outlying area of the United States, an agency or instrumentality of a State, and multi-State, regional, or interstate entity having governmental duties and powers.

(b) *Prohibition.* 31 U.S.C. 1352 prohibits a recipient of a Federal contract, grant, loan, or cooperative agreement from using appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any covered Federal actions. In accordance with 31 U.S.C. 1352 the Contractor shall not use appropriated funds to pay any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the award of this contractor the extension, continuation, renewal, amendment, or modification of this contract.

(1) The term *appropriated funds* does not include profit or fee from a covered Federal action.

(2) To the extent the Contractor can demonstrate that the Contractor has sufficient monies, other than Federal appropriated funds, the Government will assume that these other monies were spent for any influencing activities that would be unallowable if paid for with Federal appropriated funds.

(c) *Exceptions.* The prohibition in paragraph (b) of this clause does not apply under the following conditions:

(1) Agency and legislative liaison by Contractor employees.

(i) Payment of reasonable compensation made to an officer or employee of the Contractor if the payment is for agency and legislative liaison activities not directly related to this contract. For purposes of this paragraph, providing any information specifically requested by an agency or Congress is permitted at any time.

(ii) Participating with an agency in discussions that are not related to a specific solicitation for any covered Federal action, but that concern—

(A) The qualities and characteristics (including individual demonstrations) of the person's products or services, conditions or terms of sale, and service capabilities; or

(B) The application or adaptation of the person's products or services for an agency's use.

(iii) Providing prior to formal solicitation of any covered Federal action any information not specifically requested but necessary for an agency to make an informed decision about initiation of a covered Federal action;

(iv) Participating in technical discussions regarding the preparation of an unsolicited proposal prior to its official submission; and

(v) Making capability presentations prior to formal solicitation of any covered Federal action by persons seeking awards from an agency pursuant to the provisions of the Small Business Act, as amended by Pub. L. 95-507, and subsequent amendments.

(2) Professional and technical services.

(i) A payment of reasonable compensation made to an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action, if payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action.

(ii) Any reasonable payment to a person, other than an officer or employee of a person requesting or receiving a covered Federal action or an extension, continuation, renewal, amendment, or modification of a covered Federal action if the payment is for professional or technical services rendered directly in the preparation, submission, or negotiation of any bid, proposal, or application for that Federal action or for meeting requirements imposed by or pursuant to law as a condition for receiving that Federal action. Persons other than officers or employees of a person requesting or receiving a covered Federal action include consultants and trade associations.

(iii) As used in this paragraph (c)(2), "professional and technical services" are limited to advice and analysis directly applying any professional or technical discipline (for examples, see FAR 3.803(a)(2)(iii)).

(iv) Requirements imposed by or pursuant to law as a condition for receiving a covered Federal award include those required by law or regulation and any other requirements in the actual award documents.

(3) Only those communications and services expressly authorized by paragraphs (c)(1) and (2) of this clause are permitted.

(d) Disclosure.

(1) If the Contractor did not submit OMB Standard Form LLL, Disclosure of Lobbying Activities, with its offer, but registrants under the Lobbying Disclosure Act of 1995 have subsequently made a lobbying contact on behalf of the Contractor with respect to this contract, the Contractor shall complete and submit OMB Standard Form LLL to provide the name of the lobbying registrants, including the individuals performing the services.

(2) If the Contractor did submit OMB Standard Form LLL disclosure pursuant to paragraph (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, and a change occurs that affects Block 10 of the OMB Standard Form LLL (name and address of lobbying registrant or individuals performing services), the Contractor shall, at the end of the calendar quarter in which the change occurs, submit to the Contracting Officer within 30 days an updated disclosure using OMB Standard Form LLL.

(e) Penalties.

(1) Any person who makes an expenditure prohibited under paragraph (b) of this clause or who fails to file or amend the disclosure to be filed or amended by paragraph (d) of this clause shall be subject to civil penalties as provided for by 31 U.S.C.1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(2) Contractors may rely without liability on the representation made by their subcontractors in the certification and disclosure form.

(f) *Cost allowability.* Nothing in this clause makes allowable or reasonable any costs which would otherwise be unallowable or unreasonable. Conversely, costs made specifically unallowable by the requirements in this clause will not be made allowable under any other provision.

(g) *Subcontracts.*

(1) The Contractor shall obtain a declaration, including the certification and disclosure in paragraphs (c) and (d) of the provision at FAR 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions, from each person requesting or receiving a subcontract exceeding \$150,000 under this contract. The Contractor or subcontractor that awards the subcontract shall retain the declaration.

(2) A copy of each subcontractor disclosure form (but not certifications) shall be forwarded from tier to tier until received by the prime Contractor. The prime Contractor shall, at the end of the calendar quarter in which the disclosure form is submitted by the subcontractor, submit to the

Contracting Officer within 30 days a copy of all disclosures. Each subcontractor certification shall be retained in the subcontract file of the awarding Contractor.

(3) The Contractor shall include the substance of this clause, including this paragraph (g), in any subcontract exceeding \$150,000.

(End of Clause)

FAR 52.203-13 – Contractor Code of Business Ethics and Conduct (Oct 2015)

(a) *Definition.* As used in this clause--

“Agent” means any individual, including a director, an officer, an employee, or an independent Contractor, authorized to act on behalf of the organization.

“Full cooperation”—

(1) Means disclosure to the Government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to Government auditors’ and investigators’ request for documents and access to employees with information;

(2) Does not foreclose any Contractor rights arising in law, the FAR, or the terms of the contract. It does not require—

(i) A Contractor to waive its attorney-client privilege or the protections afforded by the attorney work product doctrine; or

(ii) Any officer, director, owner, or employee of the Contractor, including a sole proprietor, to waive his or her attorney client privilege or Fifth Amendment rights; and

(3) Does not restrict a Contractor from—

(i) Conducting an internal investigation; or

(ii) Defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation.

“Principal” means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (*e.g.*, general manager; plant manager; head of a division or business segment; and similar positions).

“Subcontract” means any contract entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract.

“Subcontractor” means any supplier, distributor, vendor, or firm that furnished supplies or services to or for a prime contractor or another subcontractor.

“United States” means the 50 States, the District of Columbia, and outlying areas.

(b) Code of business ethics and conduct.

(1) Within 30 days after contract award, unless the Contracting Officer establishes a longer time period, the Contractor shall—

(i) Have a written code of business ethics and conduct;

(ii) Make a copy of the code available to each employee engaged in performance of the contract.

(2) The Contractor shall—

(i) Exercise due diligence to prevent and detect criminal conduct; and

(ii) Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law.

(3)

(i) The Contractor shall timely disclose, in writing, to the agency Office of the Inspector General (OIG), with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed—

(A) A violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code; or

(B) A violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(ii) The Government, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the Contractor’s disclosure as confidential where the information has been marked “confidential” or “proprietary” by the company. To the extent permitted by the law and regulation, such information will not be released by the Government to the public pursuant to a Freedom of Information Act request, 5 U.S.C. Section 552, without prior notification to the Contractor. The Government may transfer documents provided by the Contractor to any department or agency within the Executive Branch if the information relates to matters within the organization’s jurisdiction.

(iii) If the violation relates to an order against a Governmentwide acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any

other procurement instrument intended for use by multiple agencies, the Contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract.

(c) *Business ethics awareness and compliance program and internal control system.* This paragraph (c) does not apply if the Contractor has represented itself as a small business concern pursuant to the award of this contract or if this contract is for the acquisition of a commercial item as defined at FAR 2.101. The Contractor shall establish the following within 90 days after contract award, unless the Contracting Officer establishes a longer time period:

(1) An ongoing business ethics awareness and compliance program.

(i) This program shall include reasonable steps to communicate periodically and in a practical manner the Contractor's standards and procedures and other aspects of the Contractor's business ethics awareness and compliance program and internal control system, by conducting effective training programs and otherwise disseminating information appropriate to an individual's respective roles and responsibilities.

(ii) The training conducted under this program shall be provided to the Contractor's principals and employees, and as appropriate, the Contractor's agents and subcontractors.

(2) An internal control system.

(i) The Contractor's internal control system shall—

(A) Establish standards and procedures to facilitate timely discovery of improper conduct in connection with Government contracts; and

(B) Ensure corrective measures are promptly instituted and carried out.

(ii) At a minimum, the Contractor's internal control system shall provide for the following:

(A) Assignment of responsibility at a sufficiently high level and adequate resources to ensure effectiveness of the business ethics awareness and compliance program and internal control system.

(B) Reasonable efforts not to include an individual as a principal, whom due diligence would have exposed as having engaged in conduct that is in conflict with the Contractor's code of business ethics and conduct.

(C) Periodic reviews of company business practices, procedures, policies, and internal controls for compliance with the Contractor's code of business ethics and conduct and special requirements of Government contracting, including—

(1) Monitoring and auditing to detect criminal conduct;

(2) Periodic evaluation of the effectiveness of the business ethics awareness and compliance program and internal control system, especially if criminal conduct has been detected; and

(3) Periodic assessment of the risk of criminal conduct, with appropriate steps to design, implement, or modify the business ethics awareness and compliance program and the internal control system as necessary to reduce the risk of criminal conduct identified through this process.

(D) An internal reporting mechanism, such as a hotline, which allows for anonymity or confidentiality, by which employees may report suspected instances of improper conduct, and instructions that encourage employees to make such reports.

(E) Disciplinary action for improper conduct or for failing to take reasonable steps to prevent or detect improper conduct.

(F) Timely disclosure, in writing, to the agency OIG, with a copy to the Contracting Officer, whenever, in connection with the award, performance, or closeout of any Government contract performed by the Contractor or a subcontractor thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation of Federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 U.S.C. or a violation of the civil False Claims Act (31 U.S.C. 3729-3733).

(1) If a violation relates to more than one Government contract, the Contractor may make the disclosure to the agency OIG and Contracting Officer responsible for the largest dollar value contract impacted by the violation.

(2) If the violation relates to an order against a Governmentwide acquisition contract, a multi-agency contract, a multiple-award schedule contract such as the Federal Supply Schedule, or any other procurement instrument intended for use by multiple agencies, the contractor shall notify the OIG of the ordering agency and the IG of the agency responsible for the basic contract, and the respective agencies' contracting officers.

(3) The disclosure requirement for an individual contract continues until at least 3 years after final payment on the contract.

(4) The Government will safeguard such disclosures in accordance with paragraph (b)(3)(ii) of this clause.

(G) Full cooperation with any Government agencies responsible for audits, investigations, or corrective actions.

(d) Subcontracts.

(1) The Contractor shall include the substance of this clause, including this paragraph (d), in subcontracts that have a value in excess of \$5.5 million and a performance period of more than 120 days.

(2) In altering this clause to identify the appropriate parties, all disclosures of violation of the civil False Claims Act or of Federal criminal law shall be directed to the agency Office of the Inspector General, with a copy to the Contracting Officer.

(End of clause)

FAR 52.204-19 – Incorporation by Reference of Representations and Certifications (Dec 2014)

The Contractor’s representations and certifications, including those completed electronically via the System for Award Management (SAM), are incorporated by reference into the contract.

(End of clause)

52.212-5 -- Contract Terms and Conditions Required to Implement Statutes or Executive Orders -- Commercial Items (Jan 2019)

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

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(4) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(5) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

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

[Contracting Officer check as appropriate.]

X (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

(2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

X (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Oct 2018) (Pub. L. 109-282) (31 U.S.C. 6101 note).

(5) [Reserved]

X (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

(7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government' Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

X (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Oct 2018) (41 U.S.C. 2313).

(10) [Reserved]

(11)(i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

(ii) Alternate I (Nov 2011) of 52.219-3.

(12) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

(ii) Alternate I (Jan 2011) of 52.219-4.

(13) [Reserved]

(14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

(ii) Alternate I (Nov 2011).

(iii) Alternate II (Nov 2011).

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

(ii) Alternate I (Oct 1995) of 52.219-7.

(iii) Alternate II (Mar 2004) of 52.219-7.

(16) 52.219-8, Utilization of Small Business Concerns (Oct 2018) (15 U.S.C. 637(d)(2) and (3)).

(17) (i) 52.219-9, Small Business Subcontracting Plan (Oct 2018) (15 U.S.C. 637 (d)(4))

(ii) Alternate I (Nov 2016) of 52.219-9.

(iii) Alternate II (Nov 2016) of 52.219-9.

(iv) Alternate III (Nov 2016) of 52.219-9.

(v) Alternate IV (Aug 2018) of 52.219-9.

(18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

(19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).

(20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

(21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).

(22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).

(23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).

(24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).

X (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

X (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).

- X (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).
- X (28) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
- X (29) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
- X (30) 52.222-36, Affirmative Action for Workers with Disabilities (July 2014) (29 U.S.C. 793).
- X (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).
- X (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).
- X (33) (i) 52.222-50, Combating Trafficking in Persons (Jan 2019) (22 U.S.C. chapter 78 and E.O. 13627).
- (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).
- (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (Executive Order 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)
- (35)(i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)
- (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).
- (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).
- (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514).
- (ii) Alternate I (Oct 2015) of 52.223-13.
- (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).
- (ii) Alternate I (Jun 2014) of 52.223-14.

(40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

(41) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514)

(ii) Alternate I (Jun 2014) of 52.223-16.

X (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).

(43) 52.223.20, Aerosols (Jun 2016) (E.O. 13693).

(44) 52.223.21, Foams (Jun 2016) (E.O. 13696).

X (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(ii) Alternate I (Jan 2017) of 52.224-3.

X (46) 52.225-1, Buy American Act--Supplies (May 2014) (41 U.S.C. chapter 83).

(47) (i) 52.225-3, Buy American Act--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

(ii) Alternate I (May 2014) of 52.225-3.

(iii) Alternate II (May 2014) of 52.225-3.

(iv) Alternate III (May 2014) of 52.225-3.

(48) 52.225-5, Trade Agreements (Aug 2018) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

X (49) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

(50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2303 Note).

(51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

(52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

(53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

(54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

X (55) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Oct 2018) (31 U.S.C. 3332).

(56) 52.232-34, Payment by Electronic Funds Transfer— Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

(57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

X (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

(59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

(60) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

(ii) Alternate I (Apr 2003) of 52.247-64.

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

[Contracting Officer check as appropriate.]

(1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)

X (2) 52.222-41, Service Contract Labor Standards (Aug 2018) (41 U.S.C. chapter 67.).

(3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

X (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (Aug 2018) (29 U.S.C.206 and 41 U.S.C. chapter 67).

(5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

(6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

(7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

(8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015)

(9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

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

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

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

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

(e) (1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than

those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds \$700,000 (\$1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(v) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (Aug 2018), (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64

(2) While not required, the contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

FAR 52.217-8 Option to Extend Services (Nov 1999): The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor prior to task order expiration

(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 prior to expiration of the contract term; 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 2 years and 6 months.

(End of Clause)

FAR 52.227-14 – Rights in Data - General (May 2014)

(a) *Definitions.* As used in this clause--

“Computer database” or “database” means a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

“Computer software”—

(1) *Means*

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

“Computer software documentation” means owner’s manuals, user’s manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

“Data” means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

“Form, fit, and function data” means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating, and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics,

and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

“Limited rights” means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of subparagraph (g)(2) if included in this clause.

“Limited rights data” means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

“Restricted computer software” means computer software developed at private expense and that is a trade secret; is commercial or financial and is confidential or privileged; or is copyrighted computer software, including minor modifications of the computer software.

“Restricted rights,” as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

“Technical data” means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 116).

“Unlimited rights” means the right of the Government 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.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

- (i) Data first produced in the performance of this contract;
- (ii) Form, fit, and function data delivered under this contract;
- (iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and
- (iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

- (i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate use of, add or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) *Copyright*—

(1) *Data first produced in the performance of this contract.*

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may establish, without prior approval of the Contracting Officer, claim to copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government. For computer software, the Contractor grants to the Government and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in subparagraph (c)(1) of this clause or; if such data are restricted computer software, the Government shall acquire a copyright license as set forth in subparagraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract which contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless otherwise specifically authorized otherwise in writing by the Contracting Officer.

(e) *Unauthorized marking of data.*

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g)(4) of this clause and use of the notices is not authorized by this clause, or if such data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 4703, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in subdivision (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be canceled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination shall become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government shall continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in subparagraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of this clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as a result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) *Omitted or incorrect markings.*

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of such data, permission to have authorized notices placed on qualifying data at the Contractor's expense, and the Contracting Officer may agree to do so if the Contractor—

- (i) Identifies the data to which the omitted notice is to be applied;
- (ii) Demonstrates that the omission of the notice was inadvertent;
- (iii) Establishes that the use of the proposed notice is authorized; and
- (iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

- (i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized, or
- (ii) Correct any incorrect notices.

(g) *Protection of limited rights data and restricted computer software.*

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

- (i) Identify the data being withheld; and
- (ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government such rights, the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

(End of Clause)

52.227-16 -- Additional Data Requirements (Jun 1987)

(a) In addition to the data (as defined in the clause at 52.227-14, Rights in Data -- General clause or other equivalent included in this contract) specified elsewhere in this contract to be delivered, the Contracting Officer may, at any time during contract performance or within a period of 3 years after acceptance of all items to be delivered under this contract, order any data first produced or specifically used in the performance of this contract.

(b) The Rights in Data -- General clause or other equivalent included in this contract is applicable to all data ordered under this Additional Data Requirements clause. Nothing contained in this clause shall require the Contractor to deliver any data the withholding of which is authorized by the Rights in Data -- General or other equivalent clause of this contract, or data which are specifically identified in this contract as not subject to this clause.

(c) When data are to be delivered under this clause, the Contractor will be compensated for converting the data into the prescribed form, for reproduction, and for delivery.

(d) The Contracting Officer may release the Contractor from the requirements of this clause for specifically identified data items at any time during the 3-year period set forth in paragraph (a) of this clause.

(End of Clause)

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

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

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

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

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

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

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

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

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

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

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

(End of clause)

HSAR 3052.204-71 Contractor employee access (SEP 2012)

(a) *Sensitive Information*, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);
 - (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
 - (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
 - (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
- (c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
- (d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
- (e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
- (f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

**ALTERNATE I
(SEP 2012)**

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

- (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)

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

(a) Prohibitions.

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

(b) Definitions. As used in this clause:

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

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

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

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

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

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

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

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

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

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

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

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

(ii) Stock of such entity which is sold in a public offering related to 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]:

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 3052.222-71 Strikes or Picketing Affecting Access to a DHS Facility (DEC 2003)

If the Contracting Officer notifies the Contractor in writing that a strike or picketing: (a) is directed at the Contractor or subcontractor or any employee of either; and (b) impedes or threatens to impede access by any person to a DHS facility where the site of the work is located, the Contractor shall take all appropriate action to end such strike or picketing, including, if necessary, the filing of a charge of unfair labor practice with the National Labor Relations Board or the use of other available judicial or administrative remedies.

(End of clause)

HSAR 3052.228-70 Insurance (DEC 2003)

In accordance with the clause entitled “Insurance-Work on a Government Installation” (or Insurance-Liability to Third Persons) in Section I, insurance of the following kinds and minimum amounts shall be provided and maintained during the period of performance of this contract.

- (a) Worker’s compensation and employer’s liability. The contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).
- (b) General liability. The contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).
- (c) Automobile liability. The contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c)

(End of clause)

HSAR 3052.242-72 Contracting Officer's Technical Representative (DEC 2003)

(a) The Contracting Officer may designate Government personnel to act as the Contracting Officer's Technical Representative (COTR) to perform functions under the contract such as review or inspection and acceptance of supplies, services, including construction, and other functions of a technical nature. The Contracting Officer will provide a written notice of such designation to the Contractor within five working days after contract award or for construction, not less than five working days prior to giving the contractor the notice to proceed. The designation letter will set forth the authorities and limitations of the COTR under the contract.

(b) The Contracting Officer cannot authorize the COTR or any other representative to sign documents, such as contracts, contract modifications, etc., that require the signature of the Contracting Officer.

(End of clause)

ICE Information Governance and Privacy Requirements Clause (JUL 2017)

Guidance: In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following IGP clause must be included in its entirety in all contracts. No section of this clause may be read as self-deleting unless the terms of the contract meet the requirements for self-deletion as specified in this clause.

A. Limiting Access to Privacy Act and Other Sensitive Information

(1) Privacy Act Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974 the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNs of other agencies may be accessed through the agencies' websites or by searching FDsys, the Federal Digital System, available at <http://www.gpo.gov/fdsys/>. SORNs may be updated at any time.

(2) Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

(3) Prior Approval Required to Hire Subcontractors

The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) 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 Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

(4) Separation Checklist for Contractor Employees

Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization 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 to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

B. Privacy Training, Safeguarding, and Remediation

If the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses are included in this contract, section B of this clause is deemed self-deleting.

(1) Required Security and Privacy Training for Contractors

Contractor shall provide training for all employees, including Subcontractors and independent contractors who have access to sensitive personally identifiable information (PII) as well as the creation, use, dissemination and/or destruction of sensitive PII at the outset of the employee's work on the contract and every year thereafter. Training must include procedures on how to properly handle sensitive PII, including security requirements for the transporting or transmission of sensitive PII, and reporting requirements for a suspected breach or loss of sensitive PII. All Contractor employees are required to take the *Privacy at DHS: Protecting Personal Information* training course. This course, along with more information about DHS security and training requirements for Contractors, is available at www.dhs.gov/dhs-security-and-training-requirements-contractors. The Federal Information Security Management Act (FISMA) requires all individuals accessing ICE information to take the annual Information Assurance Awareness Training course. These courses are available through the ICE intranet site or the Agency may also make the training available through hypertext links or CD. The Contractor shall maintain copies of employees' certificates of completion as a record of

compliance and must submit an annual e-mail notification to the ICE Contracting Officer's Representative that the required training has been completed for all the Contractor's employees.

(2) Safeguarding Sensitive PII Requirement

Contractor employees shall comply with the Handbook for Safeguarding sensitive PII at DHS at all times when handling sensitive PII, including the encryption of sensitive PII as required in the Handbook. This requirement will be flowed down to all subcontracts and lower tiered subcontracts as well.

(3) Non-Disclosure Agreement Requirement

All Contractor personnel that may have access to PII or other sensitive information shall be required to sign a Non-Disclosure Agreement (DHS Form 11000-6) prior to commencing work. 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) Prohibition on Use of PII in Vendor Billing and Administrative Records

The Contractor's invoicing, billing, and other financial/administrative records/databases may not store or include any sensitive Government information, such as PII that is created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the Contracting Officer, Contracting Officer's Representative, or other ICE personnel associated with the administration of the contract in the invoices as needed.

(5) Reporting Suspected Loss of Sensitive PII

Contractors must report the suspected loss or compromise of sensitive PII to ICE in a timely manner and cooperate with ICE's inquiry into the incident and efforts to remediate any harm to potential victims.

1. The Contractor must develop and include in its security plan (which is submitted to ICE) an internal system by which its employees and Subcontractors are trained to identify and report the potential loss or compromise of sensitive PII.
2. The Contractor must report the suspected loss or compromise of sensitive PII by its employees or Subcontractors to the ICE Security Operations Center (480-496-6627), the Contracting Officer's Representative (COR), and the Contracting Officer within one (1) hour of the initial discovery.
3. The Contractor must provide a written report to ICE within 24 hours of the suspected loss or compromise of sensitive PII by its employees or Subcontractors. The report must contain the following information:
 - a. Narrative or detailed description of the events surrounding the suspected loss or compromise of information.
 - b. Date, time, and location of the incident.
 - c. Type of information lost or compromised.

- d. Contractor's assessment of the likelihood that the information was compromised or lost and the reasons behind the assessment.
- e. Names of person(s) involved, including victim, Contractor employee/Subcontractor and any witnesses.
- f. Cause of the incident and whether the company's security plan was followed and, if not, which specific provisions were not followed.
- g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
- h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

4. 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.

5. At the Government's discretion, Contractor employees or Subcontractor employees may be identified as no longer eligible to access sensitive PII or to work on that contract based on their actions related to the loss or compromise of sensitive PII.

(6) Victim Remediation

The Contractor is responsible for notifying victims and providing victim remediation services in the event of a loss or compromise of sensitive PII held by the Contractor, its agents, or its Subcontractors, under this contract. Victim remediation services shall include at least 18 months of credit monitoring and, for serious or large incidents as determined by the Government, call center help desk services for the individuals whose sensitive PII was lost or compromised. The Contractor and ICE will collaborate and agree on the method and content of any notification that may be required to be sent to individuals whose sensitive PII was lost or compromised.

C. Government Records Training, Ownership, and Management

(1) Records Management Training and Compliance

(a) The Contractor shall provide DHS basic records management training for all employees and Subcontractors that have access to sensitive PII as well as to those involved in the creation, use, dissemination and/or destruction of sensitive PII. This training will be provided at the outset of the Subcontractor's/employee's work on the contract and every year thereafter. This training can be obtained via links on the ICE intranet site or it may be made available through other means (e.g., CD or online). The Contractor shall maintain copies of certificates as a record of compliance and must submit an e-mail notification annually to the Contracting Officer's Representative verifying that all employees working under this contract have completed the required records management training.

(b) 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.

(2) Records Creation, Ownership, and Disposition

(a) The Contractor shall not create or maintain any records not specifically tied to or authorized by the contract using Government IT equipment and/or Government records or that contain Government Agency data. The Contractor shall certify in writing the destruction or return of all Government data at the conclusion of the contract or at a time otherwise specified in the contract.

(b) Except as stated in the Performance Work Statement and, where applicable, 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 and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

(d) The Contractor shall not retain, use, sell, disseminate, or dispose of any government data/records or deliverables without the express written permission of the Contracting Officer or Contracting Officer's Representative. 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.

D. Data Privacy and Oversight

Section D applies to information technology (IT) contracts. If this is not an IT contract, section D may read as self-deleting.

(1) Restrictions on Testing or Training Using Real Data Containing PII

The use of real data containing sensitive PII from any source for testing or training purposes is generally prohibited. The Contractor shall use synthetic or de-identified real data for testing or training whenever feasible. ICE policy requires that any proposal to use of real data or de-identified data for IT system testing or training be approved by the ICE Privacy Officer and Chief Information Security Officer (CISO) in advance. In the event performance of the contract requires or necessitates the use of real data for system-testing or training purposes, the Contractor in coordination with the Contracting Officer or Contracting Officer's Representative and Government program manager shall obtain approval from the ICE Privacy Office and CISO and complete any required documentation.

If this IT contract contains the Safeguarding of Sensitive Information (MAR 2015) and Information Technology Security and Privacy Training (MAR 2015) clauses, section D(2) of this clause is deemed self-deleting.

(2) Requirements for Contractor IT Systems Hosting Government Data

The Contractor is required to obtain a Certification and Accreditation for any IT environment owned or controlled by the Contractor or any Subcontractor on which Government data shall reside for the purposes of IT system development, design, data migration, testing, training, maintenance, use, or disposal.

(3) Requirement to Support Privacy Compliance

(a) The Contractor shall support the completion of the Privacy Threshold Analysis (PTA) document when it is required. PTAs are triggered by the creation, modification, upgrade, or disposition of an IT system, and must be renewed at least every three 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 adequate support to complete the PIA in a timely manner, and shall ensure that project management plans and schedules include the PTA, PIA, and SORN (to the extent required) as milestones. Additional information on the privacy compliance process at DHS, including PTAs, PIAs, and SORNs, is located on the DHS Privacy Office website (www.dhs.gov/privacy) under "Compliance." DHS Privacy Policy Guidance Memorandum 2008-02 sets forth when a PIA will be required at DHS, and the Privacy Impact Assessment Guidance and Template outline the requirements and format for the PIA.

(b) If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under "Key Personnel." 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 is 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. The Privacy Lead:

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

(c) If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if

required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Office and other offices are answered in a timely fashion.

(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)

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)

Page 205

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 206

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 207

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 208

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 209

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 210

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 211

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 212

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 213

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 214

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 215

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 216

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 217

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 218

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 219

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 220

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 221

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 222

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 223

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 224

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 225

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 226

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 227

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 228

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 229

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 230

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 231

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 232

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 233

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 234

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 235

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act