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

1. REQUISITION NUMBER	PAGE	OF
OIT209001	1	37

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS-35F-404DA	01/31/2020	70SBUR20F00000043	70SBUR19Q00000150	08/23/2019

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Charlotte Edwards	802-872-4692	

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: 9277550330000 — FACILITY CODE:

SOLUTION TECHNOLOGY SYSTEMS INC
1600 WILSON BLVD STE 1300
ARLINGTON VA 222092594

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: 927755033+0000 - ITPR-20-00101 Biometrics Development, Security, and Operations (BDSO) This order is for commercial services under GSA Schedule 70. Part I: Schedule *(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 ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

☐ 29. AWARD OF CONTRACT: _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR
William Callery
Digitally signed by William Callery
Date: 2020.01.31 14:20:15 -05'00'

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
TRACEY B HARRIOT
Digitally signed by TRACEY B HARRIOT
Date: 2020.01.31 16:05:22 -05'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
William Callery, President, STSI (CTA Lead)	**2020-01-31**	TRACEY B. HARRIOT	31 JAN 2020

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	–				
	AAP Number: 2018042525				
	Period of Performance: 03/01/2020 to 02/28/2021				
	BASE PERIOD				
	03/01/2020 - 02/28/2021				
0001	Key Personnel	[redacted]		[redacted]	[redacted]
	Base Year				
	[redacted]				
	PSC: D308				
	Accounting Info:				
	ITBIOME PMO EX 20-01-00-000				
	23-20-0900-00-00-00-00 GE-25-86-00 000000				
	Funded: [redacted]				
	Accounting Info:				
	ITBIOME NAS EP 20-05-00-000				
	23-20-0900-00-00-00-00 GE-25-86-00 000000				
	Funded: [redacted]				
	Accounting Info:				
	ITBIOME NAS EX 20-01-00-000				
	23-20-0900-00-00-00-00 GE-25-86-00 000000				
	Funded: [redacted]				
	Accounting Info:				
	ITBIOME CFM EP 20-05-00-000				
	23-20-0900-00-00-00-00 GE-25-86-00 000000				
	Funded: [redacted]				
	Accounting Info:				
	Continued ...				

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)
	ITBIOME CFM EX 20-01-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted]				
0002	DevSecOps Teams Not to Exceed Ceiling of [redacted] Base Year [redacted] PSC: D308 Accounting Info: ITBIOME CFM EX 20-01-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: ITBIOME CFM EP 20-05-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: ITBIOME NAS EX 20-01-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted] Accounting Info: ITBIOME NAS EP 20-05-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted]				[redacted]
0002 AA	DevSecOps Team 1 Base Year (Price Included in [redacted]) PSC: D308 [redacted]	[redacted]			
0002 AB	DevSecOps Team 2 Base Year (Price Included in [redacted]) PSC: D308 [redacted]	[redacted]			
0002 AC	DevSecOps Team 3 Base Year (Price Included in [redacted]) PSC: D308 [redacted]	[redacted]			

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0002 AD	DevSecOps Team 4 Base Year [redacted] PSC: D308 [redacted]	[redacted]			
0002 AE	DevSecOps Team 5 Base Year [redacted] PSC: D308 [redacted]	[redacted]			
0002 AF	DevSecOps Team 6 Base Year [redacted] PSC: D308 [redacted]	[redacted]			
0002 AG	DevSecOps Team 7 Base Year [redacted] PSC: D308 [redacted]	[redacted]			
0003	Travel [redacted] Base Year [redacted] PSC: D308 Accounting Info: ITBIOME NAS EP 20-05-00-000 23-20-0900-00-00-00-00 GE-25-86-00 000000 Funded: [redacted]				[redacted]
0004	Optional Design Personnel Team 1 Base Year [redacted] PSC: D308 [redacted]	[redacted]		[redacted]	

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
0005	Optional DevSecOps Team 1 [redacted] Base Year [redacted] PSC: D308 Amount: [redacted]				[redacted]
0006	Optional DevSecOps Team 2 [redacted] Base Year [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]				[redacted]
0007	Optional DevSecOps Team 3 [redacted] Base Year [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]				[redacted]
0008	Optional DevSecOps Team 4 [redacted] Base Year [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]				[redacted]
	OPTION PERIOD 1 03/01/2021 - 02/28/2022				
1001	Key Personnel Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise [redacted]	[redacted]			

Continued ...

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1002	DevSecOps Teams Not to Exceed Ceiling of [redacted] Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
1002 AA	DevSecOps Team 1 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1002 AB	DevSecOps Team 2 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1002 AC	DevSecOps Team 3 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1002 AD	DevSecOps Team 4 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Continued ...	[redacted]			[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1002 AE	DevSecOps Team 5 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1002 AF	DevSecOps Team 6 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1002 AG	DevSecOps Team 7 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]	[redacted]			[redacted]
1003	Travel [redacted] Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted]				[redacted]
1004	Optional Design Personnel Team 1 Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted] Continued ...	[redacted]			

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1005	Optional DevSecOps Team 1 [redacted] Option Year 1 [redacted]1 PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
1006	Optional DevSecOps Team 2 [redacted] Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
1007	Optional DevSecOps Team 3 [redacted] Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
1008	Optional DevSecOps Team 4 [redacted] Option Year 1 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted] OPTION PERIOD 2 03/01/2022 - 02/28/2023 Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2001	Key Personnel Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]	12	MO	[redacted]	
2002	DevSecOps Teams [redacted] Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
2002 AA	DevSecOps Team 1 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted] Accounting Info: Funded: [redacted]				[redacted]
2002 AB	DevSecOps Team 2 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted] Accounting Info: Funded: [redacted]				[redacted]
2002 AC	DevSecOps Team 3 Option Year 2 [redacted] PSC: D308 Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted] Accounting Info: Funded: [redacted]				
2002 AD	DevSecOps Team 4 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted])				[redacted]
2002 AE	DevSecOps Team 5 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted]				[redacted]
2002 AF	DevSecOps Team 6 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted]				[redacted]
2002 AG	DevSecOps Team 7 Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] [redacted]				[redacted]
2003	Travel [redacted] Option Year 2 [redacted] Continued ...				[redacted]

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				
2004	Optional Design Personnel Team 1 Option Year 2 [redacted] PSC: D308 Amount: [redacted] [redacted] 02/01/2022 Accounting Info: Funded: [redacted]			[redacted]	
2005	Optional DevSecOps Team 1 [redacted] Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
2006	Optional DevSecOps Team 2 [redacted] Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted]				[redacted]
2007	Optional DevSecOps Team 3 [redacted] Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Continued ...				[redacted]

NAME OF OFFEROR OR CONTRACTOR
SOLUTION TECHNOLOGY SYSTEMS INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: Funded: [redacted]				
2008	Optional DevSecOps Team 4 [redacted] Option Year 2 [redacted] PSC: D308 Amount: [redacted] Anticipated Exercise Date: [redacted] Accounting Info: Funded: [redacted] The total amount of award: [redacted]				[redacted]

Contractor Teaming Arrangement (CTA)

This task order award is issued to STSI on behalf of the Flashy Biometrics Contractor Teaming Arrangement. Membership of the CTA is identified below.

"Flashy Biometrics" CTA: Composed of [redacted]

"Flashy Biometrics" CTA Team Lead: Solution Technology Systems, Inc. (STSI)

DUNS Numbers: [redacted]

Solution Technology Systems (STSI) [redacted]

The following labor categories and rates are applicable to the CLINs below.

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Part II—Task Order Clauses

This task order is subject to the terms and conditions of the GSA Schedule Contract.

Federal Acquisition Regulation (FAR) Clauses Incorporated by Reference

52.252-2 Clauses Incorporated By Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses: http://www.acquisition.gov/far.

(End of clause)

52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.204-14 Service Contract Reporting Requirements (Oct 2016)

52.209-10 Prohibition on Contracting With Inverted Domestic Corporations (Nov 2015)

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

Alternate 1 (Jan 2017)
Fill-ins: (i)(1) (ii)(D)(1) [travel]; (i)(1)(ii)(D)(2): [$0]

52.217-8 Option to Extend Services (Nov 1999)
fill-in: 30 days before the task order expires

52.227-17 Rights in Data—Special Works (Dec 2007)

52.237-3 Continuity of Services (Jan 1991)

52.245-1 Government Property (Jan 2017)

52.245-9 Use and Charges (Apr 2012)

Federal Acquisition Regulation (FAR) Clauses Incorporated in Full Text

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

(a) The government may extend the term of this contract by written notice to

the contractor within **15 days of task order expiration**; provided that the government gives the contractor a preliminary written notice of its intent to extend at least **60 days** before the contract expires. The preliminary notice does not commit the government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **36 months**.

(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" wherever such application is appropriate.

(End of clause)

52.252-6 Authorized Deviations in Clauses (Apr 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(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.

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:

(b) Clauses.

__X__3052.203-70 Instructions for Contractor Disclosure of Violations.

__X__3052.204-70 Security Requirements for Unclassified Information Technology Resources.

__X__3052.204-71 Contractor Employee Access.

__X__Alternate I

__X__3052.205-70 Advertisement, Publicizing Awards, and Releases.

__X__3052.215-70 Key Personnel or Facilities.

The Key Personnel or Facilities under this Contract:

Program Manager
DevSecOps Solutions Architect Lead
UI/UX Design Lead
Data Architect/Scientist Lead
__X__3052.242-72 Contracting Officer's Technical Representative.

(End of clause)

Safeguarding Of Sensitive Information (Mar 2015)
(HSAR Class Deviation 15-01)

(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 107296,

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 ofthe 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 tothe *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 thirdparty 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)
(HSAR Class Deviation 15-01)

(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)

Other Task Order Requirements

II-1. ADDITIONAL INVOICING INSTRUCTIONS

In accordance with the CTA, invoices shall only be submitted by the CTA Lead.

INVOICE SUBMISSION INSTRUCTIONS (Addendum to FAR 52.212-4(g))

(a) Each invoice shall contain the following additional information:

(1) GSA contract number and task order number

(2) Name of the Contract Specialist and/or Contracting Officer

(b) Each invoice must be submitted to the designated billing office via one of the following modes (listed in descending order of preference):

(1) Electronically – Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically using the "To" line in the e-mail address to **USCISInvoice.Consolidation@ice.dhs.gov** with each email conforming to a size limit of 500 KB.

(2) Via mail – If a paper invoice is submitted, mail the invoice to:

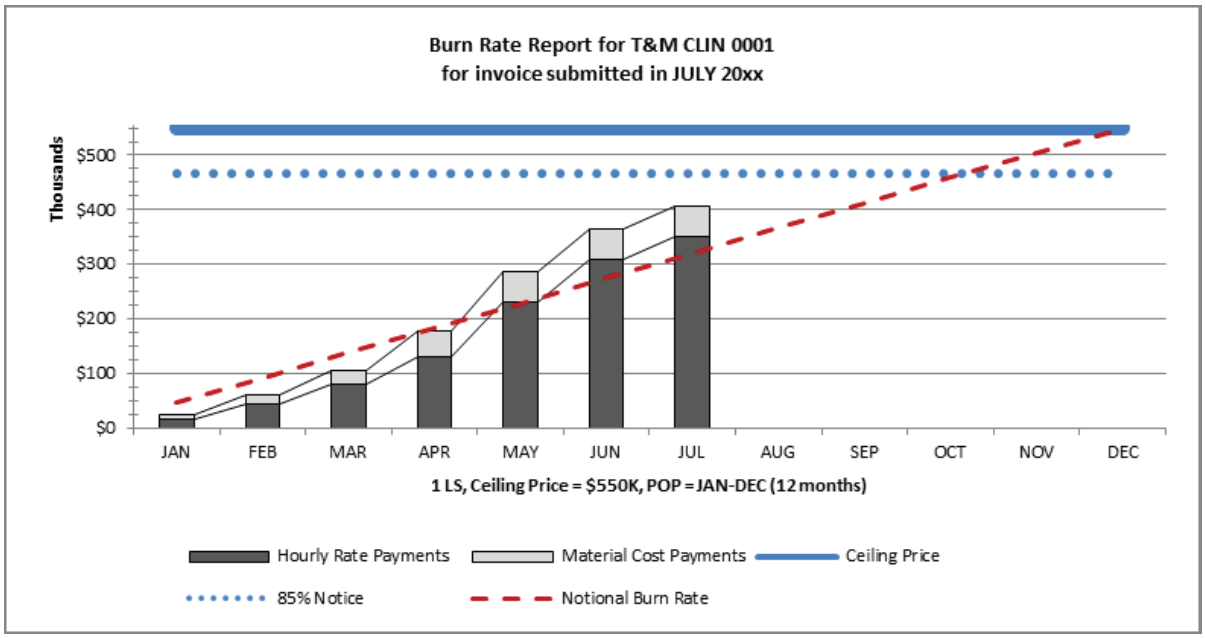
USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

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

(d) 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.

(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.

II-2. POSTING OF ORDER IN FOIA READING ROOM

(a) The government intends to post the 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 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.

II-3. NOTICE TO BEGIN PERFORMANCE

(a) Performance of the work requires unescorted access to government facilities or automated systems, and/or access to sensitive but unclassified information. Security Requirements in Part II-5 apply.

(b) The contractor is responsible for submitting packages from employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations, and for submitting them in a timely manner. A government decision to not grant a favorable EOD decision or suitability determination, or to later withdraw or terminate such decision or termination, shall not excuse the contractor from performance of obligations under this task order.

(c) The contractor may submit background investigation packages immediately following task order award.

(d) This 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 performance to begin no later than 60 days following task order award (allowing up to 60 days for EOD period). Once a suitable number of personnel have received a favorable EOD (as determined by the government Program Manager (PM) and Contracting Officer), the CO will issue a notice to begin performance. This notice will be provided at least one business day prior to anticipated performance start date.

II-4. GOVERNMENT-FURNISHED PROPERTY

(a) The Government will provide contractor personnel with the GFP specified in PWS Section 8.3.

(b) The contractor shall notify personnel that there shall be no expectation of privacy on any USCIS Systems.

(c) The contractor shall operate Government provided property in accordance with USCIS procedures and manufacturer's specifications.

(d) The contractor shall initiate and track maintenance calls and/or service requests for government provided IT equipment to the DHS Helpdesk. The contractor shall notify the COR and/or government PM of any repair needs and/or problems with maintenance/service contractor activities within four hours of each occurrence.

(e) The Government provides computer laptops and software in various hardware configurations, and reserves the right to upgrade, add, delete, or replace equipment and software.

II-5. SECURITY REQUIREMENTS

SECURITY CLAUSE 5 (JUN 2019)

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.

FITNESS 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 Fitness authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment Fitness 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 Fitness 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 Unclassified Information Non-Disclosure Agreement

3. FD Form 258, Fingerprint Card **(2 cards)**

4. Form DHS 11000-9, Disclosure and Authorization Pertaining to Consumer Reports 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 Federal Contract 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 duty for 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 own training)
- **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 out so 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.

II-6. 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—List of Attachments

Attachment	Title/Description	Pages
1	Performance Work Statement (PWS)	22
2	DHS Enterprise Architecture Compliance	1
3	Capitalized Property, Plant & Equipment (PP&E) Assets Internal Use Software (IUS)	2
4	Section 508 Requirements	3
[redacted]	[redacted]	[redacted]

Attachment 1

Performance Work Statement (PWS)
United States Citizenship and Immigration Services (USCIS)
Biometrics Development, Security, and Operations (BDSO)

1. OVERVIEW

U.S. Citizenship and Immigration Services (USCIS) administers the nation's lawful immigration system, safeguarding its integrity and promise by efficiently and fairly adjudicating requests for immigration benefits while protecting Americans, securing the homeland, and honoring our values.

Biometrics Development, Security, and Operations (BDSO) will consist of teams of personnel to provide development, security, and operations (DevSecOps) services that include artificial intelligence / machine learning (AI/ML) to support USCIS Information Technology (IT) system delivery. The BDSO personnel will perform DevSecOps services for USCIS systems hosted in any of the USCIS datacenters or cloud environments. Currently, that environment is located in Amazon Web Services (AWS) but may eventually be located in a different cloud environment. The BDSO personnel will be operating and modernizing complex, legacy, large-scale, Internet-facing websites and IT systems in the cloud using forward-thinking, modern, open source technologies and backend systems with heavy customer engagement.

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 BDSO contractor will be responsible for developing IT capabilities working within those architectures and processes to meet the business requirements.

2. SCOPE

The BDSO contractor shall engage in the maintenance and DevSecOps for USCIS Biometrics efforts to accomplish, but not limited to, the following requirements:

(1) The contractor shall be responsible for teams that perform the full suite of DevSecOps tasks in AWS cloud environment using agile methodologies, including participating in creating user stories for both business functionality and technical requirements and defining, but not limited to acceptance criteria; estimating the size of stories; designing solutions including business/system/data architecture.

(2) The contractor shall perform continuous DevSecOps services in AWS cloud environment and have total responsibility of all the system and software development lifecycle including, but not limited to, development, operations, security, and testing each set of

capabilities in all applicable environments to release to end-users. The contractor shall use an automated-first with integrated security gates for continuous development, continuous delivery, and continuous integration (CI/CD). The contractor is also expected to evolve current best practices and adopt cutting edge best practices for IT delivery as needed. This includes integrating AI/ML into the DevSecOps approach, fuzzy based automated testing; seamless sustainment and quality management of code in production; managing data architectures for transactions and analytical solutions. The contractor shall also maintain team managed deployment (TMD) approval and continuously test its product to ensure its quality.

(3) The contractor shall perform engineering tasks to meet agency needs such as designing, implementing, and maintaining scalable serverless/containerized platforms with AI/ML and/or other types of advanced algorithms (i.e. Natural Language Processing, and rules inference) that can be scientifically tested and proven. These automated systems will have to be subjected to external review and audits at the government's discretion. The contract shall also establish a data governance framework to enforce data standards and improve accuracy using integrated internal and external disparate data sources.

USCIS will manage system roadmaps, project plans, and product and release backlogs that will be the basis for the USCIS BDSO contractor's work and the contractor will support as needed. A USCIS Product Owner (PO) 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 USCIS BDSO 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 PO, 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, SCRUM, Kanban, and Lean Software Development, and the contractor will be expected to conform its processes to these approaches.

Services in support of BDSO shall be provided by a program management team and specified labor categories with demonstrated experience in executing an agile program and using technologies as described in *Section 2.1 Technical Landscape*. Each labor categories shall cover the skills and experience necessary to accomplish agile work using these tools. In addition, DevSecOps refers to primary principles of integrating multi-disciplinary labor categories to provide agile teams with "zero-trust", "automation-first" and "infrastructure as code" mindset of automating everything possible through well documented and tested code and scripts.

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 a serverless, containerized micro-services, and other AWS FedRAMP offerings. The contractor shall provide expertise in this area.

2.1 Technical Landscape

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

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.

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 ecosystem may include, but is not limited to the table below:

Table 1: Current Tool Suite and Platforms

Name	Function
Apache ActiveMQ	Messaging Provider
Apache Atlas	Data Governance and Metadata framework for Hadoop
Apache Hadoop	A collection of open-source software utilities that facilitate using a network of many computers to solve problems involving massive amounts of data and computation.
Apache Hive	A data warehouse software project built on top of Apache Hadoop for providing data summarization, query and analysis.
Apache Jmeter	Performance testing
Apache Kafka / Zookeeper	Message Streaming Platform
Apache Ranger	Framework for data security for Hadoop
Apache Spark	Apache Spark is an open-source cluster-computing framework
Apache Sqoop	A tool designed for efficiently transferring bulk data between Hadoop and structured datastores such as relational databases.
Apache Ignite	In Memory Databases
Apache MXNet	Machine Learning Platform
Apache Tomcat	Application server
Artifactory	Repository manager
AWS Cloud	Public cloud platform. USCIS currently uses EC2, ECS, EMR, S3, ECR, RDS, CloudFormation, CloudWatch, CloudTrails, Lambda, and a number of other AWS services
AWS Linux	AMI/Operating System
BouncyCastle (FIPS)	Crytography API
Brakeman	Code analysis tool which checks Ruby on Rails applications for security vulnerabilities
Cassandra	Database
Chaos Monkey	Application Resiliency Tool
ChaosMonkey	Performance and reliability assessment tool
Chef	Deployment scripting
Cucumber/Jasmine/Selenium	Integration Testing
Databricks	Data platform for machine learning
DeQue FireEyes	508 Development Test tool

Docker	Containerization
Elasticsearch	Big data searching
Fortify	Security test tool
Git / Enterprise GitHub	Distributed version control
GoldenGate	Data replication tool
GraphDB	Open Native Graph DB (ONgDB)
HashiCorp Terraform	Cloud resource creating and management tool
HashiCorp Vault	Secrets Management
Hortonworks Data Platform	Data platform that provides Apache suite of tools
Jackson	Java Representation of JSON
Jasper	PDF file generation
Java Mail	Email message generation
Java, Javascript, Ruby	Programming Language
JAXB	Java Representation of XML
Jenkins	Continuous integration server
Jira	Agile lifecycle management tool
JUnit	Java Unit testing library
Keras	Machine Learning Libraries
Kibana	An open source data visualization plugin for Elasticsearch.
KNIME	Analytics platform
Liquibase	Database automation
Logstash	An open source data collection engine with real-time pipelining capabilities.
Maven	Java artifacts and dependency managements framework
Metacat	Metadata explore
Neo4J	Graph DB
New Relic	Application and Infrastructure Monitoring
Nexus	Repository manager
nTeract.io	Interactive code development
NumPY	Programming Language / Statistical Analysis Packages
OpenCV	Machine Learning Libraries
OpenShift	Container Platform
Oracle & PL/SQL	Database
OWASP	Open Web Application Security Project
PostgreSQL	Database
Python / Anaconda	Programming Language / Statistical Analysis Packages

R / R Studio	Statistical Analysis Software
R Studio	Analytics platform
RCov	Test coverage tool
React Storybooks	Rapid Prototyping
ReactJS / AngularJS / VueJS	Javascript Frameworks
RSpec	Domain Specific Language' (DSL) testing tool
SAS	Statistical Analysis Software
SciKit-Learn	Machine Learning Libraries
Selenium	Automated web browser testing
Service Now	Help desk ticketing system
Snap	Continuous integration and delivery platform
SonarQube	Code quality inspection service
Spark/Scala	Hadoop platform and corresponding programming language
sparkML	Machine learning library
Splunk	Logs and Analysis
Spring Framework	Application Framework
Tableau	Data analytics platform
TensorFlow	Modeling and simulation
Vert.x / SiteMesh	Java web application framework

3. TASKS

The contractor shall be responsible for performing the full systems and software architecture and lifecycle for DevSecOps and full stack engineering tasks using Agile methodologies participating in creating user stories for business functionality and technical requirements and defining acceptance criteria.

This includes all activities related to code delivery and sustainment including any technical debt that is incurred as a result. The contractor shall balance core productivity with technical debt, and should never trade off 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.

While USCIS expects the quality of the development to not require it, in the event of a critical or high severity production issue, the contractor shall designate no more than 5 people on the current staffing mix as an incident response group to be available to restore system availability and functionality 24 hours a day, seven days a week (24x7). The government may allow additional people to support the

incident if necessary.

Continuous delivery and sustainment will follow Agile and DevSecOps government and industry best practices for the following tasks:

3.1 Engineering and Sustainment - Development, Security and Operations

- Contractor shall be responsible for estimating the size of stories, designing solutions, developing code and automated tests, creating deployment scripts, managing code in production, and managing any database solutions.
- Contractor shall use behavior driven development (BDD) and test-driven development (TDD) which includes robust testing of the products to ensure its quality, and shall deploy its code.
- Contractor shall be responsible for the operation in production of the capabilities they develop including monitoring triggers to effectively reveal production issues in less than 2 hours.
- Contractor shall provide root cause analysis on all outages with actionable recommendations on how to prevent issues going forward.
- Contractor shall ensure that the operational dashboards are available to monitor end-to-end of the system to reveal any production issues when they occur and to monitor the performance of the application. This may include System and Web Services Health Checks, Logs, ICD and other related dashboards.
- 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.
- Contractor shall ensure that there is an automated method to monitor for network-related production issues, providing the capability to rule out application issues.
- The contractor shall ensure that appropriate monitoring is in place and shall work with the DHS/USCIS Network Operations Center (NOC) and or other data partners NOC on monitoring alerts and escalation processes.
- Contractor shall alert the NOC in the event of an outage as soon as it is known by the team, and will lead resolution and coordination of resolution, in full transparency, in conjunction with the NOC.
- The contract shall obtain and maintain approval for TMD.

3.2 Continuous Live Documentation

- Contractor shall maintain a living dynamic repository of documentation.
- 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.
- Contractor shall document system design and procedures in the wiki that USCIS uses for artifacts such as System Security Plan (SSP) and System Design Document (SDD) concurrent with DevSecOps activities. In general, USCIS prefers relatively

lightweight but effective and usable documentation.

3.3 User-Centered, Business Driven Design and Experiences

- 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.
- Contractor will be responsible for designing and implementing business processes and user interfaces and for working with USCIS stakeholder and users to maximize the usability of the system. Design will be done in conformance with USCIS design standards and in collaboration with USCIS.

3.4 End-to-End Testing and Integration

The contractor shall provide end-to-end automated testing with integrated reporting on overall code coverage, technical debt, and quality assurance to the government.

- Contractor shall be responsible for creating stories acceptance criteria, test cases and automated test scripts to support test automation activities.
- Testing shall primarily be automated, reflecting the government/industry best-practice "testing pyramid" with an emphasis on excellent code coverage through unit tests. Unit test should cover a minimum of 90% of the code including models and the contractor shall provide at least monthly reporting on code coverage and technical debt to the government. The build pipeline will also include USCIS standard tools for code standards, test coverage, security testing, and Section 508 Compliance.
- 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. Code and tests will be reviewed by the USCIS OIT Independent Validation & Verification (IV&V) team, comprised of both federal employees and contractor(s), to ensure that the testing is appropriate, adequate, effective, and that it mitigates key risks.
    - Perform automated integration testing with all external nodes (systems and data)
    - Conduct automated load and performance testing with every deployment.
    - Provide continuous application performance reports
- 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 should be deployable at any time.
    - Contractor shall deploy features such that the government can decide when the features will be activated.
    - Contractor shall assist with crafting validation steps (both positive and negative testing) for user acceptance testing on an as needed basis.
- Contractor shall perform security scans and automated testing with each build to support ongoing authorization and continuously improved security posture.

3.5 Program Management and Administrative Activities

- The contractor shall provide reports such as status briefings that support task order management.
- 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 contractor shall collaborate with stakeholders, support contractors, and third-party vendors regarding 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 task order. The contractor shall manage and coordinate its team(s) on a day-to-day basis and ensure plans are communicated to team members.
- The contractor shall organize, direct and coordinate planning and execution of all task order activities.
- Automation and transparency, such as the agency Agile Application Lifecycle Management (ALM) tool, shall be continuously- and well maintained and organized with relevant data so that reports and dynamic dashboards can be generated as needed.
- Annotated and descriptive user stories, diagrams, defects, tasks and their status are available to stakeholders. Task boards and collaboration sites, meetings, and demos shall be used to share information and report progress.
- In the event the government requires additional information related to contract technical or schedule performance, risks, resources, or any contract-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.
- Contractor shall be responsible for conducting working groups for items such as impact mapping, business architecture, data architecture, etc.
- The contractor shall conduct and report out on retrospectives for overall team and government improvement.
- The contractor will be responsible for all transition activities as stated in *Section 5: Transition.*

4. PERSONNEL AND MINIMUM QUALIFICATIONS FOR LABOR CATEGORIES

All members of the Program Management Team are key personnel on the task order. 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 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 personnel when necessary.

The purpose of the DevSecOps teams and Product Design personnel are to provide application development, operations, security, and testing requirements. The contractor should use a behavior driven development (BDD) and test-driven development (TDD) approach as appropriate. The contractor's work shall conform to the architecture and design provided by USCIS and the Agile processes set up by USCIS, but this work will be managed by the contractor. It's the government expectation that there will be a base of seven (7) 12-person teams, however it is up to the contractor to right-size teams to meet the needs of the requirement. The requirement also includes four (4) optional 12-person DevSecOps teams and one optional design personnel team to increase support as needed. The teams must have all of the skills necessary to perform the tasks indicated in *Section 3: Tasks*. It is important that the contract personnel assigned to the task order as a whole have the skills necessary for development, operations, security, test, and maintenance, but that does not mean that specific team members must be designated as testers, coders, etc. Team flexibility is important and teams should have more than one skill. After USCIS prioritization of the backlog, it is up to the contractor to structure the teams so that it can provide all of the necessary functions at a high level of productivity and quality. The teams should be experienced with the latest enterprise systems development techniques, technologies, programming languages, and AWS cloud offerings.

The team structure shall adhere to the following requirements:

- Full-Stack Engineers shall have the ability to perform, but not limited to automation and engineering tasks, AI/ML implementation, data, infrastructure/operations, and security engineer tasks in USCIS cloud environments.
- Business Analysis and UX/UI Design shall have the ability to perform, but not limited to impact mapping, design-thinking, and facilitate/coordinate business architecture working groups.
- These personnel must have problem solving skills with aptitude to support self-organizing multi-disciplinary teams with experience in persona development, data visualization, high-fidelity prototyping, and business process design.
- The Contractor shall accredit at least one member for the task order as a certified Information Systems Security Officer (ISSO) as part of their team composition. This role will be ancillary to the contractor's primary

developer/engineer role. The ISSO is expected to provide software security input and direction to each of the teams and work closely with the USCIS Information Security Division to provide updated guidance to ensure compliance with USCIS security directives.

(1) The Contractor must provide a Trusted Tester certified by DHS OAST 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. 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.

(2) 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 also be provided within 10 working days of any change in the Trusted Tester population.

USCIS requires the following specialized minimum experience for each labor category below:

4.1 Program Management Team (Key Personnel)

- **Program Manager**
  - Shall have a minimum of ten (10) years of IT Project Management experience, focusing on agile projects, inclusive of the following:
    - Shall have at least two (2) years specialized experience in leading IT DevSecOps projects managing over (50) people on multiple Agile teams.
    - Shall have at least three (3) years specialized experience in business process analysis and change management.

- **DevSecOps Solutions Architect Lead**
  - Shall have a minimum of ten (10) years of experience in the Information Technology field focusing on AI/ML engineering projects, DevSecOps and technical architecture specifically inclusive of following:
    - Shall possess strong architecture & design experience, including at least three (3) years of experience deploying production enterprise applications in AWS that use AI/ML.
  - Shall have experience in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.
  - Shall have, at a minimum, a Bachelor's degree in Computer Science, Information Technology Management or Engineering.

- **User Interface/User Experience (UI/UX) Design Lead**

- Shall have a minimum of eight (8) years of experience in the Information Technology field focusing on engineering projects with specific Business and UX Design inclusive of the following:
    - Shall have experience with architecture & design experience, including at least three (3) years of experience providing UX Design expertise for enterprise applications on AWS.
- Shall have experience with large scale, high performance enterprise application deployment and UX Design on complex heterogeneous environments.
- Shall have, at a minimum, a Bachelor's degree in Computer Science, Graphic Design, or Visual Communications.

- **Data Architect/Scientist Lead**
    - Shall have a minimum of ten (10) years of IT experience, focusing on data architecture or data services inclusive of the following:
        - Shall have three (3) years of experience leading data teams in such efforts as: data migration, transformation, data lake implementation/support as well as O&M.
        - Shall have at least five (5) years of proven expertise in Relational and Dimensional Data Modeling
    - Must have experience of cloud architecture, specifically AWS, as it relates to data processing (i.e., EC2, S3, Redshift, etc.)
    - Shall have experience briefing the benefits and constraints of technology solutions to technology partners, stakeholders, team members, and senior levels of management
    - Shall have, at a minimum, a Bachelor's degree in data science, engineering, statistics.

4.2 DevSecOps Personnel

All personnel must have problem-solving skills with aptitude to work in multiple roles. It is expected the contractor will organize personnel into multi-disciplinary teams with a mix of every labor category to meet the requirements of this task order. USCIS does not anticipate using single labor category teams.

- **Scrum Master/Agile Lead**
    - Shall be a certified Scrum Master
    - Shall have a minimum of three (3) years of experience focusing on business architecture analysis and UX/UI Design inclusive of:
        - A minimum of one (1) year experience in building business process models, writing acceptance criteria, and designing user interfaces for a production system.

- **Business Analyst**

- Shall have a minimum of three (3) years of experience focusing on business architecture analysis and UX/UI Design inclusive of:
    - A minimum of one (1) year experience in building business process models, writing acceptance criteria, and designing user interfaces for a production system.

- **Full-Stack Engineer**
    - Shall have a minimum of five (5) years of experience in the Information Technology field focusing on development projects using DevSecOps and AWS cloud environments and experience in AI/ML inclusive of:
        - Experience with full stack engineering (defined as proficient in database development/integration as well as server and client application development/integration), including three (3) years of experience deploying production enterprise applications in AWS.
    - Shall have an additional three (3) years of specific software engineering experience related to front-end and back-end applications and/or data services.
    - Shall possess experience in large scale, high performance enterprise big data application deployment and solution architecture on complex heterogeneous environments in AWS.
    - Shall possess experience with automation and engineering tasks, AI/ML implementation, data, infrastructure/operations, and security engineer tasks in USCIS cloud environments.

- **Systems Developer**
    - Shall have a minimum of five (5) years of experience in writing and testing enterprise software solutions. Experience requirements may be substituted with a Bachelor's degree in Computer Science plus three years of experience in writing and testing enterprise software solutions.
    - Shall also have three (3) years of experience in troubleshooting software which may overlap with the experience requirements above.
    - Shall have experience working in AWS, software containerization and Agile development processes.

- **Data Engineer**
    - Shall have a minimum of five (5) years in modern data development, upgrading, support and design. Experience requirements may be substituted with a Bachelor's degree in Computer Science plus three years of experience in modern data development, upgrading, support, and design.
    - Shall have experience in establishing performance and statistical monitoring of enterprise databases to include, but not limited to; wellness checks, data integrity, privacy and security scans.
    - Shall have experience in supporting cloud database environments, specifically AWS (i.e., EC2, S3, Neptune or Redshift) to include backup and archiving of data.

- **UI/UX Analyst**
  - Shall have a minimum of three (3) years of experience in the Information Technology field focusing on engineering projects with specific Business and UX Design inclusive of:
    - Experience with architecture & design experience, including an additional three (3) years of experience providing UX Design expertise for enterprise applications on AWS.
  - Shall have experience with large scale, high performance enterprise application deployment and UX Design on complex heterogeneous environments.
  - Shall have, at a minimum, a Bachelor's degree in Computer Science, Graphic Design, or Visual Communications.

4.3 Design Personnel (Optional)

- **Technical Writer**
  - Shall have a minimum of five (5) years of experience in the Information Technology field focusing on planning, writing, and communicating technical concepts in a user focused, plain language structure for enterprise applications on AWS.

- **Business Analyst**
  - Shall have a minimum of five (5) years of experience in the Information Technology field focusing on conducting business workflow analysis and user interviews for enterprise applications on AWS.

- **Graphics Specialist**
  - Shall have a minimum of five (5) years of experience in the Information Technology field focusing on projects and UX Design including at least three (3) years of experience with architecture & UX design expertise for enterprise applications on AWS.

5. TRANSITION SUPPORT

5.1 Transition In (Not to exceed 3 Months)

Once the notice to proceed is granted, the contractor transition in will begin *Section 3: Tasks* and will have 3 months to transition all previous task from the previous contractor. During this time knowledge acquisition is expected to occur within iterations or in the process of performing tasks using agile ceremonies such as Scrum or Kanban process.

5.2 Transition Out

Upon completion of performance of this task order, the contractor shall fully support the transition of work that is turned over to another entity, either government or a successor contractor(s). The contractor shall assist with transition. 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 SDD and System Security Plan, 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. To ensure the necessary continuity of services and to maintain the current level of support, USCIS may retain services of the incumbent contractor for some, or all of, the transition period, as required.

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

- Inventory and orderly transfer of all 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
- Participation in knowledge transfer activities in accordance with the transition plan
- Providing members to participate in transition of 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

6. DELIVERABLES

The primary deliverable of this task order is deployed application code. Deployed application code is defined as:

- Application Source Code
- Application Build Scripts
- Test Code/Test Cases
- 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 high test code coverage (a minimum of 90% unit test code coverage, with a 100% coverage objective) 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 to the CO and COR (and others as specified by the CO or COR) via e-mail in the format specified in the table below. All document deliverables shall be made by close of business (COB) 4:30pm EST 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.

6.1 Deliverables Schedule

Table 2: Deliverables Schedule

Section	Item	Frequency of Delivery	Acceptable Formats
3	Section 508 DHS Trusted Tester certification	Within 90 days of award, or when standards change and	Email Attachment to

		re-certification is required by DHS OAST, re-certification for all Trusted Testers within 90 days of training availability.	PM, COR and CS/CO.
3	Trusted Tester Report	Quarterly or within 10 days of any change in the Trusted Tester population.	MS Word, Excel
3.2	Architecture design approval and all edits/updates for delivery and sustainment activities	Continuously updated	Wiki
3	In-process application code, test code/test cases deployment scripts, build scripts	Continuously, with each build	Code checked into the USCIS code repository
3	Shippable application code, test code/test cases deployment scripts, build scripts	Continuously, with each commit	Code checked into the USCIS code repository
3.3	Continuous updates for Architecture and System docs for maintaining an Authority to Operate (ATO) including the System Design Document (SDD)	Continuously updated	Wiki
3.6	Status Briefings, such as presentations, database extractions, meeting reports, burndown charts, etc.	As directed	MS Word, Excel, Visio, or PowerPoint
3.6	Staffing Report (includes departed staff and open billets and status) to COR and ITPM	Weekly for base year and then at least monthly thereafter	PowerPoint, MS Word, Excel, Visio
3.6	Contract Status Report (covers actions completed	As directed by the Government	PowerPoint, MS Word, Excel, Visio

	on each task for time period)		
3.6	Quality Management Plan, Test & Evaluation, Management Plan, and Configuration Management Plan. These plans will be identified and requested on a case by case basis as they pertain to a project or the task order as a whole.	As directed by the government	MS Word or other, as directed by government
4	Sprint Review Brief (includes burndown chart, unit testing code coverage, technical debt)	Every two weeks during Sprint Review	PowerPoint, MS Word, Excel, Visio
4	System and Web Services Health Checks, Logs, ICD and other related deliverables	As directed	MS Word, Excel, Visio or PowerPoint
5.1	Complete Transition In	90 days after award	As directed by government
5.2	Transition Out Plan	90 days prior to expiration of the TO or as directed	MS Word 2010- or other as directed by government
8.1	Corporate Telework Plan including managing Virtual Offices/Sites	As directed	MS Word 2010- or other as directed by government
8.3	GFP Inventory (must contain CIS ID number, location, name of contactor holding equipment, date)	Monthly	Excel
Security Clause 5	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.	
Solicitation II-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.

7. INSPECTION AND ACCEPTANCE

Various government stakeholders will inspect contractor services and deliverables. The CO/COR will provide official notification of rejection of deliverables. 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. Feedback and government acceptance will be provided according to the standard agile practice; however, due to the nature of the work, it is possible that re-work could be determined after a release goes out and is accepted if a noticeable issue is determined after it is put into production.

- The government will also periodically evaluate the contractor's code quality, services, health checks, 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 for the Program Management Team shall be at the

contractor provided work site. The government is amenable to remote workers as long as the work is completed efficiently and effectively. The remaining personnel, outside of the Program Management Team, are able to work remotely. If remote work and/or telework will be utilized, then the contractor shall provide a Corporate Telework Plan to be approval by the government. Of the remote work, 30% of the contractor personnel shall be located in the National Capital Region (NCR). The contractor facility shall be located in the NCR to ensure close proximity to the USCIS facility at 111 Massachusetts Ave NW, Washington D.C. USCIS anticipates relocating to a new facility located in Camp Springs, MD during performance of this task order. Meetings will take place at both the contractor site and USCIS offices in the Washington, D.C. Metropolitan Area. When contractor site meetings are needed, the contractor shall provide workspace, such as a conference room, to accommodate up to six government representatives.

8.2 Hours of Operation

Normal duty hours for the Government are from 8:00am to 5:00pm (EST/EDT), Monday through Friday, excluding Federal Government holidays. The contractor shall be available during this time period, but also available to support any outages to the systems on a 24x7 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 Furnished Property (GFP)/Government Furnished Information (GFI)

Laptops, mobile phones and PIV cards will be issued as GFP and used in performing work on this contract. No personal or company owned storage devices, (thumb drives, DVDs, or CDs) shall be used with the GFP. A webinar account, such as Adobe Connect, will be provided to the contractor to facilitate virtual demos and other meetings with stakeholders at various physical locations. Mobile devices may be provided as identified by the COR or Government Program Manager.

GFI, such as USCIS design standards, will be provided to the contractor following award.

Table 3: Government Furnished Property

Equipment / Government Property	Date / Event Indicate when the GFP will be furnished	Date / Event Indicate when the GFP will be returned	Unit	Quantity	Serial Number(s)	Manufacture & Model Number
Laptop Windows Based and MACs	After EOD	Upon Departure	EA	Up to 150	TBD	Standard USCIS approved manufacturer
Mobile	After EOD	Upon	EA	Up to 20	TBD	Standard USCIS

Phone		Departure				approved manufacturer

The contractor is responsible for all costs related to making the property available for use, such as payment of all transportation, installation or rehabilitation costs. The contractor will be responsible for receipt, stewardship, and custody of the listed GFP until formally relieved of responsibility in accordance with FAR 52.245-1 Government Property and FAR 52.245-9 Use and Charges. The property may not be used for any non-task order purpose. The contractor bears full responsibility for any and all loss of this property, whether accidental or purposeful, at full replacement value.

8.4 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 will 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 USCIS offices located at 111 Massachusetts Ave NW, Washington D.C. 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 every four weeks 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.

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 monthly cycle. The contractor and the CO will receive a copy of the evaluation. The contractor may provide comments or responses to the scorecards to the COR and the CO within one week of 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.
- Business Satisfaction. Each feature completed by a contractor team will be evaluated by the Government Product Owner for that team, and possibly by SMEs assigned to the team. At each iteration review, the functionality will be evaluated by a wider audience of Government employees.
- 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. This evaluation 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.
- Collaboration and Innovation. The contractors will operate within an ecosystem of federal and contractor staff, with multiple contractor teams working in parallel and with constant interaction with USCIS employees. The contractor will be graded based on their willingness, effort, and ability to work collaboratively.
- 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

Attachment 2

Enterprise Architecture (EA) Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

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

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

-Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Mode land Enterprise Architecture Information Repository.

-Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

-Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

Attachment 3

Capitalized Property, Plant and Equipment (PP&E) Assets Internal Use Software (IUS)

1. Background

The United States Citizenship and Immigration Services Management Directive No. 128-001, USCIS/Office of Information Technology has an ongoing requirement to report Internal Use Software (IUS) costs for the programs under their purview and assignment. This report is a monthly mandatory requirement, and must include all software releases with a cumulative cost of $500K or greater; bulk purchases of $1 Million, and a useful life of 2 years or more.

2. Requirement

Reporting: All applicable charges for application releases and/or development charges are tracked and reported; documented by each applicable release so that an OIT determination can be made if the asset meets IUS criteria. USCIS has determined that the best method for identifying IUS candidates is through monthly collection of contractor cost data for all releases in development, and will capitalize the cost of an IUS project if it is classified as a G-PP&E asset and meets the required criteria.

Definition: IUS is software that is purchased from commercial off-the-shelf (COTS) vendors or ready to use with little or no changes. Internal developed software is developed by employees of USCIS, including new software and existing or purchased software that is modified with or without a contractor's assistance. Contractor-developed software is used to design, program, install, and implement, including new software and the modification of existing or purchased software and related systems, solely to meet the entity's internal or operational needs.

Invoicing and Reporting: The contractor shall identify, capture, log, track and report the costs of IUS associated with each specific release. IUS Software is typically release centric and includes the application and operating system programs, procedures, rules, and any associated documentation pertaining to the operation of a computer system or program.

The contractor shall, after OIT's determination on whether or not the release meets the capitalization criteria, support OIT's reporting of costs incurred for the project or release, as required. The contractor shall provide the nature and cost of work completed within the relevant period. Costs considered part of IUS activities include systems administration, systems engineering, and program management. The Contractor shall provide the total cost, itemized by release and include the total sum of all applicable IUS activities. At the contractor's discretion, this information may be submitted, either as an attachment or as an itemized line item within the monthly invoices, as outlined in *Table 2: Deliverables Schedule.* For information purposes, the following activities within the development lifecycle have been identified as IUS reportable costs by the USCIS Management Directive No. 128-001:

1) Design: System Design: Design System, Update System Test Plan, Update Security Test Plan, Update Project Plan, Update Business Case, Conduct Critical Design Review and Issue Memo.

2) Programming/Construction: Establish Development Environment, Create or Modify Programs, Conduct Unit & Integration Testing, Develop Operator's Manual, Update Project Plan, Update Business Case, Migration Turnover/Test Readiness Review, Prepare Turnover Package, Develop Test Plans, Migration Turnover/Issue Test Readiness Memo

3) Testing
a. Acceptance Testing: Develop Security Test Report, Issue Security Certification, Develop System Documentation, Conduct User Acceptance Testing, Update Project Plan, Update Business Case, Conduct Production Readiness Review, Develop Implementation Plan, Issue Production Readiness Review Memo.
b. Coding
c. Installation to hardware
d. Testing, including parallel processing phase
4) Implementation Activities: Implementation/Transition: Security Accreditation(initial system accreditation only), Issue Implementation Notice, Parallel Operations, Update Project Plans, Update Business Case, Conduct Operational Readiness Review, Issue Operational Readiness Memo.
5) In addition, these cost shall contain, if not already itemized in the attachment (PER)or the invoice, the following additional costs information: Full cost (i.e., direct and indirect costs) relating to software development phase; Travel expenses by employees/contractor directly associated with developing software; Documentation Manuals; COTS purchases.

Attachment 4

SECTION 508 APPLICABLE EIT ACCESSIBILITY STANDARDS

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public who have disabilities must have access to and use of information and data that is comparable to Federal employees and members of the public without disabilities. All products, platforms, and services delivered as part of this work statement that are by definition ICT or contain ICT shall conform to the Revised 508 Standards, which are located at 36 C.F.R. § Appendices A, C, and D, and available at https://www.gpo.gov/fdsys/pkg/CFR-2017-title36-vol3/pdf/CFR-2017-title36-vol3-part1194.pdf.

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

Section 508 Applicable EIT Accessibility Standards

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

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

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

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

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

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

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): Modernized DevOps Sec

Applicable Exception: N/A **Authorization #:** N/A

Applicable Functional Performance Criteria: Does not apply

Applicable 508 requirements for software features and components: Does not apply

Applicable 508 requirements for hardware features and components: Does not 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. 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.

4. 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.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]