


SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS <small>OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30</small>				1. REQUISITION NUMBER OIT196001		PAGE OF 1 63	
2. CONTRACT NO. 47QTCK18D0015		3. AWARD/ EFFECTIVE DATE		4. ORDER NUMBER 70SBUR19F00000072		5. SOLICITATION NUMBER 70SBUR19R00000026	
						6. SOLICITATION ISSUE DATE 03/28/2019	
7. FOR SOLICITATION INFORMATION CALL:		a. NAME CELINA HEMINGWAY		b. TELEPHONE NUMBER (No collect calls) 802-872-4536		8. OFFER DUE DATE/LOCAL TIME	
9. ISSUED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403		CODE CIS		10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR <input type="checkbox"/> SET ASIDE: % FOR: <input type="checkbox"/> SMALL BUSINESS <input type="checkbox"/> HUBZONE SMALL BUSINESS <input type="checkbox"/> SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS <input type="checkbox"/> WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM <input type="checkbox"/> EDWOSB <input type="checkbox"/> 8(A) NAICS: 541519 SIZE STANDARD: \$27.5			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED <input checked="" type="checkbox"/> SEE SCHEDULE		12. DISCOUNT TERMS Net 30		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b. RATING	
15. DELIVER TO Department of Homeland Security US Citizenship & Immigration Svcs Office of Information Technology 111 Massachusetts Ave, NW Suite 5000 Washington DC 20529		CODE HQOIT		16. ADMINISTERED BY USCIS Contracting Office Department of Homeland Security 70 Kimball Avenue South Burlington VT 05403		14. METHOD OF SOLICITATION <input type="checkbox"/> RFQ <input type="checkbox"/> IFB <input type="checkbox"/> RFP	
17a. CONTRACTOR/ OFFEROR AGILE DEFENSE INC 11250 WAPLES MILL RD SOUTH TOWER SUITE 430 FAIRFAX VA 220307400		CODE [REDACTED] FACILITY CODE		18a. PAYMENT WILL BE MADE BY See Invoicing Instructions		CODE WEBVIEW	
TELEPHONE NO.				18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED <input type="checkbox"/> SEE ADDENDUM			
<input type="checkbox"/> 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER							
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES			21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: [REDACTED] Agile Software Development with Pair Programming Period of Performance is a six(6) month base with three(3) twelve(12) month options. AAP Number: none Accounting Info: ITDIDIT CMO EP 20-05-00-000 23-20-0600-00-00-00-00 GE-25-86-00 000000 Period of Performance: 04/15/2019 to 10/14/2022 Continued ... (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]	
<input type="checkbox"/> 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA <input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4, FAR 52.212-5 IS ATTACHED. ADDENDA				<input type="checkbox"/> ARE <input type="checkbox"/> ARE NOT ATTACHED. <input type="checkbox"/> ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED.			
<input type="checkbox"/> 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.				<input checked="" type="checkbox"/> 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 TERMS:			
30a. SIGNATURE OF OFFEROR/CONTRACTOR				31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) 			
30b. NAME AND TITLE OF SIGNER (Type or print)		30c. DATE SIGNED		31b. NAME OF CONTRACTING OFFICER (Type or print) Christopher C. Hatin		31c. DATE SIGNED 04/15/2019	

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	6 Month Base POP 4/15/2019 - 10/14/2019				
0001	FFP CLIN: Project Coordinator (as described in section 4 of the SOW).		MO		
0002	T&M CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), Section 4, to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Not to Exceed Amount:		EA		
0002 AA	Product Manager (as described in section 4 of the SOW) (Not Separately Priced) FOB: Destination		HR		
0002 AB	Designer(as described in section 4 of the SOW) (Not Separately Priced) Continued ...		HR		

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 <input type="checkbox"/> COMPLETE <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	37. CHECK NUMBER
<input type="checkbox"/> PARTIAL <input type="checkbox"/> 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

CONTINUATION SHEET

 REFERENCE NO. OF DOCUMENT BEING CONTINUED
 47QTCK18D0015/70SBUR19F00000072

 PAGE OF
 3 63

 NAME OF OFFEROR OR CONTRACTOR
 AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	FOB: Destination				
0002 AC	Developer (as described in section 4 of the SOW)		HR		
	(Not Separately Priced)				
	FOB: Destination				
0002 AD	Architect (as described in section 4 of the SOW)		HR		
	(Not Separately Priced)				
	FOB: Destination				
0002 AE	Platform Reliability Engineer (as described in section 4 of the SOW)		HR		
	(Not Separately Priced)				
	FOB: Destination				
0003	T&M CLIN: Travel (as described in section 7 of the SOW)		LO		
	Optional Surge CLINs for execution during 6 month base POP: 4/15/2019 - 10/14/2019				
0004	FFP Optional Surge CLIN: Project Coordinator as described in the SOW section 4. Amount: (Option Line Item) Anticipated Exercise Date: 0 Days After Award		MO		0.00
0005	T&M Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) section 4 to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Continued ...		EA		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
4 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Not to Exceed Amount: XXXXXXXXXX Amount: XXXXXXXXXX (Option Line Item) Anticipated Exercise Date: 0 Days After Award				
0005 AA	Optional Surge CLIN: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
0005 AB	Optional Surge CLIN: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
0005 AC	Optional Surge CLIN: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
0005 AD	Optional Surge CLIN: Architect (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
0005 AE	Optional Surge CLIN: Platform Reliability Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Continued ...	XXXX	HR		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

47QTCK18D0015/70SBUR19F00000072

PAGE OF

5

63

NAME OF OFFEROR OR CONTRACTOR

AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination				
0005 AF	Optional Surge CLIN: Agile Practice Leadership Enablement (APLE) (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
0005 AG	Optional Surge CLIN: Designated Support Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination 12 Month OPTION I POP 10/15/2019 - 10/14/2020		HR		0.00
1001	FFP CLIN Option I: Project Coordinator (as described in section 4 of the SOW). Amount: (Option Line Item) Anticipated Exercise Date: 10/14/2019		MO		0.00
1002	T&M CLIN Option I: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW, section 4, to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Not to Exceed Amount Amount: (Option Line Item) Anticipated Exercise Date: 10/14/2019 Continued ...		EA		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
6 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1002 AA	Option I: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 10/14/2019 (Not Separately Priced) FOB: Destination		HR		0.00
1002 AB	Option I: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 10/14/2019 (Not Separately Priced) FOB: Destination		HR		0.00
1002 AC	Option I: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 10/14/2019 (Not Separately Priced) FOB: Destination		HR		0.00
1003	T&M CLIN Option I: Travel (as described in section 7 of the SOW) Amount: (Option Line Item) Anticipated Exercise Date: 10/14/2019 Optional Surge CLINs for execution during Option I 12 month POP: 10/15/2019 - 10/14/2020		LO		0.00
1004	FFP Optional Surge CLIN: Project Coordinator (as described in section 4 of the SOW). Amount: (Option Line Item) Anticipated Exercise Date: 0 Days After Award		MO		0.00
1005	T&M Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), Section 4, Continued ...		EA		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
7 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Not to Exceed Amount: ██████████ Amount: ██████████ (Option Line Item) Anticipated Exercise Date: 0 Days After Award				
1005 AA	Optional Surge CLIN: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	████	HR		0.00
1005 AB	Optional Surge CLIN: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	████	HR		0.00
1005 AC	Optional Surge CLIN: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	████	HR		0.00
1005 AD	Optional Surge CLIN: Architect (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination Continued ...	████	HR		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

47QTCK18D0015/70SBUR19F00000072

PAGE OF

8

63

NAME OF OFFEROR OR CONTRACTOR

AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
1005 AE	Optional Surge CLIN: Platform Reliability Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
1005 AF	Optional Surge CLIN: Agile Practice Leadership Enablement (APLE) (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
1005 AG	Optional Surge CLIN: Designated Support Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination 12 Month OPTION II POP 10/15/2020 - 10/14/2021		HR		0.00
2001	FFP CLIN Option II: Project Coordinator (as described in section 4 of the SOW). Amount: (Option Line Item) Anticipated Exercise Date: 10/14/2020		MO		0.00
2002	T&M CLIN Option II: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), section 4, to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Continued ...		EA		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
9 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Attachment 1 - Established Rates and Prices Not to Exceed Amount: [REDACTED] Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date:10/14/2020				
2002 AA	Option II: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2020 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
2002 AB	Option II: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2020 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
2002 AC	Option II: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2020 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
2003	T&M CLIN Option II: Travel Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date:10/14/2020 Optional Surge CLINs for execution during Option II 12 month POP: 10/15/2020 - 10/14/2021	[REDACTED]	LO	[REDACTED]	0.00
2004	FFP Optional Surge CLIN: Project Coordinator (as described in section 4 of the SOW). Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date: 0 Days After Award Continued ...	[REDACTED]	MO	[REDACTED]	0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
10 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
2005	T&M Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), section 4, to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Not to Exceed Amount: XXXXXXXXXX Amount: XXXXXXXXXX (Option Line Item) Anticipated Exercise Date: 0 Days After Award	XXXX	EA	XXXXXXXXXX	0.00
2005 AA	Optional Surge CLIN: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
2005 AB	Optional Surge CLIN: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
2005 AC	Optional Surge CLIN: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination	XXXX	HR		0.00
2005 AD	Optional Surge CLIN: Architect (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Continued ...	XXXX	HR		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

47QTCK18D0015/70SBUR19F00000072

PAGE OF

11

63

NAME OF OFFEROR OR CONTRACTOR

AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination				
2005 AE	Optional Surge CLIN: Platform Reliability Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
2005 AF	Optional Surge CLIN: Agile Practice Leadership Enablement (APLE) (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
2005 AG	Optional Surge CLIN: Designated Support Engineer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination 12 Month OPTION III POP 10/15/2021 - 10/14/2022		HR		0.00
3001	FFP CLIN Option III: Project Coordinator (as described in section 4 of the SOW) Amount: (Option Line Item) Anticipated Exercise Date: 10/14/2021		MO		0.00
3002	T&M CLIN Option III: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), section 4, to be provided on a T&M basis. The Continued ...		EA		0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

47QTCK18D0015/70SBUR19F00000072

PAGE OF

12

63

NAME OF OFFEROR OR CONTRACTOR

AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Sub-CLINs are priced in accordance with Attachment 1 - Established Rates and Prices Not to Exceed Amount: [REDACTED] Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date:10/14/2021				
3002 AA	Option III: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2021 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
3002 AB	Option III: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2021 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
3002 AC	Option III: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date:10/14/2021 (Not Separately Priced) FOB: Destination	[REDACTED]	HR		0.00
3003	T&M CLIN Option III: Travel (as described in section 7 of the SOW) Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date:10/14/2021 Optional Surge CLINs for execution during Option III 12 month POP: 10/15/2021 - 10/14/2022	[REDACTED]	LO	[REDACTED]	0.00
3004	FFP Optional Surge CLIN: Project Coordinator (as described in section 4 of the SOW) Continued ...	[REDACTED]	MO	[REDACTED]	0.00

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED
47QTCK18D0015/70SBUR19F00000072PAGE OF
13 63NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date: 0 Days After Award				
3005	T&M Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW), section 4, to be provided on a T&M basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW. Not to Exceed Amount: [REDACTED] Amount: [REDACTED] (Option Line Item) Anticipated Exercise Date: 0 Days After Award		EA	[REDACTED]	0.00
3005 AA	Optional Surge CLIN: Product Manager (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
3005 AB	Optional Surge CLIN: Designer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
3005 AC	Optional Surge CLIN: Developer (as described in section 4 of the SOW) Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination		HR		0.00
3005 AD	Optional Surge CLIN: Architect (as described in section 4 of the SOW) Continued ...		HR		0.00

NAME OF OFFEROR OR CONTRACTOR
AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination				
3005 AE	Optional Surge CLIN: Platform Reliability Engineer (as described in section 4 of the SOW)		HR		0.00
	Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination				
3005 AF	Optional Surge CLIN: Agile Practice Leadership Enablement (APLE) (as described in section 4 of the SOW)		HR		0.00
	Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination				
3005 AG	Optional Surge CLIN: Designated Support Engineer (as described in section 4 of the SOW)		HR		0.00
	Amount: \$0.00 (Option Line Item) Anticipated Exercise Date: 0 Days After Award (Not Separately Priced) FOB: Destination . . This order is subject to the terms and conditions of the Alliant 2 contract number 47QTCK18D0015 Part II - Contract Clauses Part III - Statement of Work Attachment 1 - Established rates and Prices Attachment 2 - Brand Name Justification Continued ...				

CONTINUATION SHEET

REFERENCE NO. OF DOCUMENT BEING CONTINUED

47QTCK18D0015/70SBUR19F00000072

PAGE OF

15

63

NAME OF OFFEROR OR CONTRACTOR

AGILE DEFENSE INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The total amount of award: [REDACTED] The obligation for this award is shown in box 26.				

Part II-Contract Clauses

1. CONTRACT CLAUSES:

This order is subject to the Alliant 2 unrestricted track Contract number 47OTCK18D0015

Federal Acquisition Regulation (FAR) clauses incorporated by reference

52.204-19 Incorporation by Reference of Representations and Certifications	(Dec 2014)
52.224-3 Privacy Training	(Jan 2017)
52.232-39 Unenforceability of Unauthorized Obligations	(Jun 2013)
52.237-3 Continuity of Services	(Jan 1991)

Federal Acquisition Regulation (FAR) clauses incorporated in full text

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

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

“Internal confidentiality agreement or statement” means a confidentiality agreement or any other written statement that the contractor requires any of its employees or subcontractors to sign regarding nondisclosure of contractor information, except that it does not include confidentiality agreements arising out of civil litigation or confidentiality agreements that contractor employees or subcontractors sign at the behest of a Federal agency.

“Subcontract” means any contract as defined in subpart 2.1 entered into by a subcontractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes but is not limited to purchase orders, and changes and modifications to purchase orders.

“Subcontractor” means any supplier, distributor, vendor, or firm (including a consultant) that furnishes supplies or services to or for a prime contractor or another subcontractor.

(b) The Contractor shall not require its employees or subcontractors to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting waste, fraud, or abuse related to the performance of a Government contract to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information (e.g., agency Office of the Inspector General).

(c) The Contractor shall notify current employees and subcontractors that prohibitions and restrictions of any preexisting internal confidentiality agreements or statements covered by this

clause, to the extent that such prohibitions and restrictions are inconsistent with the prohibitions of this clause, are no longer in effect.

(d) The prohibition in paragraph (b) of this clause does not contravene requirements applicable to Standard Form 312 (Classified Information Nondisclosure Agreement), Form 4414 (Sensitive Compartmented Information Nondisclosure Agreement), or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(e) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015, (Pub. L. 113-235), and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions) use of funds appropriated (or otherwise made available) is prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(f) The Contractor shall include the substance of this clause, including this paragraph (f), in subcontracts under such contracts.

(End of clause)

52.217-9 Option to Extend the Term of the Contract

(Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 15 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the task order expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 42 months.

(End of clause)

Homeland Security Acquisition Regulation (HSAR) clauses

Incorporated in full text

3052.203-70 Instructions for Contractor Disclosure of Violations.

(SEP 2012)

When making a written disclosure under the clause at FAR 52.203-13, paragraph (b)(3), the Contractor shall use the Contractor Disclosure Form at <http://www.oig.dhs.gov> and submit the disclosure electronically to the Department of Homeland Security Office of Inspector General. The Contractor shall provide a copy of the disclosure to the Contracting Officer by email or facsimile on the same business day as the submission to the Office of Inspector General. The Contractor shall provide the Contracting Officer a concurrent copy of any supporting materials submitted to the Office of Inspector General.

(End of clause)

3052.204-71 Contractor Employee Access Alt I**(SEP 2012)**

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the Statement of work (SOW), other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- (1) There must be a compelling reason for using this individual as opposed to a U. S. citizen; and
- (2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

3052.205-70 Advertisements, Publicizing Awards, and Releases.**ALTERNATE I
(SEP 2012)**

- (a) The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

All advertisements, releases, announcements, or other publication regarding this contract or the agency programs and projects covered under it, or the results or conclusions made pursuant to performance, must be approved by the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity, release, or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer.

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

- (a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate.
- (b) Before replacing any of the specified individuals or facilities, the contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The contractor shall not replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Contract are:

Project Coordinator

(End of clause)

DHS FAR Class Deviation 17-03 - 52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) *Definition.* As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A-130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

- (1) Have access to a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or
- (3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing *Privacy at DHS: Protecting Personal Information* accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

- (1) Have access to a system of records;
- (2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or
- (3) Design, develop, maintain, or operate a system of records.

(End of clause)

Local Clauses

ADDITIONAL INVOICING INSTRUCTIONS

(a) In accordance with FAR Part 32.905, all invoices submitted to USCIS for payment shall include the following:

- (1) Name and address of the contractor.
 - (2) Invoice date and invoice number.
 - (3) Contract number or other authorization for supplies delivered or services performed (including order number and contract line item number).
 - (4) Description, quantity, unit of measure, period of performance, unit price, and extended price of supplies delivered or services performed.
 - (5) Shipping and payment terms.
 - (6) Name and address of contractor official to whom payment is to be sent.
 - (7) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
 - (8) Taxpayer Identification Number (TIN).
- (b) Invoices not meeting these requirements will be rejected and not paid until a corrected invoice meeting the requirements is received.
- (c) USCIS' preferred method for invoice submission is electronically. Invoices shall be submitted in Adobe pdf format with each pdf file containing only one invoice. The pdf files shall be submitted electronically to USCISInvoice.Consolidation@ice.dhs.gov with each email conforming to a size limit of 500 KB.
- (d) If a paper invoice is submitted, mail the invoice to:
- USCIS Invoice Consolidation
PO Box 1000
Williston, VT 05495

PERFORMANCE REPORTING

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

FINAL PAYMENT

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

GOVERNMENT-FURNISHED PROPERTY

(a) Upon the Contractor's request that a Contractor employee be granted access to a Government automated system and the Government's approval of the request, the Government will issue the following equipment to that employee by hand receipt:

Equipment	QTY	Unit	unit acquisition
HP Zbook 17 G4 Mobile	6	EA	\$8,529 - \$17,058
MacBook Pro	6	EA	\$7,797 - \$15,594

(b) The Government will issue this equipment only to contractor employees that have a successful EOD.

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

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

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

NOTICE TO PROCEED (NTP)

Full contract performance shall begin commencing on the date specified by the Contracting Officer in the Notice to Proceed directive.

(a) Performance of the work requires unescorted access to Government facilities or automated systems, and/or access to sensitive but unclassified information. The Security Requirements below applies. The Contractor is responsible for providing employees who will receive favorable entry-on-duty (EOD) decisions and suitability determinations. A Government decision not to grant a favorable EOD decision or suitability determination, or to withdraw or terminate such decision or termination, shall not excuse the Contractor from performance of obligations under this task order.

(b) The Contractor may submit background investigation packages upon issuance of the task order, so that it has adequate employees ready for the time when the Government issues the notice to proceed.

(c) The Government intends to issue a notice to proceed between 30 and 60 days after task order award.

A NTP will not be issued by the Contracting Officer until such time as satisfactory suitability determinations have been received and successfully processed by the USCIS Office of Security & Integrity for all contractor staff.

Regarding staffing, the contractor shall request through the COR to the CO to receive a Notice to Proceed once all contractor personnel for a particular CLIN or sub-CLIN have a valid EOD. If all required EOD dates are received prior to the 15th of the month, the NTP shall include the entire month in which the request was made. If EOD dates are received and an NTP requested after the 15th of the month, the NTP start cite a start date aligning with the next full month.

For those CLINs or sub-CLINs not included in the initial full performance NTP, the duration of their performance period shall be such that it ends at the same time as those started with the initial full performance NTP. Individual CLINs or sub-CLINs shall not have staggered end dates. An NTP issued after the initial full performance NTP shall capture the revised performance period per each CLIN or sub-CLIN associated with the Notice.

POSTING OF CONTRACT (OR ORDER) IN FOIA READING ROOM

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

HSAR Class Deviation 15-01 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

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

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

“Sensitive Information” is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

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

“Sensitive Personally Identifiable Information (SPII)” is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver’s license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual’s name or other unique identifier plus one or more of the following elements:

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

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

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

- (1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
- (2) DHS Sensitive Systems Policy Directive 4300A
- (3) DHS 4300A Sensitive Systems Handbook and Attachments
- (4) DHS Security Authorization Process Guide
- (5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
- (6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
- (7) DHS Information Security Performance Plan (current fiscal year) (8) DHS Privacy Incident

Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at <http://csrc.nist.gov/groups/STM/cmvp/standards.html>

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at <http://csrc.nist.gov/publications/PubsSPs.html>

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

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

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

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

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

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

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

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

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

(iii) *Support the completion of the Privacy Threshold Analysis (PTA) as needed.* As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at <http://www.dhs.gov/privacy-compliance>.

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

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

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

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the

Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan*, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

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

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

- (i) Data Universal Numbering System (DUNS);
- (ii) Contract numbers affected unless all contracts by the company are affected;
- (iii) Facility CAGE code if the location of the event is different than the prime contractor location;
- (iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);
- (v) Contracting Officer POC (address, telephone, email);
- (vi) Contract clearance level;
- (vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
- (viii) Government programs, platforms or systems involved;
- (ix) Location(s) of incident;
- (x) Date and time the incident was discovered;
- (xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
- (xii) Description of the Government PII and/or SPII contained within the system;
- (xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
- (xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

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

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

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

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

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

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

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

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

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

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

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

(2) Provide credit monitoring services to individuals whose data was under the control of the

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

- (i) Triple credit bureau monitoring;
 - (ii) Daily customer service;
 - (iii) Alerts provided to the individual for changes and fraud; and
 - (iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or
- (3) Establish a dedicated call center. Call center services shall include:
- (i) A dedicated telephone number to contact customer service within a fixed period;
 - (ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
 - (iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
 - (iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
 - (v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
 - (vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

(End of clause)

HSAR Class Deviation 15-01 INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)

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

(b) **Security Training Requirements.**

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later

than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at <http://www.dhs.gov/dhs-security-and-training-requirements-contractors>. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

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

(End of clause)

DHS ENTERPRISE ARCHITECTURE COMPLIANCE

“All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the Government intends to:

- a) All developed solutions and requirements shall be compliant with the Homeland Security Enterprise Architecture (HLS EA).
- b) All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- c) 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 Model and Enterprise Architecture Information Repository.
- d) 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.
- e) 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. ”

CAPITALIZED PROPERTY, PLANT & EQUIPMENT (PP&E) ASSETS INTERNAL USE SOFTWARE (IUS)

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.

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 3: Resource Expenditure Format and Figure 1: Resource Expenditure Format. 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:

- a) 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.
- b) 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
- c) Testing
 - i. 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.
 - ii. Coding
 - iii. Installation to hardware
 - iv. Testing, including parallel processing phase
- d) 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.
- e) 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.

SECURITY REQUIREMENTS

GENERAL

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

SUITABILITY DETERMINATION

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information based upon the results of a background investigation.

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

BACKGROUND INVESTIGATIONS

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

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

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

1. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
2. FD Form 258, "Fingerprint Card" (2 copies)
3. Form DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
4. DHS Form 11000-25 "Contractor Fitness/Security Screening Request Form"
5. USCIS Continuation Page to DHS Form 11000-25
6. OF 306, Declaration for Federal Employment (approved use for Federal Contract Employment)
7. 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.

The Contractor must agree that each employee working on this contract will have a Social Security Card issued by the Social Security Administration.

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)
- **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.

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.

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): Code

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

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components(including Internet and Intranet website; Electronic surveys; Electronic reports;): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

Applicable 508 requirements for software features and components (including Web, desktop, server, mobile client applications;): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

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

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

Item that contains Information and Communications Technology (ICT): Documentation

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

Applicable Functional Performance Criteria: All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results to achieve substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

Applicable 508 requirements for electronic content features and components(including Electronic documents; Electronic reports;): All requirements in E205 apply, including all WCAG Level AA Success Criteria Apply

Applicable 508 requirements for software features and components (including Electronic content and software authoring tools and platforms;): All requirements in Chapter 5 apply, including all WCAG Level AA Success Criteria, 502 Interoperability with Assistive Technology, 503 Application

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

Applicable 508 requirements for support services and documentation: All requirements in Chapter 6 apply

2. When providing installation, configuration or integration services for ICT, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.
3. When developing or modifying ICT for the government, the contractor shall ensure the ICT fully conforms to the applicable Section 508 Standards. When modifying a commercially available or government-owned ICT, the contractor shall not reduce the original ICT Item's level of Section 508 conformance.
4. When developing or modifying web and software ICT, the contractor shall demonstrate Section 508 conformance by providing Section 508 test results based on the versions of the DHS Trusted Tester Methodology currently approved for use, as defined at <https://www.dhs.gov/compliance-test-processes>. The contractor shall use testers who are certified by DHS on how to use the DHS Trusted Tester Methodology (e.g "DHS Certified Trusted Testers") to conduct accessibility testing. Information on how testers can become certified is located at <https://www.dhs.gov/publication/trusted-tester-resources>.

5. When developing or modifying ICT that are delivered in an electronic Microsoft Office or Adobe PDF format, the contractor shall demonstrate conformance by providing Section 508 test results based on the Accessible Electronic Documents – Community of Practice (AED COP) Harmonized Testing Guidance at <https://www.dhs.gov/compliance-test-processes>.
6. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the applicable revised Section 508 Standards for each ICT.
7. 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.

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

Section 508 Supplemental language

This action appears to include software development. Based on Management Instruction (MI) 003, it should have a requirement for the Contractor to provide Trusted Testers. Please include these two items in a supplemental Section 508 task or requirement:

1. The Contractor must provide a DHS OAST Trusted Tester certified to current test standards for each team of one or more developers that creates Information and Communications Technology (ICT), or content to be hosted on ICT, within 90 days of award. 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.

Part III – Statement of Work



**U.S. Citizenship
and Immigration
Services**

Office of Information Technology (OIT)

Digital Innovation & Development - DID(it)

Agile Software Development With Pair Programming

Statement of Work (SOW)

Statement of Work

1. Title of Project

Digital Innovation and Development – DID(it) – Agile Software Development with Pair Programming

2. Project Background

The USCIS Office of Information Technology, Systems Development Division, Digital Innovation & Development (DID(it)) Branch provides an innovative development approach and technology stack for development of small to enterprise web and database applications at the local and headquarters levels consistent with the USCIS enterprise architecture models.

DID(it) drives innovation at USCIS by evaluating open source and “bleeding-edge” technology, processes, and practices, and helps determine their usability at USCIS through small application trial efforts that may grow into larger IT solutions and new USCIS OIT standards.

Specifically, DID(it) reviews, experiments with, and potentially adopts different agile software development practices, processes, and techniques in order to drive innovation. New practices, processes, and techniques should promote adaptive planning, evolutionary development, early delivery, continuous improvement, and encourage rapid and flexible response to change. One such agile software development technique is pair programming which has two programmers work together on one project/workstation. The benefits of pair programming are continuous code learning, improved code quality, improved design quality, stronger communication, and team-building. Overall, USCIS realizes value by having products delivered faster and with higher quality when using improved agile software development practices.

3. Scope

The Contractor shall provide expert, brand name Pivotal Labs, consulting and development services by conducting the activities described in each of the individual Tasks in accordance with **Section 4.0** of this SOW. In support of these activities, the Contractor shall be responsible for documenting their efforts via contract deliverables delivered in accordance with **Section 6.0** of this SOW and coordinated through the DID(it) COR.

Expert consulting and development services shall cover agile software development DevOps, and Platform-as-a-Service (PaaS) Pivotal Cloud Foundry (PCF) industry best practices, to include processes, tools, and techniques.

Expert consulting and development services shall provide best practices that result in improvements in, but not limited to, the following areas:

- Increase flow of work (i.e. value delivery) while maintaining quality, reliability, and security.

- Enable lean startup and lean product management practices and techniques that focus on quick value delivery to the customer. Using a Build Measure Learn process, shall be able to turn ideas into products, measure how customers respond, and then learn whether to pivot or persevere.
- Enable user-centered design and other user research practices and techniques that results in end-user driven requirements, user interface prototyping and development, and business layer development and validation.
- Enable optimal architecture design patterns such as microservices or other loosely-coupled Service-Oriented Architectures (SOAs). The architecture pattern should provide a way to optimize the design of central data components such as employee models, organizational models, and case management service models. Optimal architecture patterns should be applied to both new and existing solutions.
- Enable a software development platform strategy that increases efficiency and automation throughout the software development process. The platform strategy should include the implementation and enablement of a Platform-as-a-Service (PaaS) solution Pivotal Cloud Foundry (PCF).
- Enable practices and techniques that ensure quality, reliability and security are a part of the software delivery value stream.
- Increase flow of feedback so that fast, frequent, high quality information flow throughout the value stream and organization which includes feedback and feedforward loops.
 - Improve feedback loops throughout the value stream.
 - Define, measure, and report on business value metrics.
 - Create telemetry to enable seeing and solving problems (both business and system).
 - Collect data and capture effective metrics in the business logic, application, and environment layers.
 - Analyze telemetry to better anticipate problems and achieve goals.
 - Identify tools or software solutions that facilitate the increased flow of feedback (systems monitoring, customer feedback, and other feedback tools).
- Acceleration of organizational learning and improvement through continual learning and experimentation.
 - Build a high-trust culture and a scientific approach to organizational improvement.
 - Enable and involve learning into daily work to ensure continuous learning and improvement.
 - Convert local improvement discoveries into global improvements.
 - Improve internal coaching and enablement in order to spread expertise across the organization.
 - Improve organization strategies such as organizing as a Market Oriented Organization that is optimized in responding to customer needs.

Expert consulting and development services provide high-performing teams that will work alongside The DID(it) Team using workforce pair techniques, such as pair programming, to learn and utilize agile software development and DevOps industry best practices.

4. Specific Tasks

4.1 Task 1: Project Coordination

The Contractor shall provide project coordination support for planning and completion of all contractor support activities in accordance with **Section 6** and **Section 7** of this SOW. This will be a FFP per month CLIN, but it is estimated that the Project Coordination will require 80 hours per year.

4.2 Task 2: Agile Software Development

The objectives of agile software development support are to be provided through Brand name Pivotal Labs services and include the following:

- Provide consulting services to the DID(it) team that includes agile software development and DevOps industry best practices, to include processes, tools, and techniques.
- Provide consulting and development services in support Platform-as-A-Service (PaaS) solution Pivotal Cloud Foundry (PCF).
- Provide development support services to the DID(it) Team that results in high-quality shippable code and Minimum Viable Products (MVP) with a focus on Application Programming Interfaces (API), data services, code reuse and decoupling, and extending existing functionality.
- Provide consultation and development support services for the DID(it) standard toolset engaging in mobile first development using open-source and innovated technologies (such as Ruby on Rails, HTML5, Cascading Style Sheets, JavaScript frameworks, Responsive Web Design, etc.) and agile methodologies (such as Test Driven Development, Behavior Driven Development, Automated Testing, Continuous Integration, Continuous Delivery, etc.), and other agile development practices.
- Provide consultation and development services for identifying and developing optimal architecture design patterns such as microservices or other loosely-coupled service-oriented architecture (SOA) models.
- Provide consulting and development services for identifying and implementing an optimal software development platform strategy that increases the speed and efficiency in software delivery.
- Evaluate new tools, software products, and open source technologies, and provide hands-on enablement of new tools, software, and technologies.

The Contractor shall:

- Work alongside the federal team using such techniques as pair programming.
- Provide Brand name Pivotal Labs enablement of the following roles: 1) Product Manager; 2) Designer; 3) Developer; 4) Architect 5) PCF Platform Reliability Engineer; 6) Agile Practice Leadership Enablement (APIE) and 7) Designated Support Engineer.
- Provide hands-on support and enablement of Pivotal Cloud Foundry (PCF).
- Provide Minimum Viable Product (MVP) for data services and components that will be utilized by new and existing USCIS applications. Examples are document services, employee management services, and organizational management services.
- Analyze software requirements as scoped during planning sessions and provide Minimum Viable Products (MVP). Perform analysis, design, coding, testing, implementation, and maintenance of software solutions.

Deliverables (**Section 6.0**) include: analysis of software requirements with recommended solutions; documentation to support analysis, design, coding, testing, hosting, implementation, and maintenance of software solutions.

Agile Software Development

5. Acceptable Quality Levels

Performance Measure or Standard	Target
PCF usage across portfolio.	100%
PCF platform availability and uptime.	100%
Agile software development best practices have been documented and taught to the federal development team through pair programming	100%
Requirement elicitation best practices and optimal design patterns have been documented and taught to the federal development team through pair programming	100%
Custom web-based applications have been developed, tested, and received product owner acceptance	100%

6. Deliverables

The primary deliverable of this task order is deployable application code and innovative solutions to USCIS. The contractor shall deliver this code (in conformance with procedures established by the DID(it) Team) throughout the period of performance for integration with an existing codebase in preparation for deployment.

Deliverables	Frequency	Format
Contract Kick Off Meeting Presentation	Once, within the first 15 days of contract award	A creative format to be determined and presented by the contract team
In-process application code	Continuously, with each build	Application source code
Shippable Application Code	Continuously, with each commit	Application source code and compiled code
Monthly Status Report & meeting providing a complete roll up of all contractor activities and costs associated ad hoc reporting as required by the COR or OIT Project Manager	Monthly	Report provided in Pdf, meeting will be held in-person, via teleconference, or video teleconference
Agile Development lifecycle documents, such as System Design Document (SDD), etc.	Each release	MS Word 2010
May include: user requirements definition, alternatives analyses, review assessments, web based	As requested	MS Word
May include: software requirements analyses and solutions, documentation to support analyses, design, coding, testing, hosting, implementation, and maintenance of software solutions.	As required	IAW Approved WP / Approved PP
May include : analyses of database requirements with recommended solutions, documentation to support analyses,	As required	IAW Approved WP / Approved PP
Test scripts	Continuously, with each commit	Application source code, MS Word 2010

May include: Test Plans (TPs), procedures, Test and Evaluation (T&E) reports, and documentation to support various stages of testing (e.g., unit, integration, system, performance, functional qualification, and acceptance) for all initial and updated increments/releases and components.	Continuously, with each build	IAW Approved WP / Approved PP
Monthly Capitalized property, Plant & Equipment Assets Internal Use Software required reporting	Monthly	MS Word 2010
Transition In Plan	To be provided at the Post Award Kickoff Meeting	
Transition Out Plan	To be provided 60 days prior to contract end date	

7. Task Order Administration Data

7.1 Place of Performance

The principal place of performance shall be at the contractor provided work site. The government may require some key personnel to be on-site at 111 Massachusetts Avenue NW, Washington, DC. Meetings will usually take place at OIT offices in the Washington, DC metropolitan area, including, but not limited to 20 Massachusetts Avenue, NW, and 111 Massachusetts Avenue, NW, Washington, DC.

7.2 Hours of Operation

Hours of operation are 8:00am to 5:00pm, Monday through Friday, excluding Government holidays.

- New Year's Day
- M.L. King's Birthday
- President's Day
- Memorial Day
- Independence Day
- Labor Day
- Columbus Day

- Veteran's Day
- Thanksgiving Day
- Christmas

Observance of such days by Government personnel shall not be reason for the contractor to request an additional period of performance, or entitlement of compensation except as set forth within this contract. When USCIS grants its employees "Liberal Leave," the contractor's employees are expected to work their normal hours.

7.3 Travel

The travel shall be proposed as T&M and approved by the COR prior to the initiation of any travel planning, the Contractor is responsible for obtaining COR approval (email is acceptable). The Contractor shall be reimbursed for travel in accordance with FAR Part 31 and Federal Travel Regulations, 41 Code of Federal Regulations (CFR). Upon completion of travel, all documentation associated with the respective travel shall be submitted with the invoices. The Government will not reimburse local travel within a 50-mile radius from the contractor's assigned duty station.

7.4 Post Award Meeting

The post award meeting will be scheduled by the CO as soon as possible after award. The purpose of the meeting is to identify primary points of contact and discuss scope, and tasks, in order to achieve a clear and mutual understanding of all contract requirements and to identify and resolve potential problems.

7.5 Technical Kickoff Meeting

The technical kickoff meeting at OIT HQ will take place after the CO issues the notice to proceed.

7.6 Transition-In

The contractor shall be responsible for the transition of all technical activities identified in this SOW. The technical activities, which shall be included as part of the transition-in, consist of:

- Inventory and orderly transfer of all Government Furnished Property, software and licenses.
- Transfer of documentation currently in process.
- Transfer of all software coding in process.
- Coordinating the body of work with the current contractor.

The contractor's Transition-In Plan shall be approved by USCIS OIT and shall contain a milestone schedule of events and system turnovers. The Transition-In Plan shall address transition of systems with no disruption in operational services. To ensure the necessary

continuity of services and to maintain the current level of support, the Government intends to retain services of the incumbent contractor for some or all of the transition-in period, as may be required. For the Transition-In Plan, the contractor shall include their staffing ramp-up approach and ensure that all FTEs billed on the task order are fully engaged in USCIS work and not idle while waiting for clearance(s)/badge(s).

At a minimum, the contractor's plan shall include their innovative and proactive approach to manage the following transition activities with the incumbent contractor and/or the Government:

- Assuming responsibility for current support services,
- Assuming ownership of historic data, documentation, processes, training, and tools
- Assuming user and system administration for all systems and tools
- Transferring assets
- Accepting the transfer of all compiled and un-compiled source code (all versions, updates, and patches)
- Obtaining access (keys, cards, security codes) and required training
- Conducting introduction/orientation activities

The contractor shall include their approach to provide analyses, validations, updates, and recommendations for enhancement to include, at a minimum:

- Inventory validation within 30 days after transition conclusion
- Plans and system analysis and update within 60 days after transition conclusion
- Other documentation analysis and update within 90 days after transition conclusion.

7.7 Transition-Out

The contractor shall provide a Transition-Out Plan which shall describe all required transition out activities necessary to ensure a successful and timely transition to a successor (either a Government entity, another contractor, or to the incumbent contractor under a new contract/order). The Transition-Out Plan shall also include a project schedule based on days prior to contract expiration by which the contractor will execute the activities described in the Transition-Out Plan in coordination with the Government and the successor. The Transition-Out Plan should allow for no more than 30-days for completion of transition activities to the successor.

8 Government Furnished Property (GFP) / Information (GFI)

8.1 Government Furnished Property

- (a) Upon the contractor's request that a contractor employee be granted access to a Government automated system and the Government's approval of the request, the Government will issue the equipment identified in section 8 *Government Furnished Property*.
- (b) The contractor shall have a process to create and provide GFP reports and be accountable for an inventory process.

8.2 Government Furnished Information/Support

The Government information identified below will be furnished at the post award kickoff meeting.

Document Name	Publication Number/Applicable Web Site	Date
DID(it) Ruby on Rails Development Process Programming Guide	To be provided at the Post Award Kickoff Meeting	3 June 2014
DID(it) Portfolio Level Kanban Backlog	To be provided at the Post Award Kickoff Meeting	Ongoing
DID(it) Application Portfolio (Ruby and Legacy ColdFusion applications)	To be provided as needed	Ongoing
DID(it) Ruby Style Guide	To be provided at the Post Award Kickoff Meeting	13 November 2013
DID(it) Rails Style Guide	To be provided at the Post Award Kickoff Meeting	13 November 2013
DID(it) Playbook	To be provided at the Post Award Kickoff Meeting	Ongoing

9. Documentation

Documentation specific to USCIS that is developed during the course of the work performance will become property of the Government. Examples of such documentation are USCIS agile software development best practices, USCIS development pipeline automation best practices, and USCIS workflow specifications.

Established Rates and Prices							
		Description	CLIN Type	Quantity	Unit	Rate	Total
Base: 6 month POP 4/13/2019 - 10/14/2019							
	0001	Project Coordinator as described in the SOW section 4.	FFP	1	MO	\$ 100,000	\$ 100,000
	0002	Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M	1	EA	\$ 100,000	Cumulative total of CLINs 0002AA,AB,AC,AD,AE,AF and AG - Not to exceed amount: \$ 100,000
	0002AA	Product Manager		1	HR	\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0002AB	Designer		1	HR	\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0002AC	Developer		1	HR	\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0002AD	Architect		1	HR	\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0002AE	Platform Reliability Engineer		1	HR	\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0003	Travel - Not to exceed 100,000	T&M	1	LO		\$ 100,000
	0004	Optional Surge CLIN: Project Coordinator	FFP	1	MO	\$ 100,000	\$ 100,000
	0005	Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M	1	EA	\$ 100,000	Cumulative total of CLINs 0005AA,AB,AC,AD,AE,AF and AG - Not to exceed amount: 100,000
	0005AA	Optional Surge: Product Manager		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AB	Optional Surge: Designer		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AC	Optional Surge: Developer		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AD	Optional Surge: Architect		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AE	Optional Surge: Platform Reliability Engineer		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AF	Optional Surge: Agile Practice Leadership Enablement (APLE)		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
	0005AG	Optional Surge: Designated Support Engineer		1		\$ 100,000	NOT SEPARATELY PRICED (NSP)
		Total Base					\$ 1,000,000

Option I: 12 month POP 10/15/2019- 10/14/2020							
	1001	Project Coordinator as described in the SOW section 4.	FFP		MO	\$	
	1002	Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M		EA	\$	Cumulative total of CLINs 1002AA,AB,AC,AD,AE,AF and AG - Not to exceed amount:
	1002AA	Product Manager			HR	\$	NOT SEPARATELY PRICED (NSP)
	1002AB	Designer			HR	\$	NOT SEPARATELY PRICED (NSP)
	1002AC	Developer			HR	\$	NOT SEPARATELY PRICED (NSP)
	1003	Travel - Not to exceed	T&M		LO	\$	
	1004	Optional Surge CLIN: Project Coordinator	FFP		MO	\$	
	1005	Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M		EA	\$	Cumulative total of CLINs 1005AA,AB,AC,AD,AE,AF and AG - Not to exceed amount:
	1005AA	Optional Surge: Product Manager			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AB	Optional Surge: Designer			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AC	Optional Surge: Developer			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AD	Optional Surge: Architect			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AE	Optional Surge: Platform Reliability Engineer			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AF	Optional Surge: Agile Practice Leadership Enablement (APLE)			HR	\$	NOT SEPARATELY PRICED (NSP)
	1005AG	Optional Surge: Designated Support Engineer			HR	\$	NOT SEPARATELY PRICED (NSP)
	Total Option I					\$	

Option II: 12 month POP 10/15/2020- 10/14/2021							
	2001	Project Coordinator as described in the SOW section 4.	FFP CLIN		MO	\$	
	2002	Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M		EA	\$	Cumulative total of CLINs 2002AA,AB,AC,AD,AE,AF and AG - Not to exceed amount:
	2002AA	Product Manager			HR	\$	NOT SEPARATELY PRICED (NSP)
	2002AB	Designer			HR	\$	NOT SEPARATELY PRICED (NSP)
	2002AC	Developer			HR	\$	NOT SEPARATELY PRICED (NSP)
	2003	Travel - Not to exceed	T&M		LO	\$	
	2004	Optional Surge CLIN: Project Coordinator	FFP		MO	\$	
	2005	Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M		EA	\$	Cumulative total of CLINs 2005AA,AB,AC,AD,AE,AF and AG - Not to exceed amount:
	2005AA	Optional Surge: Product Manager			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AB	Optional Surge: Designer			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AC	Optional Surge: Developer			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AD	Optional Surge: Architect			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AE	Optional Surge: Platform Reliability Engineer			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AF	Optional Surge: Agile Practice Leadership Enablement (APLE)			HR	\$	NOT SEPARATELY PRICED (NSP)
	2005AG	Optional Surge: Designated Support Engineer			HR	\$	NOT SEPARATELY PRICED (NSP)
		Total Option II				\$	

Option III: 12 month POP 10/15/2021- 10/14/2022							
	3001	Project Coordinator as described in the SOW section 4.	FFP	■	MO	\$	■
	3002	Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M	■	EA	\$	■ 3002AA,AB,AC,AD,AE,AF and AG - Not to exceed amount: ■
	3002AA	Product Manager		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3002AB	Designer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3002AC	Developer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3003	Travel - Not to exceed ■	T&M	■	LO		\$ ■
	3004	Optional Surge CLIN: Project Coordinator	FFP	■	MO	\$	■
	3005	Optional Surge CLIN: Name brand Pivotal Labs Agile Software Development with Pair Programming services as described in Statement of Work (SOW) to be provided on a Labor Hour (LH) basis. The following sub-CLINs identify the associated Labor Categories (Time) and hours to perform the requirements of the SOW.	T&M	■	EA	\$	■ Cumulative total of CLINs 3005AA,AB,AC,AD,AE,AF and AG - Not to exceed amount: ■
	3005AA	Optional Surge: Product Manager		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AB	Optional Surge: Designer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AC	Optional Surge: Developer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AD	Optional Surge: Architect		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AE	Optional Surge: Platform Reliability Engineer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AF	Optional Surge: Agile Practice Leadership Enablement (APLE)		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
	3005AG	Optional Surge: Designated Support Engineer		■	HR	\$	■ NOT SEPARATELY PRICED (NSP)
		Total Option III					\$ ■
		Total Contract Value					\$ ■

Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

JEFO No.: FY19-0106

Date: February 12, 2019

PR Number: OIT196001

1. Agency and Contracting Activity. Identification of the agency and the contracting activity, and specific identification of the document as a "Justification for an Exception to Fair Opportunity."

The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS), Office of Contracting (OCON) prepared this justification for an exception to fair opportunity.

2. Nature and/or description of the action being approved.

USCIS/OCON intends to award a task order without considering other awardees under Alliant 2 Un-restricted track for Pivotal Labs Services. Alliant 2 is a DHS strategic sourcing multiple-award IDIQ contract vehicle. Pursuant to FAR 16.505(a)(4), restricting consideration to an item peculiar to one manufacturer (Pivotal Labs) (e.g., a particular brand-name, product, or a feature of a product that is peculiar to one manufacturer) must be justified. A brand-name item, even if available on more than one contract, is an item peculiar to one manufacturer.

3. A description of the supplies or services required to meet the agency's need (including the estimated value).

The requirement is for name brand Pivotal Labs subject matter expert consulting and development services. These services cover agile software development, Development Operations (DevOps), and the currently used Platform-as-a-Service (PaaS), called Pivotal Cloud Foundry (PCF). The Pivotal Labs development support and enablement through industry best practices, to include processes, tools, and techniques that makes the system not only operational, but utilized to its full potential.

These services shall provide the following:

- Provide a team with expert knowledge of PCF with skilled consulting and development abilities to work alongside the Digital Innovation and Development DID(it) team using such techniques as pair programming in order to enable the use of industry best practices.
- Provide the following roles: 1) Product Manager; 2) Product Designer; 3) Developer; 4) PCF Platform Reliability Engineer; and 5) Program Manager.
- Provide hands-on support, through pair programming alongside DID(it) staff, and enablement of Pivotal Cloud Foundry (PCF).
- Understanding of USCIS business domains in order to effectively discover business needs and business problems and to provide rapid and high-quality solutions through the analysis, design, coding, testing, implementation, and maintenance of software solutions.

JEFO No. FY19-0016

**Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)**

- Provide high-quality shippable code and Minimum Viable Products (MVP) for data services and components that will be utilized by new and existing USCIS applications.
- Provide hands-on support, on site, for the setup and implementation of new tools, software, and technologies while enabling the DID(it) Team to utilize industry best practices.

The Period of Performance will be a total of 42 months consisting of a 6 month base and three 12 month options.

Period	Total
Base (6 months)	\$
Option I (12 months)	\$
Option II (12 months)	\$
Option III (12 months)	\$
Total	\$

4. Identify the exception to fair opportunity and supporting rationale. Only one awardee is capable of providing the supplies required at the level of quality required because the supplies ordered are unique or highly specialized pursuant to FAR 16.505(b)(2)(i)(B) and is an item peculiar to one manufacturer:

DHS/USCIS/OCON intends to procure brand name Pivotal Labs Services DHS Alliant 2 un-restricted track in accordance with FAR 16.505(a)(4). The exception is based on FAR 16.505(b)(2)(i)(B) only one manufacturer is capable of providing Pivotal Labs Services at the level of quality required because Pivotal Labs Services is unique or highly specialized and peculiar to the manufacturer.

This brand name specification must be used because Pivotal Labs Service is the only brand capable of providing pair programming services in the development, engineering, maintenance, and improvement of PCF platform as well as the enabling of teams with industry best practices. PCF is proprietary to Pivotal Labs and they do not license or authorize anyone to provide the support services for PCF. Pivotal Labs Services is uniquely positioned to provide these services due to the company's experience with developing the PCF platform and enablement of PCF industry best practices. Pivotal Labs Services is essential to the DID(it)'s requirements, and market research indicates other companies' services do not meet DID(it)'s PCF tooling knowledge needs. The pair programming services provided by Pivotal currently allows USCIS DIT(it) teams to utilize PCF to its full capabilities by using the PCF best practices. Continued use of the Pivotal labs services will enable the program to continue to deploy software faster and at a lower cost than without these Pivotal Lab services, such as the pair programming and

**Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)**

enablement of industry best practices. Other service providers do not have the PCF subject matter expertise nor can they provide the same level of services.

DID(it) is currently using PCF as part of the DID(it) infrastructure which provides a Continuous Integration / Continuous Deployment (CI/CD) pipeline for over 50 web applications. The PCF platform reduces the overhead and costs in the software development process and provides flexibility to the development team. Enablement of industry best practices of the PCF platform-as-a-service provided by Pivotal Labs provides DID(it) with continuous improvement in the delivery of mission value.

An analysis of the RFI responses (via RFI Response Matrix) found that the marketplace has a number of competitors that provide methodologies for enablement of software development best practices but is very limited for enablement of PCF best practices. Out of 18 responses to the RFI from industry, only 4 (22% of total) responded that they have some past experience using PCF in a working DevOps environment. Those 4 responses were evaluated and it was determined they did not have experience with providing PCF best practices and pair programming services needed for this requirement. The other vendors stated that they have implemented several commercial solutions on AWS Cloud platform, but either did not speak to PCF specifically or stated that they had no experience with PCF at all. Only one response (Pivotal Software Inc.) identified past experience with enablement of PCF best practices.

DID(it) also reviewed service offerings from seller, resellers, and DHS strategically sourced vehicles. Reviews included discussions with industry experts to include engineers and sales associates for the sellers and resellers, reviewing documentation with services and pricing information, and reviewing DHS strategically sourced vehicles. Reviews also included reviews of offerings from industry in response to Request for Information (RFI).

Without Pivotal Lab services, significant impacts include the following:

- PCF would be at risk of becoming inoperable and unavailable if there are platform issues that the DID(it) team is unable to resolve on their own without the services the Pivotal team provides as described above. This would result in significant impact to mission value delivery.
- PCF would be at risk of lowered security posture if there are security vulnerabilities that the DID(it) team is unable to resolve (i.e., patch) within a required amount of time. This would result in significant impact to DID(it) overall security posture and Authority to Operate (ATO).
- DID(it) would be unable to improve the PCF platform and would not be able to realize additional value from new or additional features offered through the PCF platform.

Inoperable PCF platform would cause a significant cost increase due to the following:

Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)

- Moving applications to a new infrastructure would require code and configuration changes for each application. An example is updating deployment scripts needed for each environment, i.e., Test, Staging, and Production, which would result with close to a 100 code and configuration changes for the 50 applications across 3 environments. Each change would need to be developed, tested, and validated which would take considerable time and resources to accomplish.
- Training both the federal and contract staff in using a new PaaS solution would take at least 6 months and would result in additional costs to government associated with that time and training.
- Slowdown in productivity due to the learning curve with another PaaS solution would result in longer deliver cycles and higher costs for software development and would hinder the ability to meet mission goals.

5. Determination by the contracting officer that the anticipated cost to the Government will be fair and reasonable.

The contracting officer has determined that issuing the proposed Delivery Order for Pivotal Labs Services represents the best value and will result in the lowest overall cost, considering price and administrative costs, to meet the Government's needs. As a result of the market research conducted, the Contracting Officer anticipates offers from two or more Alliant 2 awardees. As needed, proposed pricing received in response to the solicitation will be compared with competitive published price lists or compared with the Independent Government Cost Estimate, which was established using historical pricing information and published GSA price lists.

6. Any other facts supporting the justification.

Market research was conducted July 2018 through August 2018 and updated in March 2019. The following market research methodologies were used:

- Provided overview on requirement at USCIS Industry Day (June 14, 2018) and discussed requirement / capabilities available with industry participants.
- Request for Information (RFI) sent to industry with responses received on July 25, 2018.
- Reviewed DHS Strategic Sourcing options via the DHS Strategic Sourcing [REDACTED]
- Reviewed GSA IT Schedule 70 options via [REDACTED]
- Market research conversation with CarahSoft, Pivotal Labs Authorized distributor, to verify resellers available under EAGLE Next Gen group of contract. Alliant 2 unrestricted was determined to hold 2 or more resellers.

Market research concluded that Pivotal Software Inc. is uniquely positioned to provide best practice enablement services for both PCF and agile software development. USCIS

**Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)**

currently uses the PCF and requires Pivotal Labs services, including pair programming and development services for PCF. The market research showed that Pivotal Software Inc. does not contract directly with the federal government, but does provide these services and licensing through CarahSoft's resellers under Alliant 2.

7. A statement of the actions, if any, the agency may take to remove or overcome any barriers that led to the exception to fair opportunity before any subsequent acquisition for the supplies or services is made.

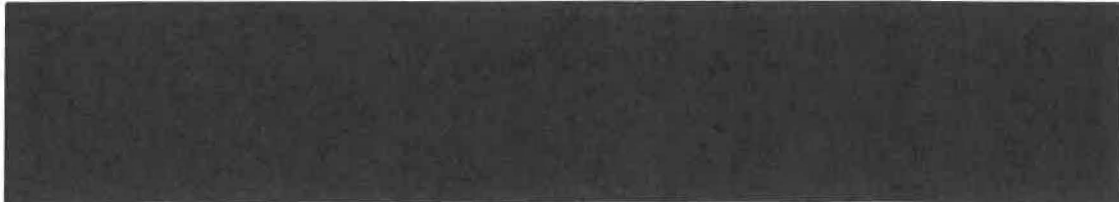
Barriers to competition may be removed or overcome if USCIS seeks to replace PCF for another platform-as-a service. However, the government intends to do continuous market research on required services in FY 2019 and out years to determine whether the marketplace has expanded for the required services. This surveillance of the marketplace will enable the Office of Information and Technology (OIT) to determine if there are alternative solutions that will allow for cost effective changes.

8. DHS intends to post this requirement on FedBizOpps pursuant to FAR 16.505(b)(2)(ii)(D).

**Justification for Brand Name Exception to Fair Opportunity
Exceeding the SAT pursuant to FAR 16.505(a)(4)**

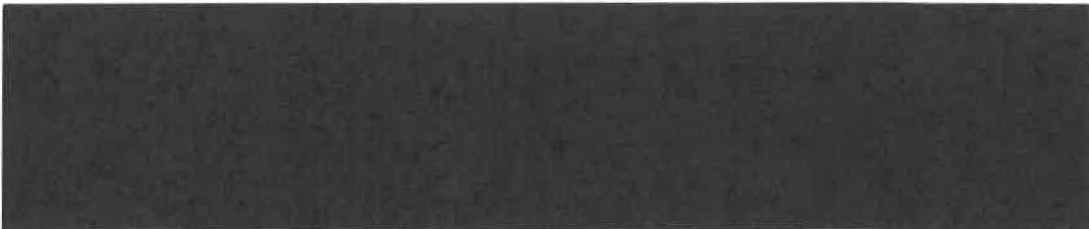
9. Technical/Requirements Personnel Certification.

Pursuant to FAR 16.505(b)(2)(ii)(B)(9), I certify that this requirement meets the Government's minimum need and that the supporting data, which form a basis for the justification, are accurate and complete.



10. Contracting Officer Certification and/or Approval *

Pursuant to FAR 16.505(b)(2)(ii)(B)(8), I certify that this justification is accurate and complete to the best of my knowledge and belief and hereby determine that the circumstances for an exception to fair opportunity exist:



11: Approval:

Pursuant to FAR 16.505(b)(2)(ii)(B)(10), I have determined that the circumstances in FAR 16.505 (b)(2)(i)(B) apply to the order:

