SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
OIT209004	1	64

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
47QTCK18D0034		70SBUR20F00000098	70SBUR19R00000057	10/18/2019

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	EMILIO CIBULA	802-872-4640	

9. ISSUED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

☐ SMALL BUSINESS
☐ HUBZONE SMALL BUSINESS
☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
☐ EDWOSB
☐ 8(A)

NAICS: 541512
SIZE STANDARD: $30.0

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☒ SEE SCHEDULE	Net 30	☐	☐RFQ ☐IFB ☐RFP

15. DELIVER TO — CODE: HQOIT

Department of Homeland Security
US Citizenship & Immigration Svcs
Office of Information Technology
111 Massachusetts Ave, NW
Suite 5000
Washington DC 20529

16. ADMINISTERED BY — CODE: CIS

USCIS Contracting Office
Department of Homeland Security
70 Kimball Avenue
South Burlington VT 05403

17a. CONTRACTOR/ OFFEROR — CODE: 1325996680000 — FACILITY CODE:

SEVATEC INC
2815 OLD LEE HWY
FAIRFAX VA 220314303

TELEPHONE NO.

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18a. PAYMENT WILL BE MADE BY — CODE: WEBVIEW

See Invoicing Instructions

☐ 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 132599668+0000 Part I - Schedule This is a hybrid Firm-Fixed Price (FFP) and Time and materials (T&M) Alliant 2 Unrestricted task order for Accounts Public DevSecOps Services (ACCTSPUB). Along with the task order terms and conditions, all Alliant 2 Unrestricted GWAC terms and conditions are applicable to the resultant task *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)* [redacted]

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. 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 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED.

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER [redacted] ISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL ND CONDITIONS SPECIFIED.

☒ 29. AWARD OF CONTRACT: 70SBUR19R00000057 OFFER DATED 10/21/2019. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS: ALL

30a. [redacted] R

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
CHRISTOPHER C HATIN Digitally signed by CHRISTOPHER C HATIN Date: 2020.04.16 17:24:09 -04'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
[redacted]	[redacted]	Christopher C. Hatin	

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	order. The applicable Product Service Code (PSC) is D302. The period of performance will consist of a four (4) month base period and two (2) twelve (12) month option periods, for a total period of performance of 28 months total with specific dates to be established at the Authorization to Proceed (ATP): Base: 4-Months Option 1: 12-Months Option 2: 12-Months Dates for the period of performance will be adjusted upon issuance of the ATP. No invoicing may occur until after the ATP. AAP Number: 2019046139 Accounting Info: ITACPB0 CN0 EP 20-05-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000				
0001	Key Personnel SOW Sections 3 and 5 (FFP)			[redacted]	
0002	DevSecOps Team One Continued ...			[redacted]	

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	SOW Section 3 (T&M)				
0003	DevSecOps Team Two SOW Section 3 (T&M)				[redacted]
0004	DevSecOps Team Three SOW Section 3 (T&M)				[redacted]
0005	Contract Access Fee (CAF) (Usage Fee) for required CLINs (Cost-Reimbursement) Not to Exceed Amount				[redacted]
0006	Optional Administrative Support Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in the base period) Amount: [redacted] (Option Line Item)				[redacted]
0007	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 0006 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
0008	Optional Mobile App Client Development Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in base period) Amount: [redacted] (Option Line Item)				[redacted]
0009	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 0008 (Cost-Reimbursement) Not to Exceed Amount Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Amount: [redacted] (Option Line Item)				
0010	Optional DevSecOps Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in base period) Amount: [redacted] (Option Line Item)			[redacted]	
0011	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 0010 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)			[redacted]	
0012	Travel SOW Section 8.3 (NTE) (Optional Line Item to be exercised anytime in base period) Amount: [redacted] (Option Line Item)			[redacted]	
0013	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 0012 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)			[redacted]	
1001	Key Personnel SOW Sections 3 and 5 (FFP) Amount: [redacted] (Option Line Item)			[redacted]	
1002	DevSecOps Team One SOW Section 3 (T&M) Amount: [redacted] (Option Line Item)			[redacted]	
1003	DevSecOps Team Two SOW Section 3 Continued ...			[redacted]	

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(T&M) Amount: [redacted] (Option Line Item)				
1004	DevSecOps Team Three SOW Section 3 (T&M) Amount: [redacted] (Option Line Item)				[redacted]
1005	Contract Access Fee (CAF) (Usage Fee) for required CLINs (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
1006	Optional Administrative Support Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in option period one) Amount: [redacted] (Option Line Item)				[redacted]
1007	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 1006 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
1008	Optional Mobile App Client Development Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in option period one) Amount: [redacted] (Option Line Item)				[redacted]
1009	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 1008 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1010	Optional DevSecOps Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in option period one) Amount: [redacted] (Option Line Item)				[redacted]
1011	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 1010 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
1012	Travel SOW Section 8.3 (NTE) (Optional Line Item to be exercised anytime in option period one) Amount: [redacted] (Option Line Item) FOB: Destination				[redacted]
1013	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 1012 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
2001	Key Personnel SOW Section 3 and 5 (FFP) Amount: [redacted] (Option Line Item)				[redacted]
2002	DevSecOps Team One SOW Section 3 (T&M) Amount: [redacted] (Option Line Item)				[redacted]
2003	DevSecOps Team Two SOW Section 3 (T&M) Amount: [redacted] (Option Line Item) Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2004	DevSecOps Team Three SOW Section 3 (T&M) Amount: [redacted] (Option Line Item)				[redacted]
2005	Contract Access Fee (CAF) (Usage Fee) for required CLINs (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
2006	Optional Administrative Support Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in option period two) Amount: [redacted] (Option Line Item)				[redacted]
2007	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 2006 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
2008	Optional Mobile App Client Development Team SOW Section 3 (T&M) (Optional Line Item to be exercised anytime in option period two) Amount: [redacted] (Option Line Item)				[redacted]
2009	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 2008 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)				[redacted]
2010	Optional DevSecOps Team SOW Section 3 Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(T&M) (Optional Line Item to be exercised anytime in option period two) Amount: [redacted] (Option Line Item)				
2011	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 2010 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item)			[redacted]	
2012	Travel SOW Section 8.3 (NTE) (Optional Line Item to be exercised anytime in option period two) Amount: [redacted] (Option Line Item) FOB: Destination			[redacted]	
2013	Contract Access Fee (CAF) (Usage Fee) for optional CLIN 2012 (Cost-Reimbursement) Not to Exceed Amount Amount: [redacted] (Option Line Item) - Part II - Task Order Clauses - Part III - Documents, Exhibits, or Attachments The total amount of award: [redacted]. The obligation for this award is shown in box 26.			[redacted]	

Part II - Task Order Clauses

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.204-9	**Personal Identity Verification of Contractor Personnel**	(Jan 2011)
52.227-17	**Rights in Data -- Special Works**	(Dec 2007)
52.232-39	**Unenforceability of Unauthorized Obligations**	(Jun 2013)
52.245-1	**Government Property**	(Jan 2017)
52.245-9	**Use and Charges**	(Apr 2012)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (AUG 2019)

(a) Definitions. As used in this clause--
Covered foreign country means The People's Republic of China. Covered telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--
    i. Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
    ii. For reasons relating to regional stability or surreptitious listening;
(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817). Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.

(c) Exceptions. This clause does not prohibit contractors from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

i. Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

ii. Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of Clause)

52.212-4 **Contract Terms and Conditions -- Commercial Items, *Alternate I*** (Oct 2018)

(a) *Inspection/Acceptance.* (1) The Government has the right to inspect and test all materials furnished and services performed under this contract, to the extent practicable at all places and times, including the period of performance, and in any event before acceptance. The Government may also inspect the plant or plants of the Contractor or any subcontractor engaged in contract performance. The Government will perform inspections and tests in a manner that will not unduly delay the work.

(2) If the Government performs inspection or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish and shall require subcontractors to furnish all reasonable facilities and assistance for the safe and convenient performance of these duties.

(3) Unless otherwise specified in the contract, the Government will accept or reject services and materials at the place of delivery as promptly as practicable after delivery, and they will be presumed accepted 60 days after the date of delivery, unless accepted earlier.

(4) At any time during contract performance, but not later than 6 months (or such other time as may be specified in the contract) after acceptance of the services or materials last delivered under this contract, the Government may require the Contractor to replace or correct services or materials that at time of delivery failed to meet contract requirements. Except as otherwise specified in paragraph (a)(6) of this clause, the cost of replacement or correction shall be determined under paragraph (i) of this clause, but the "hourly rate" for labor hours incurred in the replacement or correction shall be reduced to exclude that portion of the rate attributable to profit. Unless otherwise specified below, the portion of the "hourly rate" attributable to profit shall be 10 percent. The Contractor shall not tender for acceptance materials and services required to be replaced or corrected without disclosing the former requirement for replacement or correction, and, when required, shall disclose the corrective action taken. [*Insert portion of labor rate attributable to profit.*]

(5)

(i) If the Contractor fails to proceed with reasonable promptness to perform required replacement or correction, and if the replacement or correction can be performed within the ceiling price (or the ceiling price as increased by the Government), the Government may—

(A) By contract or otherwise, perform the replacement or correction, charge to the Contractor any increased cost, or deduct such increased cost from any amounts paid or due under this contract; or

(B) Terminate this contract for cause.

(ii) Failure to agree to the amount of increased cost to be charged to the Contractor shall be a dispute under the Disputes clause of the contract.

(6) Notwithstanding paragraphs (a)(4) and (5) above, the Government may at any time require the Contractor to remedy by correction or replacement, without cost to the Government, any failure by the Contractor to comply with the requirements of this contract, if the failure is due to--

(i) Fraud, lack of good faith, or willful misconduct on the part of the Contractor's managerial personnel; or

(ii) The conduct of one or more of the Contractor's employees selected or retained by the Contractor after any of the Contractor's managerial personnel has reasonable grounds to believe that the employee is habitually careless or unqualified.
(7) This clause applies in the same manner and to the same extent to corrected or replacement materials or services as to materials and services originally delivered under this contract.
(8) The Contractor has no obligation or liability under this contract to correct or replace materials and services that at time of delivery do not meet contract requirements, except as provided in this clause or as may be otherwise specified in the contract.
(9) Unless otherwise specified in the contract, the Contractor's obligation to correct or replace Government-furnished property shall be governed by the clause pertaining to Government property.
(b) *Assignment*. The Contractor or its assignee may assign its rights to receive payment due as a result of performance of this contract to a bank, trust company, or other financing institution, including any Federal lending agency in accordance with the Assignment of Claims Act (31 U.S.C.3727). However, when a third party makes payment (*e.g.,* use of the Governmentwide commercial purchase card), the Contractor may not assign its rights to receive payment under this contract.
(c) *Changes*. Changes in the terms and conditions of this contract may be made only by written agreement of the parties.
(d) *Disputes*. This contract is subject to 41 U.S.C. chapter 71,Contract Disputes. Failure of the parties to this contract to reach agreement on any request for equitable adjustment, claim, appeal or action arising under or relating to this contract shall be a dispute to be resolved in accordance with the clause at FAR 52.233-1, Disputes, which is incorporated herein by reference. The Contractor shall proceed diligently with performance of this contract, pending final resolution of any dispute arising under the contract.
(e) *Definitions*. (1) The clause at FAR 52.202-1, Definitions, is incorporated herein by reference. As used in this clause—
(i) *Direct materials* means those materials that enter directly into the end product, or that are used or consumed directly in connection with the furnishing of the end product or service.
(ii) *Hourly rate* means the rate(s) prescribed in the contract for payment for labor that meets the labor category qualifications of a labor category specified in the contract that are—
(A) Performed by the contractor;
(B) Performed by the subcontractors; or
(C) Transferred between divisions, subsidiaries, or affiliates of the contractor under a common control.
(iii) *Materials* means—
(A) Direct materials, including supplies transferred between divisions, subsidiaries, or affiliates of the contractor under a common control;
(B) Subcontracts for supplies and incidental services for which there is not a labor category specified in the contract;
(C) Other direct costs (*e.g.*, incidental services for which there is not a labor category specified in the contract, travel, computer usage charges, etc.);
(D) The following subcontracts for services which are specifically excluded from the hourly rate: [*Insert any subcontracts for services to be excluded from the hourly rates prescribed in the schedule.*]; and
(E) Indirect costs specifically provided for in this clause.
(iv) *Subcontract* means any contract, as defined in FAR Subpart 2.1, entered into with a subcontractor to furnish supplies or services for performance of the prime contract or a

subcontract including transfers between divisions, subsidiaries, or affiliates of a contractor or subcontractor. It includes, but is not limited to, purchase orders, and changes and modifications to purchase orders.
(f) *Excusable delays*. The Contractor shall be liable for default unless nonperformance is caused by an occurrence beyond the reasonable control of the Contractor and without its fault or negligence such as, acts of God or the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, unusually severe weather, and delays of common carriers. The Contractor shall notify the Contracting Officer in writing as soon as it is reasonably possible after the commencement of any excusable delay, setting forth the full particulars in connection therewith, shall remedy such occurrence with all reasonable dispatch, and shall promptly give written notice to the Contracting Officer of the cessation of such occurrence.
(g) *Invoice*.
(1) The Contractor shall submit an original invoice and three copies (or electronic invoice, if authorized) to the address designated in the contract to receive invoices. An invoice must include --
(i) Name and address of the Contractor;
(ii) Invoice date and number;
(iii) Contract number, line item number and, if applicable, the order number;
(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract.
(x) Electronic funds transfer (EFT) banking information.
(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (*e.g.*, 52.232-33, Payment by Electronic Funds Transfer— System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management), or applicable agency procedures.
(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.
(2) Invoices will be handled in accordance with the Prompt Payment Act (31 U.S.C. 3903) and Office of Management and Budget (OMB) prompt payment regulations at 5 CFR part 1315.
(h) *Patent indemnity*. The Contractor shall indemnify the Government and its officers, employees and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark or copyright, arising out of the performance of this contract, provided the Contractor is reasonably notified of such claims and proceedings.
(i) Payments.
(1) *Work performed.* The Government will pay the Contractor as follows upon the submission of commercial invoices approved by the Contracting Officer:

(i) Hourly rate.
(A) The amounts shall be computed by multiplying the appropriate hourly rates prescribed in the contract by the number of direct labor hours performed. Fractional parts of an hour shall be payable on a prorated basis.
(B) The rates shall be paid for all labor performed on the contract that meets the labor qualifications specified in the contract. Labor hours incurred to perform tasks for which labor qualifications were specified in the contract will not be paid to the extent the work is performed by individuals that do not meet the qualifications specified in the contract, unless specifically authorized by the Contracting Officer.
(C) Invoices may be submitted once each month (or at more frequent intervals, if approved by the Contracting Officer) to the Contracting Officer or the authorized representative.
(D) When requested by the Contracting Officer or the authorized representative, the Contractor shall substantiate invoices (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment, individual daily job timecards, records that verify the employees meet the qualifications for the labor categories specified in the contract, or other substantiation specified in the contract.
(E) Unless the Schedule prescribes otherwise, the hourly rates in the Schedule shall not be varied by virtue of the Contractor having performed work on an overtime basis.
(1) If no overtime rates are provided in the Schedule and the Contracting Officer approves overtime work in advance, overtime rates shall be negotiated.
(2) Failure to agree upon these overtime rates shall be treated as a dispute under the Disputes clause of this contract.
(3) If the Schedule provided rates for overtime, the premium portion of those rates will be reimbursable only to the extent the overtime is approved by the Contracting Officer.
(ii) Materials.
(A) If the Contractor furnishes materials that meet the definition of a commercial item at FAR 2.101, the price to be paid for such materials shall not exceed the Contractor's established catalog or market price, adjusted to reflect the--
(1) Quantities being acquired; and
(2) Any modifications necessary because of contract requirements.
(B) Except as provided for in paragraph (i)(1)(ii)(A) and (D)(2) of this clause, the Government will reimburse the Contractor the actual cost of materials (less any rebates, refunds, or discounts received by the contractor that are identifiable to the contract) provided the Contractor—
(1) Has made payments for materials in accordance with the terms and conditions of the agreement or invoice; or
(2) Makes these payments within 30 days of the submission of the Contractor's payment request to the Government and such payment is in accordance with the terms and conditions of the agreement or invoice.
(C) To the extent able, the Contractor shall—
(1) Obtain materials at the most advantageous prices available with due regard to securing prompt delivery of satisfactory materials; and
(2) Give credit to the Government for cash and trade discounts, rebates, scrap, commissions, and other amounts that are identifiable to the contract.
(D) *Other Costs.* Unless listed below, other direct and indirect costs will not be reimbursed.
(1) Other direct Costs. The Government will reimburse the Contractor on the basis of actual cost for the following, provided such costs comply with the requirements in paragraph (i)(1)(ii)(B) of this clause: Travel
(2) Indirect Costs (Material handling, Subcontract Administration, etc.). The Government

will reimburse the Contractor for indirect costs on a pro-rata basis over the period of contract performance at the following fixed price: $0
(2) *Total cost.* It is estimated that the total cost to the Government for the performance of this contract shall not exceed the ceiling price set forth in the Schedule and the Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within such ceiling price. If at any time the Contractor has reason to believe that the hourly rate payments and material costs that will accrue in performing this contract in the next succeeding 30 days, if added to all other payments and costs previously accrued, will exceed 85 percent of the ceiling price in the Schedule, the Contractor shall notify the Contracting Officer giving a revised estimate of the total price to the Government for performing this contract with supporting reasons and documentation. If at any time during the performance of this contract, the Contractor has reason to believe that the total price to the Government for performing this contract will be substantially greater or less than the then stated ceiling price, the Contractor shall so notify the Contracting Officer, giving a revised estimate of the total price for performing this contract, with supporting reasons and documentation. If at any time during performance of this contract, the Government has reason to believe that the work to be required in performing this contract will be substantially greater or less than the stated ceiling price, the Contracting Officer will so advise the Contractor, giving the then revised estimate of the total amount of effort to be required under the contract.
(3) *Ceiling price.* The Government will not be obligated to pay the Contractor any amount in excess of the ceiling price in the Schedule, and the Contractor shall not be obligated to continue performance if to do so would exceed the ceiling price set forth in the Schedule, unless and until the Contracting Officer notifies the contractor in writing that the ceiling price has been increased and specifies in the notice a revised ceiling that shall constitute the ceiling price for performance under this contract. When and to the extent that the ceiling price set forth in the Schedule has been increased, any hours expended and material costs incurred by the Contractor in excess of the ceiling price before the increase shall be allowable to the same extent as if the hours expended and material costs had been incurred after the increase in the ceiling price.
(4) *Access to records.* At any time before final payment under this contract, the Contracting Officer (or authorized representative) will have access to the following (access shall be limited to the listing below unless otherwise agreed to by the Contractor and the Contracting Officer):
(i) Records that verify that the employees whose time has been included in any invoice met the qualifications for the labor categories specified in the contract.
(ii) For labor hours (including any subcontractor hours reimbursed at the hourly rate in the schedule), when timecards are required as substantiation for payment—
(A) The original timecards (paper-based or electronic);
(B) The Contractor's timekeeping procedures;
(C) Contractor records that show the distribution of labor between jobs or contracts; and
(D) Employees whose time has been included in any invoice for the purpose of verifying that these employees have worked the hours shown on the invoices.
(iii) For material and subcontract costs that are reimbursed on the basis of actual cost—
(A) Any invoices or subcontract agreements substantiating material costs; and
(B) Any documents supporting payment of those invoices.
(5) *Overpayments/Underpayments.* Each payment previously made shall be subject to reduction to the extent of amounts, on preceding invoices, that are found by the Contracting Officer not to have been properly payable and shall also be subject to reduction for overpayments or to increase for underpayments. The Contractor shall promptly pay any such reduction within 30 days unless the parties agree otherwise. The

Government within 30 days will pay any such increases, unless the parties agree otherwise. The Contractor's payment will be made by check. If the Contractor becomes aware of a duplicate invoice payment or that the Government has otherwise overpaid on an invoice payment, the Contractor shall—
(i) Remit the overpayment amount to the payment office cited in the contract along with a description of the overpayment including the—
(A) Circumstances of the overpayment (*e.g.,* duplicate payment, erroneous payment, liquidation errors, date(s) of overpayment);
(B) Affected contract number and delivery order number, if applicable;
(C) Affected line item or subline item, if applicable; and
(D) Contractor point of contact.
(ii) Provide a copy of the remittance and supporting documentation to the Contracting Officer.
(6)
(i) All amounts that become payable by the Contractor to the Government under this contract shall bear simple interest from the date due until paid unless paid within 30 days of becoming due. The interest rate shall be the interest rate established by the Secretary of the Treasury, as provided in 41 U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six month period as established by the Secretary until the amount is paid.
(ii) The Government may issue a demand for payment to the Contractor upon finding a debt is due under the contract.
(iii) Final Decisions. The Contracting Officer will issue a final decision as required by 33.211 if—
(A) The Contracting Officer and the Contractor are unable to reach agreement on the existence or amount of a debt in a timely manner;
(B) The Contractor fails to liquidate a debt previously demanded by the Contracting Officer within the timeline specified in the demand for payment unless the amounts were not repaid because the Contractor has requested an installment payment agreement; or
(C) The Contractor requests a deferment of collection on a debt previously demanded by the Contracting Officer (see FAR 32.60702).
(iv) If a demand for payment was previously issued for the debt, the demand for payment included in the final decision shall identify the same due date as the original demand for payment.
(v) Amounts shall be due at the earliest of the following dates:
(A) The date fixed under this contract.
(B) The date of the first written demand for payment, including any demand for payment resulting from a default termination.
(vi) The interest charge shall be computed for the actual number of calendar days involved beginning on the due date and ending on—
(A) The date on which the designated office receives payment from the Contractor;
(B) The date of issuance of a Government check to the Contractor from which an amount otherwise payable has been withheld as a credit against the contract debt; or
(C) The date on which an amount withheld and applied to the contract debt would otherwise have become payable to the Contractor.
(vii) The interest charge made under this clause may be reduced under the procedures prescribed in 32.608-2 of the Federal Acquisition Regulation in effect on the date of this contract.
(viii) Upon receipt and approval of the invoice designated by the Contractor as the "completion invoice" and supporting documentation, and upon compliance by the Contractor with all terms of this contract, any outstanding balances will be paid within 30

days unless the parties agree otherwise. The completion invoice, and supporting documentation, shall be submitted by the Contractor as promptly as practicable following completion of the work under this contract, but in no event later than 1 year (or such longer period as the Contracting Officer may approve in writing) from the date of completion.

(7) *Release of claims.* The Contractor, and each assignee under an assignment entered into under this contract and in effect at the time of final payment under this contract, shall execute and deliver, at the time of and as a condition precedent to final payment under this contract, a release discharging the Government, its officers, agents, and employees of and from all liabilities, obligations, and claims arising out of or under this contract, subject only to the following exceptions.

(i) Specified claims in stated amounts, or in estimated amounts if the amounts are not susceptible to exact statement by the Contractor.

(ii) Claims, together with reasonable incidental expenses, based upon the liabilities of the Contractor to third parties arising out of performing this contract, that are not known to the Contractor on the date of the execution of the release, and of which the Contractor gives notice in writing to the Contracting Officer not more than 6 years after the date of the release or the date of any notice to the Contractor that the Government is prepared to make final payment, whichever is earlier.

(iii) Claims for reimbursement of costs (other than expenses of the Contractor by reason of its indemnification of the Government against patent liability), including reasonable incidental expenses, incurred by the Contractor under the terms of this contract relating to patents.

(8) *Prompt payment.* The Government will make payment in accordance with the Prompt Payment Act (31 U.S.C 3903) and prompt payment regulations at 5 CFR part 1315.

(9) *Electronic Funds Transfer (EFT).* If the Government makes payment by EFT, see 52.212-5(b) for the appropriate EFT clause.

(10) *Discount.* In connection with any discount offered for early payment, time shall be computed from the date of the invoice. For the purpose of computing the discount earned, payment shall be considered to have been made on the date that appears on the payment check or the specified payment date if an electronic funds transfer payment is made.

(j) *Risk of loss*. Unless the contract specifically provides otherwise, risk of loss or damage to the supplies provided under this contract shall remain with the Contractor until, and shall pass to the Government upon:

(1) Delivery of the supplies to a carrier, if transportation is f.o.b. origin; or

(2) Delivery of the supplies to the Government at the destination specified in the contract, if transportation is f.o.b. destination.

(k) *Taxes*. The contract price includes all applicable Federal, State, and local taxes and duties.

(l) *Termination for the Government's convenience.* The Government reserves the right to terminate this contract, or any part hereof, for its sole convenience. In the event of such termination, the Contractor shall immediately stop all work hereunder and shall immediately cause any and all of its suppliers and subcontractors to cease work. Subject to the terms of this contract, the Contractor shall be paid an amount for direct labor hours (as defined in the Schedule of the contract) determined by multiplying the number of direct labor hours expended before the effective date of termination by the hourly rate(s) in the contract, less any hourly rate payments already made to the Contractor plus reasonable charges the Contractor can demonstrate to the satisfaction of the Government using its standard record keeping system that have resulted from the termination. The Contractor shall not be required to comply with the cost accounting standards or contract cost principles for this purpose. This paragraph does not give the Government any right

to audit the Contractor's records. The Contractor shall not be paid for any work performed or costs incurred that reasonably could have been avoided.
(m) *Termination for cause.* The Government may terminate this contract, or any part hereof, for cause in the event of any default by the Contractor, or if the Contractor fails to comply with any contract terms and conditions, or fails to provide the Government, upon written request, with adequate assurances of future performance. Subject to the terms of this contract, the Contractor shall be paid an amount computed under paragraph (i) Payments of this clause, but the "hourly rate" for labor hours expended in furnishing work not delivered to or accepted by the Government shall be reduced to exclude that portion of the rate attributable to profit. Unless otherwise specified in paragraph (a)(4) of this clause, the portion of the "hourly rate" attributable to profit shall be 10 percent. In the event of termination for cause, the Contractor shall be liable to the Government for any and all rights and remedies provided by law. If it is determined that the Government improperly terminated this contract for default, such termination shall be deemed a termination for convenience.
(n) *Title*. Unless specified elsewhere in this contract, title to items furnished under this contract shall pass to the Government upon acceptance, regardless of when or where the Government takes physical possession.
(o) *Warranty*. The Contractor warrants and implies that the items delivered hereunder are merchantable and fit for use for the particular purpose described in this contract.
(p) *Limitation of liability*. Except as otherwise provided by an express warranty, the Contractor will not be liable to the Government for consequential damages resulting from any defect or deficiencies in accepted items.
(q) *Other compliances*. The Contractor shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract.
(r) *Compliance with laws unique to Government contracts.* The Contractor agrees to comply with 31 U.S.C. 1352 relating to limitations on the use of appropriated funds to influence certain Federal contracts; 18 U.S.C. 431 relating to officials not to benefit; 40 U.S.C. chapter 37, Contract Work Hours and Safety Standards; 41 U.S.C. chapter 87, Kickbacks; 41 U.S.C. 4712 and 10 U.S.C. 2409 relating to whistleblower protections; 49 U.S.C. 40118, Fly American; and 41 U.S.C. chapter 21 relating to procurement integrity.
(s) *Order of precedence*. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:
(1) The schedule of supplies/services.
(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, and Unauthorized Obligations paragraphs of this clause.
(3) The clause at 52.212-5.
(4) Addenda to this solicitation or contract, including any license agreements for computer software.
(5) Solicitation provisions if this is a solicitation.
(6) Other paragraphs of this clause.
(7) The Standard Form 1449.
(8) Other documents, exhibits, and attachments.
(9) The specification.
(t) Reserved
(u) Unauthorized Obligations.
(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any End Use 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:
(i) Any such clause is unenforceable against the Government.
(ii) 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.
(iii) Any such clause is deemed to be stricken from the EULA, TOS, or similar legal instrument or agreement.
(2) Paragraph (u)(1) of this clause does not apply to indemnification by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.
(v) *Incorporation by reference*. 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** (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.]
_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).
_X__ (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's 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) (i) 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.
_X__ (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 (Aug 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 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) (i) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).
___ (ii) Alternate I (Feb 1999) of 52.222-26.
_X__ (29) (i) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).
___ (ii) Alternate I (July 2014) of 52.222-35.
_X__ (30) (i) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).
___ (ii) Alternate I (July 2014) of 52.222-36.
_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).
_X__ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 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) (i) 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).
_X__ (ii) Alternate I (Jan 2017) of 52.224-3.
___ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).
___ (47) (i) 52.225-3, Buy American--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 (June 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. 2302 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).
_X__ (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)).
_X__ (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).
_X__ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(13)).
___ (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.
___ (iii) Alternate II (Feb 2006) 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*.]
_X__ (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.).
_X__ (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).
_X__ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O.

13658).
_X__ (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 (Jan 2019) (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 (Oct 2018) (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 2019) (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 (Jan 2019) (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)

52.217-8 **Option to Extend Services** (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within __**30 days**___.

(End of clause)

52.217-9 **Option to Extend the Term of the Contract** (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within **30 days of contract expiration**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **45 days** before the task order expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
The total duration of this contract, including the exercise of any options under this clause, shall not exceed **28 months**.

(End of clause)

52.252-2 **Clauses Incorporated by Reference** (Feb 1998)
This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): https://acquisition.gov/

(End of clause)

52.252-4 **Alterations in Contract** (Apr 1984)

Portions of this contract are altered as follows: Use of the word "contract" is understood to mean "task order" whenever such application is appropriate.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses incorporated in full text

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:
[The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]
(a) Provisions.
_X___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.
__X__3052.203-70 Instructions for Contractor Disclosure of Violations.
____3052.204-70 Security Requirements for Unclassified Information Technology Resources.
__X__3052.204-71 Contractor Employee Access.
____Alternate I
__X__3052.205-70 Advertisement, Publicizing Awards, and Releases.
__X__3052.209-73 Limitation on Future Contracting.
__X__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.
__X__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.
__X__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.
__X__3052.247-72 F.o.B. Destination Only.

(End of clause)

3052.215-70 **Key Personnel or Facilities** (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.

(b) Before replacing any of the specified individuals or facilities, the contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The contractor shall not replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Contract are:

- *Program Manager*
- *DevSecOps Architect Lead*
- *UI/UX Design Lead*

(End of clause)

Security, Privacy, Local, Invoicing

SECURITY REQUIREMENTS (Security Clause 5)

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to sensitive but unclassified information, and that the Contractor will adhere to the following.

SUITABILITY DETERMINATION

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

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract as outlined in the DHS Form 11000-25, Contractor Fitness/Security Screening Request Form and the USCIS Continuation Page to the DHS Form 11000-25. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through OSI PSD.

To the extent the DHS Form 11000-25 and the USCIS Continuation Page to the DHS Form 11000-25 reveals that the Contractor will not require access to sensitive but unclassified information or access to USCIS IT systems, OSI PSD may determine that preliminary security screening and or a complete background investigation is not required for performance on this contract.

Completed packages must be submitted to OSI PSD for prospective Contractor employees no less than 30 days before the starting date of the contract or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor. The Contractor shall follow guidelines for package submission as set forth by OSI PSD. A complete package will include the following forms, in conjunction with security questionnaire submission of the SF-85P, "Security Questionnaire for Public Trust Positions" via e-QIP:

1. Additional Questions for Public Trust Positions – Branching
2. DHS Form 11000-6, "Conditional Access to Sensitive But UnclassifiedInformation Non-Disclosure Agreement"
3. FD Form 258, "Fingerprint Card" **(2 copies)**
4. Form DHS 11000-9, "Disclosure and Authorization Pertaining to ConsumerReports

Pursuant to the Fair Credit Reporting Act"

5. DHS Form 11000-25 "Contractor Fitness/Security Screening Request Form"
6. USCIS Continuation Page to DHS Form 11000-25
7. OF 306, Declaration for Federal Employment (approved use for FederalContract Employment)
8. Foreign National Relatives or Associates Statement

EMPLOYMENT ELIGIBILITY

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

Only U.S. citizens are eligible for employment on contracts requiring access to Department of Homeland Security (DHS) Information Technology (IT) systems or involvement in the development, operation, management, or maintenance of DHS IT systems, unless a waiver has been granted by the Director of USCIS, or designee, with the concurrence of both the DHS Chief Security Officer and the Chief Information Officer or their designees. In instances where non-IT requirements contained in the contract can be met by using Legal Permanent Residents, those requirements shall be clearly described.

CONTINUED ELIGIBILITY

If a prospective employee is found to be ineligible for access to USCIS facilities or information, the Contracting Officer's Representative (COR) will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

In accordance with USCIS policy, contractors are required to undergo a periodic reinvestigation every five years. Security documents will be submitted to OSI PSD within ten business days following notification of a contractor's reinvestigation requirement.

In support of the overall USCIS mission, Contractor employees are required to complete one-time or annual
DHS/USCIS mandatory trainings. The Contractor shall certify annually, but no later than December 31st each year, or prior to any accelerated deadlines designated by USCIS, that required trainings have been completed. The certification of the completion of the trainings by all contractors shall be provided to both the COR and Contracting Officer.

- **USCIS Security Awareness Training** (required within 30 days of entry on dutyfor new contractors, and annually thereafter)
- **USCIS Integrity Training** (Annually)
- **DHS Insider Threat Training** (Annually)
- **DHS Continuity of Operations Awareness Training** (one-time training for contractors identified as providing an essential service)
- **Unauthorized Disclosure Training** (one time training for contractors who require access to USCIS information regardless if performance occurs within USCIS facilities or at a company owned and operated facility)
- **USCIS Fire Prevention and Safety Training** (one-time training for contractors working within USCIS facilities; contractor companies may substitute their owntraining)
- **USCIS PKI Initiative Training** (if supervisor determines the need for a PKI certificate)
- **Computer Security Awareness Training** (if contractor requires access to USCIS IT

systems, training must be completed within 60 days of entry on duty for new contractors, and annually thereafter)

USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising sensitive but unclassified information and/or classified information.

Contract employees will report any adverse information concerning their personal conduct to OSI PSD. The report shall include the contractor's name along with the adverse information being reported. Required reportable adverse information includes, but is not limited to, criminal charges and or arrests, negative change in financial circumstances, and any additional information that requires admission on the SF-85P security questionnaire or on any security form listed above.

In accordance with Homeland Security Presidential Directive-12 (HSPD-12) http://www.dhs.gov/homeland-security-presidential-directive-12 contractor employees who require access to United States Citizenship and Immigration Services (USCIS) facilities and/or utilize USCIS Information Technology (IT) systems, must be issued and maintain a Personal Identity Verification (PIV) card throughout the period of performance on their contract. Government-owned contractor-operated facilities are considered USCIS facilities.

After the Office of Security & Integrity, Personnel Security Division has notified the Contracting Officer's Representative that a favorable entry on duty (EOD) determination has been rendered, contractor employees will need to obtain a PIV card.

For new EODs, contractor employees have [*10 business days unless a different number is inserted*] from their EOD date to comply with HSPD-12. For existing EODs, contractor employees have [*10 business days unless a different number of days is inserted*] from the date this clause is incorporated into the contract to comply with HSPD-12.

Contractor employees who do not have a PIV card must schedule an appointment to have one issued. To schedule an appointment:
http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/PIV/default.aspx

Contractors who are unable to access the hyperlink above shall contact the Contracting Officer's Representative (COR) for assistance.
Contractor employees who do not have a PIV card will need to be escorted at all times by a government employee while at a USCIS facility and will not be allowed access to USCIS IT systems.

A contractor employee required to have a PIV card shall:

- Properly display the PIV card above the waist and below the neck with the photo facing outso that it is visible at all times while in a USCIS facility
- Keep their PIV card current
- Properly store the PIV card while not in use to prevent against loss or theft http://ecn.uscis.dhs.gov/team/mgmt/Offices/osi/FSD/HSPD12/SIR/default.aspx

OSI PSD must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS issued identification cards and HSPD-12 card, or those of

terminated employees to the COR. If an identification card or HSPD-12 card is not available to be returned, a report must be submitted to the COR, referencing the card number, name of individual to whom issued, the last known location and disposition of the card.

SECURITY MANAGEMENT

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

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

The Contractor shall be responsible for all damage or injuries resulting from the acts or omissions of their employees and/or any subcontractor(s) and their employees to include financial responsibility.

(End of clause)

SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT RESPONSE

Privacy Clause Requirements

GENERAL

U.S. Citizenship and Immigration Services (USCIS) has determined that performance of this contract requires the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), to access information that meet the definition of Personally Identifiable Information (PII) and/or Sensitive PII, set forth below. Accordingly, the Contractor will adhere to the following:

(a) Definitions.

"Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, acquisition, and/or access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Sensitive PII is a subset of PII which requires additional precautions to prevent exposure or compromise.

Examples of PII include: 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), Internet protocol addresses, biometric identifiers (e.g., fingerprints), 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 Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:
(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but it is not sensitive.

(b) Systems Access. Work to be performed under this contract requires the handling of PII and/or Sensitive PII. The contractor shall provide USCIS access to GFE, and information regarding systems the contractor operates on behalf of USCIS under this contract, when requested by USCIS, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with USCIS in assuring compliance with such requirements. USCIS access shall include independent validation testing of controls, system penetration testing by USCIS, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security. In performing its duties related to management, operation, and/or access of systems, owned and or operated by USCIS or provided to the contractor, containing PII and/or Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in Department of Homeland Security (DHS) Sensitive System Publication 4300A or any superseding publication, and Rules of Behavior.

In addition, use of contractor-owned laptops or other mobile media storage devices to include external hard drives and memory sticks to process or store PII/Sensitive PII is prohibited under this contract unless the Contracting Officer (CO) in coordination with the USCIS Chief Information Security Officer (CISO) approves. If approval is granted the contractor shall provide written certification that the following minimum requirements are met:
(1) Laptops shall employ full disk encryption using NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
(2) Mobile computing devices use anti-viral software and a host-based firewall mechanism;
(3) When no longer needed, all mobile media and laptop hard drives shall be processed (i.e., sanitized, degaussed, and/or destroyed) in accordance with DHS security requirements set forth in DHS Sensitive System Publication 4300A. The USCIS reserves the right to audit random media for effectiveness of sanitization or degaussing. The contractor shall provide the requested equipment to USCIS no later than 15 days from the date of the request.
(4) The contractor shall maintain an accurate inventory of devices used in the performance of this contract and be made available upon request from USCIS;
(5) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished

in accordance with DHS Sensitive System Publication 4300A, which the Contracting Officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure PII/Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When PII/Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the PII/Sensitive PII irretrievable.

The contractor shall only use PII/Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer. At expiration or termination of this contract, the contractor shall turn over all PII/Sensitive PII obtained under the contract that is in its possession to USCIS.

(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of PII/Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer , the Contracting Officer's Representative (COR), and the USCIS Service Desk and complete an Incident Report with the Service Desk Representative. The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. Email notification shall be used to document all telephonic notifications.

(f) Personally Identifiable Information Notification Requirement. The contractor will have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by USCIS. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of USCIS, based upon a risk-based analysis conducted by USCIS in accordance with DHS Privacy incident Handling Guidance and USCIS Privacy Incident Standard Operating Procedures. Notification shall not proceed unless USCIS has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to USCIS analysis of the breach and the terms of its instructions to the contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by USCIS. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information.

The contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the contractor or employee actions, but the contractor is an unintentional recipient of privacy data. Actions may include allowing USCIS incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile

devices (BlackBerry, Smart Phone, iPad, USB thumbdrives, etc…). In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the Contracting Officer and at no cost to USCIS, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should USCIS elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing USCIS for those expenses. To ensure continuity with existing government identity protection and credit monitoring efforts, the contractor shall use the identity protection service provider specified by USCIS.

(g) Privacy Training Requirement. The performance of this contract has been determined to have the potential of allowing access, by Offeror employees, to Personally Identifiable Information (PII) and/or Sensitive PII, which is protected under the Privacy Act of 1974, as amended at 5 USC §552a. The Offeror is responsible for ensuring all employees who have access to information protected under the Privacy Act complete annual mandatory USCIS Privacy Awareness Training. New Offeror employees shall complete PII training within 30 days of entry on duty. The Offeror shall use the USCIS provided web-based Privacy Training which is available through the USCIS Performance and Learning Management System (PALMS) training system https://etms.uscis.dhs.gov to satisfy this requirement. Any employees who do not have access to the online PALMS training system shall take Privacy training via a USCIS provided DVD. The Offeror shall certify as soon as this training is completed by its employees and annually thereafter on September 30th. The certification of the completion of the training by all employees shall be provided to both the COR and CO; within 60 days of contract award, within 45 days of new employee accession and no later than September 30th for the annual recertification.

(h) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

(i) Ability to Restrict Access to Information. USCIS reserves the right and prerogative to deny and/or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct or whom USCIS determines to present a risk of compromising Personally Identifiable Information (PII), Sensitive PII (SPII), Sensitive But Unclassified (SBU) information and/or classified information.

(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)

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)

SECTION 508 REQUIREMENTS

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

1. All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT or that contain ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Apps. A, C & D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards.

   Item that contains Information and Communications Technology (ICT): Accounts Public
   Applicable Exception: N/A **Authorization #:** N/A
   Applicable Functional Performance Criteria: All functional performance criteria apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.
   Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications; Software infrastructure): All WCAG Level AA Success Criteria Apply except 2.4.1 Bypass Blocks, 2.4.5 Multiple Ways, 3.2.3 Consistent Navigation, 3.2.4 Consistent Identification, 502 Interoperability with Assistive Technology, 503 Application
   Applicable 508 requirements for hardware features and components (including Servers): All requirements apply
   Applicable support services and documentation: All requirements apply

2. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

3. When providing maintenance upgrades, substitutions, and replacements to ICT, the contractor shall not reduce the original ICT's level of Section 508 conformance prior to upgrade, substitution or replacement. The agency reserves the right to request an Accessibility Conformance Report (ACR) for proposed substitutions and replacements prior to acceptance. The ACR should be created using the on the Voluntary Product Accessibility Template Version 2.1 or later. The template can be located at https://www.itic.org/policy/accessibility/vpat

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.

5. Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office

of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017.

6. Where ICT conforming to one or more requirements in the Revised 508 Standards is not commercially available, the agency shall procure the ICT that best meets the Revised 508 Standards consistent with the agency's business needs, in accordance with 36 CFR E202.7. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated January 29, 2016 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated January 11, 2017 and 36 CFR E202.6.

POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

(a) The Government intends to post the contract (or order) resulting from this solicitation to a public FOIA reading room.
(b) Within 30 days of award, the Contractor shall submit a redacted copy of the executed contract (or order) (including all attachments) suitable for public posting under the provisions of the Freedom of Information Act (FOIA). The Contractor shall submit the documents to the USCIS FOIA Office by email at foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the contracting officer.
(c) The USCIS FOIA Office will notify the contractor of any disagreements with the Contractor's redactions before public posting of the contract or order in a public FOIA reading room.

EXPECTATION OF CONTRACTOR PERSONNEL

The government expects competent, productive, qualified IT professionals to be assigned to the Task Order. The Contracting Officer may, by written notice to the contractor, require the contractor to remove any employee that is not found to be competent, productive, or qualified IT professional.

PERFORMANCE REPORTING

The Government intends to record and maintain contractor performance information for this task order in accordance with FAR Subpart 42.15. The contractor is encouraged to enroll at www.cpars.gov so it can participate in this process.

FINAL PAYMENT

As a condition precedent to final payment, a release discharging the Government, its officers, agents and employees of and from all liabilities, obligations, and claims arising out of or under this contract shall be completed. A release of claims will be forwarded to the contractor at the end of each performance period for contractor completion as soon thereafter as practicable.

AUTHORIZATION TO PROCEED (ATP)

(a) Performance of the work requires unescorted access to Government facilities and/or automated systems, and/or access to sensitive information. Security requirements in Part II of this Solicitation (70SBUR19R00000057) apply.
(b) The Contractor is responsible for submitting packages for employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A Government decision not to grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such, shall not excuse the Contractor from performance of its obligations under this contract (or task order).
(c) The Contractor may submit background investigation packages immediately following contract (or task order) award.
(d) This contract (or task order) does not provide for direct payment to the Contractor for EOD

efforts. Work for which direct payment is not provided is a subsidiary obligation of the Contractor.
(e) The Government intends for each ATP to be issued within 60 days after contract (or task order) award. The Contracting Officer will issue ATPs individually per CLIN once it has been determined there are a sufficient number of contractors who have received their EOD to perform development prescribed under a CLIN. At a minimum, all three (3) key personnel must receive their EOD before an ATP can be issued. The PM will have discretion as to whether sufficient Contract personnel have received their EOD before issuing an ATP. Generally speaking CLINS associated with Agile teams must reach 75% EOD staffing or higher before the Government can issue an ATP. Once a CLIN approaches that threshold or higher the PM will advise the Contracting Officer that there are a sufficient number of EODs to issue an ATP. This notice will then be given to the contractor at least one day before performance is to begin.
(f) The Government intends for full performance to begin **90** days after contract (or task order) award.

INVOICING INSTRUCTIONS

(a) A proper invoice must include the following items (except for interim payments on cost reimbursement contracts for services):

(i) Name and address of the contractor.

(ii) Invoice date and invoice number. (Contractors should to date invoices as close as possible to the date of mailing or transmission.)

(iii) Contract number or other authorization for supplies delivered or services performed (including order number and line item number).

(iv) Description, quantity, unit of measure, unit price, and extended price of supplies delivered or services performed.

(v) Shipping and payment terms (*e.g.*, shipment number and date of shipment, discount for prompt payment terms). Bill of lading number and weight of shipment will be shown for shipments on Government bills of lading.

(vi) Name and address of contractor official to whom payment is to be sent (must be the same as that in the contract or in a proper notice of assignment).

(vii) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

(viii) Taxpayer Identification Number (TIN). The contractor must include its TIN on the invoice only if required by agency procedures. (See 4.9 TIN requirements.)

(ix) Electronic funds transfer (EFT) banking information.

(A) The contractor must include EFT banking information on the invoice only if required by agency procedures.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the contractor must have submitted correct EFT banking information in accordance with the applicable solicitation provision (*e.g.,* 52.232-38, Submission of Electronic Funds Transfer-System for Award Management, or 52.232-34, Payment by Electronic Funds Transfer-Other Than System for Award Management), or applicable agency procedures.

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

(x) Any other information or documentation required by the contract (*e.g.*, evidence of shipment).

(b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.

(c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500KB.

(d) If a paper invoice is submitted, mail the invoice to:

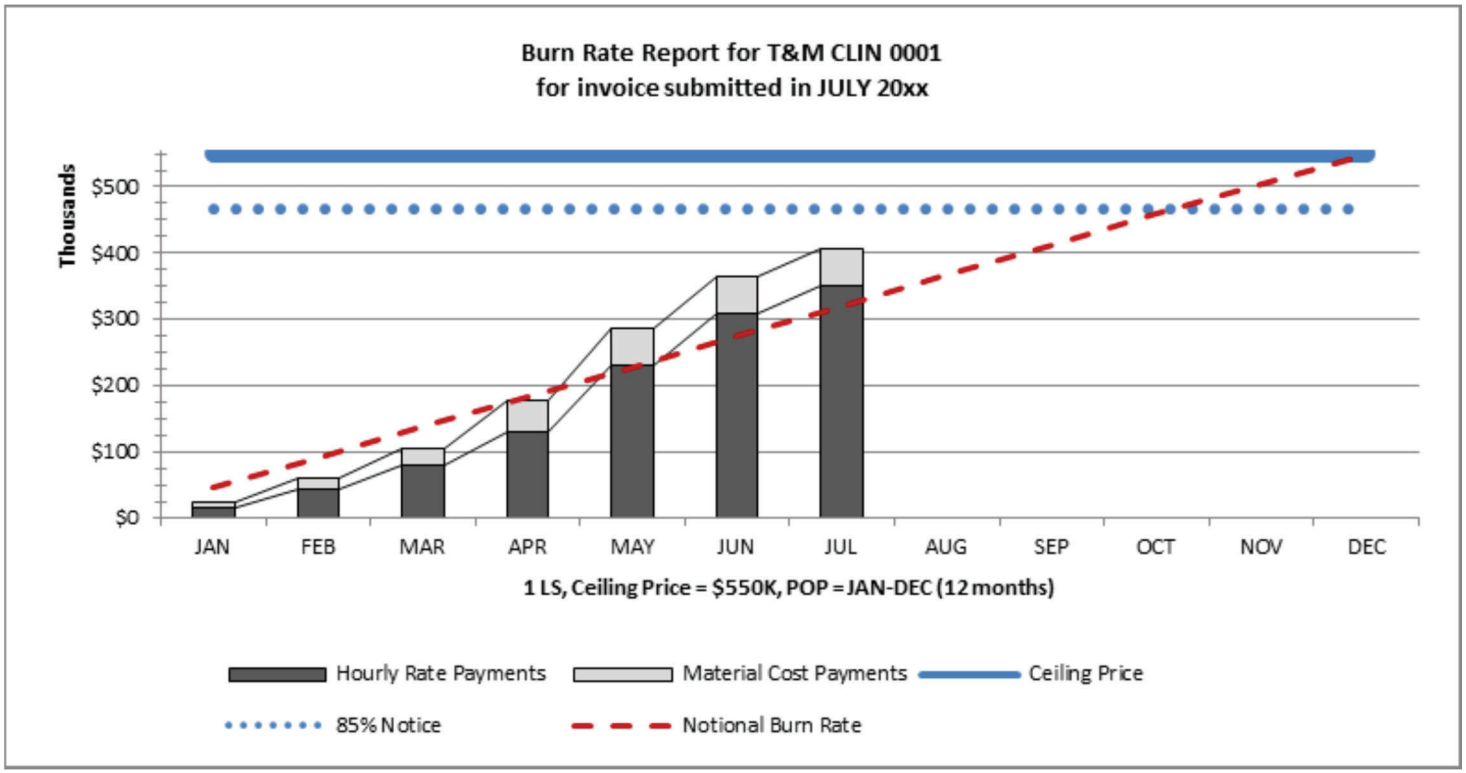
USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

(e) Invoices including T&M CLINs shall also contain a breakdown to include fully burdened labor rates, hours, and total price for each employee by CLIN or subCLIN to ensure invoices can be approved in a timely fashion. Delayed costs, including travel receipts and subcontract labor, shall be clearly identified as to the period in which the costs were incurred.

BURN RATE CHART AND TABLE DELIVERABLES

(1) The Contractor shall submit a chart and table, in the Contractor's format as approved by the contracting officer, showing its projected and actual burn rates for each time-and-materials (T&M) CLIN as supporting documentation for each invoice or voucher it submits to the Government for payment.

(2) The chart shall display the current period of performance, the ceiling price, and the cumulative amounts for hourly rate charges and materials charges for the instant and all previous invoices or vouchers submitted during the current period of performance. A notional sample is provided below for the convenience of the Contractor—



(3) The table shall include all the data used to develop the chart, and may include additional data that might be helpful in the Government's understanding of the Contractor's progress and experience under the contract or order.

(4) Nothing in this section relieves the Contractor of its responsibility to give timely and proper notice to the contracting officer of the possibility of exceeding the ceiling price. The chart and table called for by this section shall not serve as that notice.

EMPLOYMENT ELIGIBILITY VERIFICATION

In accordance with FAR 52.222-54, the contractor is required to enroll as a Federal Contractor in the E-Verify program within 30 calendar days of contract award. Once enrolled, the contractor is required to use E-Verify to electronically verify employment authorization of: (1) all new employees hired during the contract term; and (2) all employees performing work in the United States on the contract. Some exemptions may apply, please see guidance at www.uscis.gov/e-verify/federal-contractors on who is to be verified.

The contractor shall provide assertion of its enrollment in E-Verify and use of the system within 30 days of contract award to include any applicable employee exemptions to the Contracting Officer. If these assertions are not received or it cannot be completed, please provide the plan to ensure compliance with the Employment Eligibility Verification FAR Clause. The assertion shall be from the prime contractor and each subcontractor.

Part III – Documents, Exhibits, or Attachments

GOVERNMENT-FURNISHED PROPERTY (GFP)

(a) Upon the Contractor's request that a Contractor employee be granted access to a Government automated system and the Government's approval of the request, the Government may issue the following equipment for this task order:

Description	Quantity	Date/Event Indicate when the GFP will be furnished	Date/Event Indicate when the GFP will be returned
MacBook laptop Computers	33	Upon authorized Entry on Duty (EOD)	Upon Task Order completion or contractor employee departures
Windows Laptop Computers	14	Upon authorized Entry on Duty (EOD)	Upon Task Order completion or contractor employee departures
iPhones	10	Upon authorized Entry on Duty (EOD)	Upon Task Order completion or contractor employee departures

(b) The Contractor is responsible for all costs related to making this equipment available for use, such as payment of all transportation costs. The Contractor bears full responsibility for any and all loss of this equipment, whether accidental or purposeful, at full replacement value.

(c) This equipment will be provided on a rent-free basis for performance under this contract (or task order). It shall not be used for any non-contract or non-governmental purpose. The Contractor shall ensure the return of the equipment immediately upon the demand of the Contracting Officer or the end of contract (or task order) performance.

(d) A Contractor request may be for a subcontractor employee. If so, the Contractor retains all the responsibilities of this clause for equipment issued to that employee.

Statement of Work
Accounts Public DevSecOps Services (ACCTSPUB)

1. OVERVIEW

Accounts Public (ACCTSPUB) will consist of teams to provide development, security and operations (DevSecOps) services to support U.S. Citizenship and Immigration Services (USCIS) Information Technology (IT) system delivery. The teams will be operating and modernizing complex, large-scale Identity Management systems for public facing websites and IT systems in the cloud using DevSecOps delivery, open source technologies, and agile project management practices.

2. SCOPE

USCIS will manage system roadmaps, project plans, and product and release backlogs that will be the basis for the contractor's work and the contractor will support as needed. A USCIS Product Owner will specify high-level requirements to this and other contractors' agile teams. As in typical agile processes, USCIS Subject Matter Experts (SMEs) will work together with the contractor team to define user stories and establish acceptance criteria. These acceptance criteria will specify expected functionality for a user story, as well as any non-functional requirements that must be met in the development of the story. The USCIS Product Owner(s), supported by SMEs and business analysts, will determine whether or not acceptance criteria have been satisfied. USCIS may adopt various agile processes such as, but not limited to, Extreme Programming (XP), SCRUM, Kanban, and Lean Software Development, and the contractor will be expected to adapt its processes to these approaches.

Critical elements of the ACCTSPUB team will be:

- High productivity
- High quality work
- High level of initiative and ownership
- Collaboration and cooperation with other USCIS teams and participants
- Technical skills and expertise as necessary
- Estimation and planning skills
- Innovation and creativity in problem solving

The contractor shall adopt evolving USCIS design and coding standards in the course of their application development. The contractor shall provide technical methods, techniques, and concepts that are innovative, practical, cost-effective, and conducive to agile application development. The contractor shall develop IT capabilities based on requirements that are evolving and emerge as the business climate shifts.

ACCTSPUB developers will be required to develop high quality code and are responsible for any technical debt that is incurred as a result of their development activities. ACCTSPUB developers shall intelligently balance core productivity with technical debt, and should never tradeoff quality in favor of productivity. Technical debt should be addressed as it occurs and should not become so overwhelming that it must be addressed using an entire or several entire sprints.

Services in support of ACCTSPUB shall be provided by experts with demonstrated experience using

USCIS specified tools and technologies as described in section *2.1 Technical Landscape*. DevSecOps involves some degree of analysis, requirements collection, design, development, test, platform engineering, and production operations in addition to the support functions of configuration management, planning, and project management. In addition, DevSecOps should be considered to be "infrastructure as code" with the mindset and practice of automating through code everything possible. The specific tasks applicable under this contract are detailed in section *4 Tasks.* Delivery and operation will follow agile and DevSecOps industry best practices.

2.1 Technical Landscape

All USCIS requirements, epics/stories, source code and tests are stored in the agency's Enterprise Confluence, JIRA, and Enterprise Git repository, which the vendor shall use. Also, the artifacts in these repositories are shared between different vendors and projects where appropriate.

The contractor shall use USCIS enclaves in the AWS public cloud, and/or other cloud environment specified by the government, for development, testing, and production. The current cloud environment is AWS; however the Government may change to another Cloud Service Provider sometime in the future. The build pipeline will also include USCIS standard tools for code standards, test coverage, security testing, and Section 508 compliance.

DevSecOps

One of USCIS's goals is to use platforms and tools that are familiar to a broad range of developers; this has influenced our selection of open source products and frameworks. USCIS is currently using containerized micro-services, and AWS FedRAMP offerings. The contractor is expected to support the development of and integration with software Application Programming Interfaces (APIs). In addition the contractor will be required to design and author code that aligns to the overarching USCIS micro-services enterprise architecture. The contractor shall provide expertise in this arena.

The contractor shall integrate security and code quality scanning tools into the CD/CI pipeline. The contractor shall remediate the results of code quality and security scans in compliance with USCIS Quality Assurance and Information Security Division policies.

User Authentication and Identity Proofing

Contractors shall have a strong understanding of Identity and Credential management policies and technologies as defined in NIST SP 800-63 Digital Identity Guidelines. Contractors shall be capable of building and operating solutions consistent with the normative sections of NIST SP 800-63-3, SP 800-63A, SP 800-63B, and SP 800-63C .Contractors will be expected to support NIST SP 800-63 best practices in combination with USCIS specific digital identity business requirements. Contractors will assist in documenting these combined requirements in Agile user stories. User stories will drive the development team work. In addition to supporting the existing NIST best practices around digital identities, the contractor shall be adaptive to the continually evolving marketplace around digital identity. This may include researching and prototyping new marketplace capabilities.

Enrollment and Identity Proofing

Contractors shall have both policy and technical experience with the process of developing and supporting service that support remote identity proofing. Remote identity proofing shall be based on the NIST best practices for Identity Assurance Level (IAL) 1 and 2.

Authentication and Lifecycle Management

Contractors shall have both policy and technical experience to build and maintain a secure services capable of issuing the enrolled users, authenticators compliant with NIST best practices for Authenticator Assurance Level (AAL) 1, 2, and 3.

Federation and Assertions

Contractors shall have both policy and technical experience to build and maintain a secure services capable of federating. Federation shall be based on the NIST best practices for Federation Assurance Level (FAL) 1, 2, and 3.

Contractors shall be familiar with and capable of supporting solutions which implement the following Identity Protocols:

- OAuth 2.0 authorization framework
- OpenID Connect (OIDC)
- Security Assertion Markup Language (SAML)

USCIS Technical Stack

This task order will use the USCIS standard platform and tools. This platform will evolve over time to continue to fit the needs of USCIS, and the contractor is expected to support an ever evolving tool stack. The current platform is described in the table below:

Table 1: Current Tool Suite and Platforms

Name	Function
Apache	HTTP Server
Apigee	Lifecycle API management platform using Apigee Edge
AWS Cloud	Public cloud platform. USCIS currently uses EC2, ECS, EMR, S3, ECR, RDS, CloudFormation, Lambda, SES and a number of other AWS services
Amazon CloudWatch	Cloud monitoring services
Amazon KMS	A managed service that can be used to create and control the encryption keys used to encrypt data.
Amazon Rekognition	Facial analysis and facial recognition on images
BouncyCastle (FIPS)	Crytography API
Brakeman	Code analysis tool which checks Ruby on Rails applications for security vulnerabilities

Name	Function
CentOS	Enterprise class UNIX distribution
Chef	Configuration Management
DeQue FireEyes	508 Development Test tool
Docker	Containerization
Fortify	Static code scanning tool
Git / Enterprise GitHub	Distributed version control
Google Cloud Vision	Image analysis tools
Google ML Kit	Google Machine Learning SDK
Java	Programming Language
JavaScript	Programming Language
Jenkins	Continuous integration server
Jira	Agile lifecycle management tool
JUnit	Java Unit testing library
JSON	JavaScript Object Notation
Kafka	Data streaming platform
Kotlin	Programming Language
Microsoft Cognitive Services	Microsoft Azure AI platform
mySQL	OpenSource Relational Database
New Relic	Application and Infrastructure Monitoring
OpenShift	Open source container application platform
OpenSSL	Open source secure communication software library
PKI	Public key infrastructure
PostgreSQL	OpenSource Relational Database
Python	Programming Language
RCov	Test coverage tool
Redis	In-memory data structure store
RSpec	Domain Specific Language' (DSL) testing tool
Ruby	Programming Language
Ruby on RAILS	Web application framework
Service Now	Help desk ticketing system
SideKiq	Reads jobs from Redis queue, sends email and sms
SonarQube	Code quality inspection service
Splunk	Logs and Analysis
Spring Framework	Application Framework
Swagger	Open-source software framework for RESTful web services
Swift	Programming Language
TOTP	Time-Based One-Time Password
Twilio	Cloud communications platform for SMS, Voice & Messaging

Name	Function
Twistlock	Cybersecurity platform for hosts, containers, and images
Ubuntu	Unix distribution Operating System

2.2 Technical Support Tiers

The contractor will be required to provide Tier-II and Tier-III support as described in Section 4.7. Below are the USCIS definitions of each Tier.

Tier-I support is a basic level of customer support initiated by the public, private sector employers, and Government agencies other than USCIS. The customer representative providing Tier-I support is a generalist with a broad understanding of the product and may not understand the inner workings. They identify the customer's needs and provide tips on how to manage a problem. Tier-I solutions are in a frequently asked questions (FAQ) template or a knowledge base. The government will use a knowledge base to respond to a majority of customer calls. When a Tier-I support provider is not able to resolve the issue, they classify the problem, issue a tracking ticket to the customer and pass it on to the appropriate Tier-II contractor employee.

Tier-II technicians tend to have a specialization and will determine which specialization best matches the customer's needs before helping them. If their technical specialization is one that can help the customer, the technician then determines whether this problem is a new issue or an existing one. Advanced diagnostic tools may be used and data analysis performed at this point. If the issue is an existing one, the Tier-II contractor technician ascertains if there is a solution or a workaround in the contractor database. If there is such a solution, the customer is told how to fix their problem. However, in some cases there might be no solution as the problem is an open bug. In that case, the Tier-II contractor employee adds an entry to the bug list. Then, depending on the number of instances where customers are experiencing the same problem, the help desk could ask the developers to fix the bug. If a customer experiences a new issue, further analysis has to be performed to see if it can be dealt with. The help desk employee then explains to the customer how to fix their issue. If the Tier II technician cannot fix the problem, the problem goes to Tier-III.

Tier-III requires a contractor employee with specialized skills to deal with complex issues above the skill level of Tier-II contractor employees. To solve the problem, the teams must collect as much data as possible of the production environment and end-user feedback.

3 TEAMS

The ACCTSPUB contractor shall provide DevSecOps teams to perform the tasks as described, with expert level ability in the technologies stated in section *2.1 Technical Landscape.*

The team structure shall adhere to the following requirements:

- **One (1) Program Management Team** –Three (3) staff members, including a Program Manager, a DevSecOps Architect and a User Interface (UI)/User Experience (UX) who will work with the DevSecOps teams to deliver the required services. All members of the Program Management team will be key personnel on the contract.

- **One (1) DevSecOps Team** – One (1) eight (8) person team that includes a certified Scrum Master/Agile Lead, a Business Analyst, a Database Specialist, and a mix of developers and full stack Cloud Engineers that are also available to provide operations support when necessary and during any system outages. A full stack engineer shall have the ability to perform as a developer, operations, and security engineer in USCIS cloud environments. At least one (1) of developers shall also have the capacity to act as a Quality Assurance tester in a capacity secondary to their development role.

- **Two (2) DevSecOps Teams** – Two (2) eight (8) person teams that each include a Business Analyst, a Database Specialist , Quality Assurance tester and a mix of developers and full stack Cloud Engineers that are also available to provide operations support when necessary and during any system outages. A full stack engineer shall have the ability to perform as a developer, operations, and security engineer in USCIS cloud environments. At least one (1) of developers on each team shall also have the capacity to act as a Quality Assurance tester in a capacity secondary to their development role.

- **One (1) Optional Administrative Support Team** – To include four (4) staff members, including a Technical Writer, a Graphics Specialist and two (2) Business analysts.

- **One (1) Optional Mobile App Client Development Team *** - One (1) eight (8) person team that includes a Business Analyst, a Database Specialist, and a mix of developers and full stack Cloud Engineers that are also available to provide operations support when necessary and during any system outages. A full stack engineer shall have the ability to perform as a mobile app developer, operations, and security engineer in USCIS cloud environments.

- **One (1) Optional DevSecOps Team** – One (1) eight (8) person team that includes a Business Analyst, a Database Specialist, and a mix of developers and full stack Cloud Engineers that are also available to provide operations support when necessary and during any system outages. A full stack engineer shall have the ability to perform as a developer, operations, and security engineer in USCIS cloud environments.

Team structure can be adjusted to fit project specific needs, but only when approved by the Government.

The contractor shall have all personnel as full time. Part-time personnel are not permitted. Each team is not required to have the exact same mix of labor categories. The contractor shall determine the labor mix for each team to provide the best overall solution to the government.

The contractor shall use a test driven development (TDD) approach. The contractor's work shall conform to the architecture and design provided by USCIS and the agile processes set up by USCIS but managed by the contractor teams. The teams must have all of the skills of a full stack engineer necessary to perform the tasks indicated in section *4 Tasks*. It is important that the team as a whole have the skills necessary for development, operations, security, and test – but that does not mean that specific team members must be designated as testers, coders, etc. Most of the team members should have more than one skill.

The contractor must provide a DHS OAST Trusted Tester certified to current test standards for each team of one or more developers that creates Information and Communications Technology (ICT), or

content to be hosted on ICT, within 90 days of award. To clarify, there shall be one certified DHS OAST Trusted Tester for every two (2) DevSecOps teams, in accordance with Section 508 compliance (see Attachment 5). The trusted tester duty is considered an ancillary role for the team member who is provided to meet this requirement. When standards change and re-certification is required by DHS OAST, then the Contractor must ensure that all Trusted Testers re-certify within 90 days of training availability. The Contractor must provide a quarterly report that lists the contract name, number, and COR with each Trusted Tester's name, certification level, certification date, certification number, E-mail address, phone number, and supported projects to the COR and USCIS Section 508 Coordinator. This report must be provided within 10 working days of any change in the Trusted Tester population. The DHS Office of Accessible Systems and Technologies (OAST) administers the certification training and test. You can find their site here: http://dhsconnect.dhs.gov/org/comp/mgmt/cio/oast/Pages/default.aspx

4 TASKS

Each team shall work effectively within itself, conduct retrospectives to improve processes/performance and collaborate/coordinate with the Government, as well as with other contractor teams working for the government, to achieve the Government's needs.

The contractor shall prioritize the development of the automation Continuous Integration / Continuous Delivery (CI/CD) pipeline and the sustainment of secure (infrastructure or application) code utilizing industry and government security requirements and best practices. Additionally, the contractor shall automate all forms of testing and evaluation including quality assurance and compliancy where possible. The contractor shall be transparent and resolve any flaws discovered during all stages of development and sustainment.

The required tasks are identified in the following sections.

4.1 Development, Operations, and Security

- The Government will oversee the architecture and design of the IT capabilities, the agile methodologies to be used, product planning, and the flow of requirements; the contractor shall be responsible for developing high-quality IT capabilities working within those architectures and processes to meet the business requirements.
- The contractor shall be responsible for the teams that perform the full suite of DevSecOps tasks using agile methodologies, including participating in creating user stories for both business functionality and technical requirements and defining acceptance criteria; estimating the size of stories; designing solutions; developing code and automated tests; creating deployment scripts; managing code in production; managing any database solutions. The contractor will test its product and ensure its quality; and will deploy its code. The required deliverable is functional deployable code that meets the standards set forth in section *7 Deliverables*.
- The contractor shall perform software DevSecOps services in AWS Cloud environment, or other environments as specified by the Government. The contractor shall perform complete software development lifecycle and will have total responsibility for development, operations, security, and testing each set of capabilities in all applicable environments to release to end-users. The contractor

shall use a CI/CD approach and is expected to adopt cutting edge best practices for IT delivery.

- The contractor shall create the full suite of DevSecOps user stories necessary for both business functionality and technical requirements, including defining acceptance criteria; estimating the size of stories; designing solutions; developing code and automated tests; creating deployment scripts; managing code in production; and all data management across the environments. The contractor will deploy, test and remediate issues to ensure quality for end-user acceptance.

4.2 Documentation

- The contractor shall assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story.
- The contractor shall document system design and procedures in the USCIS designated repositories used for System Design Document (SDD) concurrent with development activities, including any other necessary DHS System Engineering Lifecycle documents such as Interface Control Agreements (ICA). In general, USCIS prefers relatively lightweight but effective and usable documentation.
- The contractor shall author Knowledge Base articles as needed to support code that has been developed. The articles will serve as reference material for by federal employees and contractors in support of Tier I inquiries.
- The contractor may be asked to assist in documenting an ACCTPUB Practice Statement. A practice statement is a formal statement of the practices followed by the parties to an authentication process (e.g., CSP or verifier). It describes the parties' policies and practices.

4.3 Design

- The contractor shall participate in the design of technical solutions to meet the business need, working within standards defined by USCIS and subject to review by the agency.
- The contractor will be responsible for designing and implementing user interfaces and for working with users to maximize the usability of the system. Design shall be done in conformance with USCIS design standards and in collaboration with USCIS. This includes working with prototypes, wireframes, etc., to ensure end-users interactions and to facilitate capturing end-users needs.

4.4 Test and Integration

- The contractor shall be responsible for creating test cases and automated test scripts to support test automation activities. Automated tests are considered an important deliverable for this task order.
- The contractor's code shall meet the functional and non-functional requirements, and the automated and manual tests performed shall verify that it does so. Test efficacy shall be confirmed by USCIS OIT Independent Validation & Verification (IV&V) personnel to ensure that the tests are appropriate, adequate, and effective,.
- The contractor shall use CI/CD techniques. Code shall be deployed to production at least weekly, with preference of daily releases to production in small change sets.

The system shall be deployable at any time.
    - The contractor shall deploy features such that the government can decide when the features will be activated.
    - The contractor shall assist with constructing validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
- The contractor shall perform security scans and automated tests with each build to support ongoing authorization and continuously improved security posture.
- The contractor shall perform automated load and performance testing with every deployment. In addition, the contractor shall provide a mechanism or manage the mechanism to provide regular reporting on application performance.
- The contractor shall perform automated integration testing with all internal and external connections and applications.
- Testing shall primarily be automated, reflecting the best-practice "testing pyramid" with an emphasis on excellent code coverage through unit tests. Unit tests should cover a minimum of 85% of the code and the contractor shall provide at least monthly reporting on code coverage and technical debt to the government.
- The contractor shall test compatibility with current government approved web-browsers and mobile applications.

4.5 Sustainment

- The contractor shall be responsible for the operation in production of existing and future capabilities.
- The contractor shall build in monitoring triggers, including scalability options, and effectively monitor the system to reveal any production issues as they happen and to monitor the performance of the application.
- The contractor shall provide root cause analysis on all outages with actionable recommendations on how to prevent issues going forward.
- The contractor shall ensure that the systems are monitored effectively to reveal user analytics and interactions and provide the capability to automatically report on such activities.
- The contractor shall ensure that there is an automated way to monitor for network-related production issues, providing the capability to rule out application issues.
- The primary responsibility for monitoring production network systems is held by the USCIS Network Operations Center (NOC). The contractor shall ensure that appropriate monitoring is in place and work with the USCIS NOC on monitoring alerts and escalation processes.
- The government expects 24x7 application and system monitoring with incident response that shall not exceed 15 minutes response time to the government point of contact (POC) after first notice of the incident. The contractor shall have the availability of designated full stack engineers and other needed personnel for resolution of critical or high severity production issues if and when they occur. The contractor shall be available to troubleshoot and restore system availability and functionality. The number of support requests received outside of normal business hours varies, but averages to approximately five (5) times per month.
- The contractor shall provide scheduled (i.e., recurring) and unscheduled reports

derived from data contained in the Accounts Public application. The requests for unscheduled reports shall be initiated by stakeholders within the Government in response to inquiries from entities such as DHS Security, members of Congress, and the Office of Inspector General.

- The contractor shall be responsible for responding to system audit inquiries made by Information Security Division personnel. The contractor shall coordinate with the ACCTPUB ISSO in responding appropriately with required artifacts, system documentation, and evidence.

4.6 Administrative Activities

- The contractor shall collaborate with stakeholders, support contractors, and third party vendors throughout system integration, performance, security, Section 508, system acceptance, user acceptance, usability, and test and evaluation reporting.
- The contractor shall manage all contractor resources and supervise all contractor staff in the performance of work on this contract. The contractor shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members. Likewise, the contractor must ensure that the health and progress against those plans are adequately reported.
- The contractor shall organize, direct and coordinate planning and execution of all contract activities.
- Tools for transparency, such as the agency Agile Application Lifecycle Management (ALM) tool, shall be populated so that reports and charts can be generated as needed, and so that user stories, defects, and tasks and their status are available to stakeholders. Task boards and SharePoint sites, meetings, and demos can be used to share information and report progress.
- The contractor shall conduct and report out on retrospectives for overall team and government improvement.

4.7 Provide Technical Assistance

- Tier-I Support will be provided by the government.
- The contractor shall provide Tier-II support as part of their DevSecOps Agile team function. Tier-II support requires technical knowledge and is staffed by contractor technicians who have troubleshooting capabilities beyond the Tier-I level.
- The contractor shall collaborate, coordinate and interface with, and provide knowledgebase data, scripts, and procedures to, the USCIS Tier-I Service Desk for their responses to internal USCIS technical service requests.
- The contractor shall provide Tier-III support as part of their DevSecOps Agile team function, and shall respond directly to external technical assistance requests.
- The contractor shall collect relevant data, and provide meaningful analytics and insights for incidents in order to resolve service requests. The contractor shall respond to service requests within 15 minutes of notification to the contractor POC for Tier II and III requests. The contractor shall track the history of incidents and conduct analysis for forecasting and retrospectives.

- The contractor shall provide subject matter expertise to USCIS OIT and third-party vendors in support of troubleshooting issues related to the applications, such as emergency software fixes and application interface problems. The contractor shall maintain the list of troubleshooting steps for common issues regarding the applications and augment as needed.
- The contractor shall provide technical assistance to triage and support averages about 500 support tickets per month.

5 KEY PERSONNEL

The contractor shall identify key personnel and provide statements of qualifications for these individuals as a part of the solicitation process. Key Personnel shall be current, full time employees of the prime or subcontractor. This task order requires the following Key Personnel: a Program Manager, a DevSecOps Architect Lead, and a UI/UX Design Lead who should be leading and providing guidance to the DevSecOps teams listed in section *3 Teams*. These individuals must have extensive expertise in the Agile and DevSecOps software development approaches, and experience using many of the tools included in the Development/Test Tool Suite identified previously. Since this is a team-oriented contract, all of the key personnel may have other duties that coincide with their skillsets, such as business analyst, tester, or Scrum Master functions.

The Program Manager shall ensure that all work on this contract complies with contract terms and conditions and shall have access to contractor corporate senior leadership when necessary. The contractor's Program Manager shall be the primary interface with the USCIS Contracting Officer's Representative (COR) and Contracting Officer (CO) and shall attend status meetings and ad hoc meetings with stakeholders as required, accompanied by other key personnel when necessary.

The DevSecOps Architect shall ensure architecture compliance and maintain a healthy technical roadmap working with the government technical lead. The UI/UX Design Lead shall maintain overall design consistency and the voice of the end-users.

Key Personnel Minimum Qualifications:

- **Program Manager**
  - Shall have a minimum of six (6) years of IT Project Management experience focusing on development projects. Within this six (6) year timeframe the individual:
    - Shall have at least two (2) years of specialized experience in managing IT DevSecOps projects.
    - Shall have at least three (3) years of experience managing scrum team(s).
  - Shall have a current Project Management Professional (PMP) Certification from PMI.
  - Shall have, at a minimum, a Bachelor's degree in Computer Science, Information Technology Management or Engineering.
- **DevSecOps Architect Lead**
  - Shall have a minimum of ten (10) years of experience in the Information Technology field focusing on development projects, DevSecOps and technical architecture specifically. Within this ten (10) year timeframe the individual:
    - Shall possess strong architecture & design experience, including at least three (3)

years of experience deploying enterprise applications in cloud platforms, preferably in AWS.
    - Shall have, at a minimum, a Bachelor's degree in Computer Science, Information Technology Management or Engineering.
    - Shall possess expertise in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.
- **UI/UX Design Lead**
    - Shall have a minimum of ten (10) years of experience in the Information Technology field focusing on development projects and UI/UX Design specifically. Within this ten (10) year timeframe the individual:
        - Shall possess strong architecture & design experience, including at least three (3) years of experience providing UI/UX Design expertise for enterprise applications on AWS.
    - Shall possess expertise in large scale, high performance enterprise application deployment and UI/UX Design on complex heterogeneous environments in AWS.
    - Shall have, at a minimum, a Bachelor's degree in Computer Science, Information Technology Management or Engineering.

6 TRANSITION SUPPORT

6.1 Transition In

Once the Authorization to Proceed is granted, the Contractor transition in will begin with the first sprint in accordance with agile principles. Knowledge acquisition is expected to occur within iterations or in the process of performing tasks in the Scrum or Kanban process.

6.2 Transition Out

Upon completion of performance of this contract, the contractor shall fully support the transition of the contractor's work that is turned over to another entity, either government or a successor offeror(s). The contractor shall assist with transition iterations. To help ensure smooth transition, it is expected that the incoming and outgoing contractors will use techniques such as pair programming to facilitate knowledge sharing without disrupting development.

Because the contractor will have automated the development, test, and deployment pipeline, and because the contractor will have documented important design decisions and processes in the SDD, the expectation is that this automation and documentation will be utilized to enable a smooth transition. The contractor shall be responsible for the implementation of the transition and application cutover activities. The transition shall cause no disruption in development services.

The contractor shall be responsible for the transition of all technical activities identified in this contract. As part of the transition, the contractor shall be responsible for:

- Inventory and orderly transfer of all Government Furnished Property (GFP), to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process

- Transfer of all software code in process
- Certification that all non-public DHS information has been purged from any contractor- owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management team

Transition planning generally begins 120 days before the transition deadline. If the government provides a Transition Plan template, the contractor shall complete it as assigned; otherwise the contractor shall submit a Transition Plan at the direction of the government. The Transition Plan shall:

- Document the strategic approach
- Identify equipment, hardware, software, documents and other artifacts that are included in the transition
- Establish milestones and schedules
- Establish activities
- Identify transition risks and risk mitigation
- Define roles and responsibilities
- Define transition approval authorities and lines of communication
- Define appropriate labor mix to perform CI/CD activities
- Define a knowledge transfer approach
- Define a property inventory and transition approach
- Create bi-party or tri-party agreements
- Provide checklists

7 DELIVERABLES

The primary deliverable of this contract is deployed application code. The contractor shall deliver this code throughout the period of performance. Deployed application code is defined as, but not limited to:

- Application source code
- Application build scripts
- Test code and reports
- Environment build scripts
- Deployment scripts

All deployed application code shall be checked into the enterprise source code repository. Please note that the test code for automated tests is a critical deliverable: USCIS expects good test code coverage (a minimum of 85% unit test code coverage) and effective tests, as these will become part of the regression test suite to be used in future development work as well.

The contractor shall deliver system design documentation on the Software Design Document wiki, as well as scripts for manual testing when appropriate.

The contractor shall submit electronic copies of document deliverables that are indicated in the table

below to the CO and COR (and other cc's as may be specified by the CO and/or COR) via e-mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30 PM local time Monday through Friday, unless stated otherwise.

All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.

7.1 Task Order Management Artifacts

The contractor shall provide standard and ad hoc reports such as status briefings that support task order management, as described below:

- As required by the COR, the contractor shall attend meetings with the COR and/or other USCIS stakeholders in order to review work accomplished, work in progress, plans for future work, transition plans and status, and issues pertinent to the performance of work tasks that require USCIS attention. The meetings may be scheduled regularly or may be ad hoc.
- In the event the government requires additional information related to task order technical or schedule performance, risks, resources, or any task order-related data, the contractor shall provide this report information in the format requested by the government. Requests for reporting may vary in scope and complexity and may require the contractor to attend OIT meetings to obtain required information, review and research applicable documentation, and extract applicable database information required to assemble the report.

7.2 Deliverables Schedule

The deliverables that apply to this contract, and that the contractor shall provide are outlined in *Table 2: Deliverables Schedule*.

Table 2: Deliverables Schedule

Section 4 - Task	Item	Frequency of Delivery	Acceptable Formats
3.0	Trusted Tester Report	Quarterly or within 10 working days of any change in the Trusted Tester population	MS Word or MS Excel
4.1	In-process application code, test code, deployment scripts, build scripts	Continuously, with each build	Code checked into the USCIS code repository
4.1	Shippable application code, test code, deployment scripts, build scripts	Continuously, with each commit	Code checked into the USCIS code repository
4.2	System Design Document (SDD)	Continuously updated	USCIS Repositories

4.2	Web Services Logs, ICD and other related deliverables	As directed by PM	MS Word, Excel, Visio or PowerPoint
4.5	Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	As directed by the OIT Program Manager	MS Word, Excel, Visio, or PowerPoint
4.5	Sprint Review Brief (includes burndown chart, unit testing code coverage, technical debt) - Unit testing shall have, a minimum of 85% code coverage - Technical debt shall include risk and cost.	At least every two (2) weeks during Sprint Review	PowerPoint, MS Word, Excel, Visio
4.1	Performance Updates	At least every release	Email, MS Excel, dashboards
4.5	Staffing Report (includes EOD'd staff and open billets and status)	Weekly for Base Period and then at least monthly thereafter	PowerPoint, MS Word, Excel, Visio
4.5	Contract Status Report (covers actions completed on each task for time period)	Monthly	PowerPoint, MS Word, Excel, Visio
6.2	Transition Out Plan	120 days prior to expiration of the TO as directed	MS Word
8.1	Corporate Telework / Remote work Plan	Contract NTP	MS Word
8.3, Attachment 6	GFP Report (Make, Model, SN, Contractor Name, Location, Dates)	Monthly	MS Excel
Solicitation, C-3	Redacted copy of the executed task order including all attachments suitable for public posting under the provisions of the Freedom of Information Act (FOIA)	Within 30 days of task order award	Email to foiaerr.nrc@uscis.dhs.gov with a courtesy copy to the CO.

Attachment 2 – Security Clause with IT	DHS Mandatory Training	Annually by December 31st of each year	MS Word
	DHS Rules of Behavior	Prior to accessing DHS systems and sensitive information	MS Word
	Separation Notification	The CO and COR must be notified of each contract employee termination/resignation within five (5) days of each occurrence. The COR will then notify the Office of Security & Integrity (OSI) Personnel Security Division (PSD) to coordinate the exit clearance forms.	Exit Clearance Forms

7.3 Inspection and Acceptance

Various government stakeholders will inspect contractor services and deliverables. The CO will provide official notification of acceptance and rejection of deliverables. The COR will provide notice of acceptance. Inspection and acceptance of deliverables will use the following procedures:

- The government will decide whether to accept functionality delivered after it is demonstrated to a government product owner. The product owner and other stakeholders might provide feedback that requires re-work on the contractor's part. This process follows normal Agile software development practices.
- The government will also periodically evaluate the contractor's code quality, test coverage, test and deployment code quality, security, and so on. Based on these periodic reviews, the government may require rework on the contractor's part. The government expects high quality work that meets standards specified by the government, and does not expect to find significant problems during these reviews.

8 TASK ORDER ADMINISTRATION DATA

8.1 Place of Performance

The principal place of performance shall be at the contractor provided work site. The key personnel and at least two (2) full DevSecOps team must be located at the contractor provided work site. The government will allow remote work for the remaining contractor employees as long as the work is completed efficiently and effectively. This may change due to contractor performance. If remote work and/or telework will be utilized, then the contractor shall provide remote work and and/or telework plans for approval by the government.

The contractor shall maintain a facility to be in close proximity to the USCIS facility at 111

Massachusetts Ave NW, Washington D.C., not to exceed a distance of 20 miles radius. Meetings will take place at both the contractor site and USCIS offices in the Washington, D.C. Metropolitan Area, including, but not limited to 20 Massachusetts Avenue, N.W., and 111 Massachusetts Avenue, N.W., Washington DC. Meetings may also occur at the contractor's work site, especially when close collaboration between stakeholders and the development team is needed. The contractor shall be available to meet with the Government within reasonable notice. The contractor shall provide workspace, such as a team room, to accommodate up to six (6) Government representatives, with the capacity to accommodate up to 25 individuals.

8.2 Hours of Operation

The core duty hours for the Government are from 8:00 AM to 4:30 PM, Monday through Friday, excluding Federal Government holidays. The contractor shall be available during this time period, but also available to support Tier II/III issues or any outages to the systems on a 24x7x365 basis. It is the expectation of the government that the systems are built in such a way that they do not go down and therefore this support should be minimal.

8.3 Government Directed Travel

Travel may be required in order to perform certain tasks assigned by the government. The contractor shall be reimbursed for travel in accordance with the GSA Federal Travel Regulations, 41 Code of Federal Regulations (CFR), and Chapters 300 through 304. The contractor shall be responsible for obtaining COR approval (email is acceptable) for all reimbursable travel in advance of each travel event. The travel request should summarize the purpose of travel, dates, per diem, hotel and airline costs. The contractor may not be compensated for unapproved travel requests. Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices.

Travel within the local commuting area will not be reimbursed. For the purpose of this task order the local commuting area is defined as a fifty (50) mile radius from their primary office location. The contractor shall be responsible for obtaining COR approval (email is acceptable) for all reimbursable travel in advance of each travel event. Home to work travel is not reimbursable.

9 Performance Criteria

A balanced scorecard approach will be used to evaluate contractor performance. The contractor teams will be evaluated at a minimum every quarter, and the evaluation will be discussed with the contractor. The purpose of the scorecard and discussions is to enhance performance. In addition, in the aggregate, the scorecards and discussions will be used partially as a basis for past performance reporting.

Within the balanced scorecard, the relative weights of the evaluation categories will be adjusted by the Government based on its experiences, and will be communicated to the contractor after each quarterly cycle. The Contracting Officer and contractor will receive a copy of the evaluation. The contractor may provide comments or responses to the scorecards to the COR and the Contracting Officer within a week after receipt of the scorecard and grade.

It is anticipated that the contractor will be evaluated along the following dimensions:

- Code Quality and Standards Adherence. Contractor code will be evaluated by Government teams and IV&V providers.
- Test Quality and Test Coverage. Because automated tests are a key component of this process, test scripts and code will be treated as deliverables under this task order. These test scripts and code will be assessed for their quality and for the extent to which they test the appropriate functions. Evaluations will be performed by the IV&V test team, or Government employees.
- Production Performance. The contractor will be evaluated on the performance of their code in production: its availability, response time, usability, accuracy and lack of defects.
- Process and Continuous Improvement. The contractor teams will be assessed on the processes they implement, their conformance to USCIS processes, their conformance with Systems Engineering Life Cycle (SELC) and other required frameworks, and their use of retrospectives to continuously improve these processes.
- Productivity. Velocity and story point completion will be measured and compared against historic team averages, the Government will evaluate the value delivered and also to note any unproductive behavior.
- Compliance. Maintaining system boundary authority to operate.
- Performance of technical support response times to outages and customer initiated issues