

<b>SOLICITATION/CONTRACT/ORDER FOR COMMERICAL ITEMS</b> <i>DEFEROR TO COMPLETE BLOCKS 1, 17, 23, 24, &amp; 30</i>				1. REQUISITION NUMBER 2416206CT0631		PAGE OF 1 37	
2. CONTRACT NO. HSTS03-13-A-CT0549		3. AWARD EFFECTIVE DATE 10/04/2016		4. ORDER NUMBER HSTS03-16-J-CT0631		5. SOLICITATION NUMBER	
7. <b>FOR SOLICITATION INFORMATION CALL:</b>		a. NAME Polly Hall		b. TELEPHONE NUMBER 571227 (b)(6)		8. OFFER DUE DATE/LOCAL TIME	
9. ISSUED BY OFFICE OF ACQUISITION 701 S 12TH STREET ARLINGTON VA 20598				10. THIS ACQUISITION IS <input checked="" type="checkbox"/> UNRESTRICTED OR SETASIOE: % FOR: SMALL BUSINESS WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM NAICS 541511 UBZONE SMALL BUSINESS EDWOSB SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS 8(A) SIZE STANDARD. (b)(4)			
11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED SEE SCHEDULE		12. DISCOUNT TERMS Net 30		13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)		13b. RATING	
16. DELIVER TO		16. ADMINISTERED BY TSA INFRASTRUCTURE 701 S 12th St ARLINGTON VA 20598		14. METHOD OF SOLICITATION RFQ IFB RFP			
17a. CONTRACTOR/OFFEROR INTERNATIONAL BUSINESS MACHINES CORPORATION Attn: (b)(6) 6710 ROCKLEDGE DR BETHESDA MD 208171826  TELEPHONE NO. (b)(6)		17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUPPLY ADDRESS IN OFFER		18a. PAYMENT WILL BE MADE BY US Coast Guard Financial Center TSA Commercial Invoices P.O. Box 4111 Chesapeake VA 23327-4111			
19. ITEM NO.		20. SCHEDULE OF SUPPLIES/SERVICES		21. QUANTITY		22. UNIT	
00001		GSA Contract #: GS-35F-4984H Tax ID Number: 13-0871985 DUNS Number: 835130485 This Time and Materials - Labor Hour Task Order HSTS03-16-J-CT0631 is issued against BPA HSTS03-13-A-CT0549 for application development services to enhance and expand the iShare platform.  CTIN 00001 - iShare/Workflow Development & Continued <i>(Use Reverse and/or Attach Additional Sheets as Necessary)</i>		1		JB	
25. ACCOUNTING AND APPROPRIATION DATA See schedule		26. TOTAL AWARD AMOUNT (For Govt Use Only) \$1,083,574.07		27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4, FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ARE ARE NOT ATTACHED. <input checked="" type="checkbox"/> 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4 FAR 52.212-5 IS ATTACHED. ADDENDA ARE <input checked="" type="checkbox"/> ARE NOT ATTACHED.			
28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.				29. AWARD OF CONTRACT: REF. OFFER DATED YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS.			
30a. SIGNATURE OF CONTRACTOR		30b. NAME AND TITLE OF SIGNER (Type or print) Mike McGowan, IBM Contracts Manager		30c. DATE SIGNED 9/30/2016		31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER) Polly Hall	
31b. NAME OF CONTRACTING OFFICER (Type or print) Polly Hall		31c. DATE SIGNED 09/30/2016					

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Technical Support - Base Period  Accounting Info: 5TS167AC00020161TS010GE000075006700670C10-67C50C00 00000000-251D-TSA DIRECT-DEF. TASK-D Funded: (b)(4) Period of Performance: 10/04/2016 to 02/03/2017  Authorized Labor Categories:  Project Manager (b)(4) /hour Subject Matter Expert (Government) (b)(4) /hour Subject Matter Expert (Contractor) (b)(4) /hour Systems Architect (b)(4) /hour Project Manager (b)(4) /hour Business Process Reengineering Specialist (b)(4) /hour Application Developer/Programmer (b)(4) /hour Applications Engineer (Intermediate) (b)(4) /hour  NTE Hours 4,932 NTE Dollars (b)(4)				
00002	CLIN 00002 - OGS Sharepoint Team Site Support - Base Period  Accounting Info: 5AV167AC0002016ADE010GE0000250066006600GS-66C10C03 00000000-253D-TSA DIRECT-DEF. TASK-D Continued ...	1	CB	(b)(4)	

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  <input type="checkbox"/> PARTIAL <input type="checkbox"/> FINAL	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
--	--------------------	---------------------------------	--	------------------

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)

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
 HSTS03-13-A-CIO549/HSTS03-16-C-CIO631

PAGE OF  
 3 37

NAME OF OFFEROR OR CONTRACTOR  
 INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Funded: (b)(4) Period of Performance: 10/04/2016 to 02/03/2017  Authorized Labor Categories:  Project Manager (b)(4)/hour Business Process Reengineering Specialist (b)(4)/hour Application Developer/Programmer (b)(4)/hour  NTE Hours 1,737 NTE Dollars (b)(4)				
00003	CLIN 00003 - OLE/FAMS, OOS FASDS Enhancement Support - Base Period  Accounting Info: 5TS167A000D2016ITS010GE0000750067006700C10-67050000 00000000-251D-TSA DIRECT-DEF. TASK-D Funded: (b)(4) Period of Performance: 10/04/2016 to 02/03/2017  Authorized Labor Categories:  Systems Architect (b)(4)/hour Business Process Reengineering Specialist (b)(4)/hour Application Developer/Programmer (b)(4)/hour  NTE Hours 1,236 NTE Dollars (b)(4)	1	CB	(b)(4)	(b)(4)
00004	CLIN 00004 - OLE/FAMS, SSA, Security, PERSEC, Enterprise Contractor Database Support - Base Period  Accounting Info: 5TS167A000D2016ITS010GE0000750067006700C10-67050000 00000000-251D-TSA DIRECT-DEF. TASK-D Funded: (b)(4) Period of Performance: 10/04/2016 to 02/03/2017  Authorized Labor Categories:  Project Manager (b)(4)/hour Application Developer/Programmer (b)(4)/hour  Continued ...	1	CB	(b)(4)	(b)(4)

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
HSTS03-13-A-C10549/HSTS03-16-J-C10631

PAGE OF  
4 37

NAME OF OFFEROR OR CONTRACTOR  
INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	NTE Hours 814 NTE Dollars (b)(4)				
00005	CLIN 00005 - Reserved - Base Period	1	JB	0.00	0.00
00006	CLIN 00006 - OIA Strategic Communications (Optional CLIN) - Base Period Amount: (b)(4) Option Line Item  Period of Performance: 10/04/2016 to 02/03/2017  Authorized Labor Categories:  Systems Architect (b)(4) /hour Project Manager (b)(4) /hour Business Process Reengineering Specialist (b)(4) /hour Application Developer/Programmer (b)(4) hour Applications Engineer (Intermediate) (b)(4) /hour  NTE Hours 1,716 NTE Dollars (b)(4)	1	JB	(b)(4)	0.00
10001	CLIN 10001 - iShare/Workflow Development & Technical Support - Option Period Amount: (b)(4) (Option Line Item) 01/04/2017  Period of Performance: 02/04/2017 to 06/03/2017  Authorized Labor Categories:  Project Manager (b)(4) hour and (b)(4) /hour Subject Matter Expert (Government) (b)(4) /hour and (b)(4) /hour Subject Matter Expert (Contractor) (b)(4) /hour and (b)(4) hour Systems Architect (b)(4) and (b)(4) /hour Project Manager (b)(4) /hour and (b)(4) /hour Business Process Reengineering Specialist (b)(4) /hour and (b)(4) /hour Application Developer/Programmer (b)(4) /hour and (b)(4) /hour Applications Engineer (Intermediate) (b)(4) /hour and (b)(4) /hour  Continued ...	1	JB	(b)(4)	0.00

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
 HSTS03-13-A-C10549/HSTS03-16-J-C10631

PAGE OF  
 5 37

NAME OF OFFEROR OR CONTRACTOR  
 INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
10002	<p>NTE Hours 4,466                      NTE Dollars (b)(4)</p> <p>CLIN 10002 - OGS Sharepoint Team Site Support -                      Option Period                      Amount: (b)(4) (Option Line Item)                      01/04/2017</p> <p>Period of Performance: 02/04/2017 to 06/03/2017</p> <p>Authorized Labor Categories:</p> <p>Project Manager (b)(4)/hour and (b)(4)/hour                      Business Process Reengineering Specialist                      (b)(4)/hour and (b)(4)/hour                      Application Developer/Programmer (b)(4)/hour and                      (b)(4)/hour</p> <p>NTE Hours 1,737                      NTE Dollars (b)(4)</p>	1	JB	(b)(4)	0.00
10003	<p>CLIN 10003 - OLR/FAMS, OOS PASDS Enhancement                      Support - Option Period                      Amount: (b)(4) (Option Line Item)                      01/04/2017</p> <p>Period of Performance: 02/04/2017 to 06/03/2017</p> <p>Authorized Labor Categories:</p> <p>Systems Architect (b)(4) hour and (b)(4)/hour                      Business Process Reengineering Specialist                      (b)(4)/hour and (b)(4)/hour                      Application Developer/Programmer (b)(4)/hour and                      (b)(4)/hour</p> <p>NTE Hours 677                      NTE Dollars (b)(4)</p>	1	JB	(b)(4)	0.00
10004	<p>CLIN 10004 - OLE/FAMS, SSA, Security, PERSEC,                      Enterprise Contractor Database Support                      Amount: (b)(4) (Option Line Item)                      01/04/2017</p> <p>Period of Performance: 02/04/2017 to 06/03/2017</p> <p>Authorized Labor Categories:                      Continued ...</p>	1	JB	(b)(4)	0.00

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
 HSTS03-13-A-C10549/HSTS03-16-J-C10631

PAGE OF  
 6 37

NAME OF OFFEROR OR CONTRACTOR  
 INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Project Manager (b)(4) /hour and (b)(4) /hour Application Developer/Programmer (b)(4) /hour and (b)(4) /hour  NTE Hours 1,217 NTE Dollars (b)(4)				
10005	CLIN 10005 - Reserved - Option Period Amount: \$0.00 (Option Line Item)  Period of Performance: 02/04/2017 to 06/03/2017	1	CB	0.00	0.00
10006	CLIN 10006 - OIA Strategic Communications - Option Period Amount: (b)(4) (Option Line Item) 01/04/2017  Period of Performance: 02/04/2017 to 06/03/2017  Authorized Labor Categories:  Systems Architect (b)(4) /hour and (b)(4) /hour Project Manager (b)(4) /hour and (b)(4) /hour Business Process Reengineering Specialist (b)(4) /hour and (b)(4) /hour Application Developer/Programmer (b)(4) /hour and (b)(4) /hour Applications Engineer (Intermediate) (b)(4) /hour and (b)(4) /hour  NTE Hours 1,400 NTE Dollars (b)(4)  The total amount of award: \$2,438,030.15. The obligation for this award is shown in box 26.	1	CB	(b)(4)	0.00

## 1 GENERAL INFORMATION

This task order is in support of the Transportation Security Administration (TSA), Office of Information Technology (OIT), to perform application development services to enhance and expand the iShare platform.

### 1.1 Period of Performance

The period of performance for this task order is:  
 Base Period 10/04/2016 – 02/03/2017  
 Option Period 02/04/2017 – 06/03/2017

### 1.2 Type of Order

This is a Time and Materials – Labor Hour task order.

## 2 SCHEDULE OF SUPPLIES AND SERVICES

The schedule of supplies and services for this task order is provided below.

<b>Base Period</b>		
<b>CLIN No.</b>	<b>DESCRIPTION</b>	<b>PRICE</b>
00001	iShare/Workflow Development & Technical Support	(b)(4)
00002	OGS Sharepoint Team Site Support	
00003	OLE/FAMS, OOS FASDS Enhancement Support	
00004	OLE/FAMS, SSA, Security, PERSEC, Enterprise Contractor Database Support	
00005	RESERVED	
00006	OIA Strategic Communications (Optional)	
<b>Base Period Total</b>		<b>\$1,286,576.19</b>
<b>CLIN No.</b>	<b>DESCRIPTION</b>	<b>PRICE</b>
10001	iShare/Workflow Development & Technical Support	(b)(4)
10002	OGS Sharepoint Team Site Support	
10003	OLE/FAMS, OOS FASDS Enhancement Support	
10004	OLE/FAMS, SSA, Security, PERSEC, Enterprise Contractor Database Support	
10005	RESERVED	
10006	OIA Strategic Communications (Optional)	
<b>Option Period Total</b>		<b>\$1,151,453/96</b>
<b>Task Order Total</b>		<b>\$2,438,030.15</b>

### **3 SPECIFIC REQUIREMENTS**

Performance requirements for this task order are provided in the Performance Work Statement (PWS) attached to this RFQ.

### **4 SUPPLEMENTAL CLAUSES AND PROVISIONS**

The following clauses are included in this task order.

#### **4.1 Clauses incorporated by reference**

All clauses found in the Vendor's OASIS II BPA are included in this task order.

##### **4.1.1 52.227-3 PATENT INDEMNITY (APR 1984)**

##### **4.1.2 52.232-7(e) PAYMENTS UNDER TIME-AND-MATERIALS AND LABOR-HOUR CONTRACTS (AUG 2012)**

##### **4.1.3 52.232-25 PROMPT PAYMENT (JUL 2013)**

#### **4.2 Clauses incorporated by full text**

##### **4.2.1 FAR 52.217-9 – OPTION TO EXTEND THE TERM OF THE CONTRACT (Mar 2000)**

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 8 months.

**(End of Clause)**

##### **4.2.2 5200.243.001 CONTRACTING OFFICER (CO)**

The Contracting Officer is the only person authorized to make any changes, approve any changes in the requirements of this contract, issue orders, obligate funds and authorize the expenditure of funds, and notwithstanding any term contained elsewhere in this contract, such authority remains vested solely in the Contracting Officer. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) In the event, the Contractor makes any changes at the direction of any person other than the



Contracting Officer, the change will be considered to have been without authority and no adjustment will be made in the contract price to cover any increase in costs incurred as a result thereof.

The following Primary Contracting Officer is assigned to this contract. Alternate Contracting Officers may be assigned:

TSA Contracting Officer:  
NAME: Kevin C. Dillon  
PHONE NUMBER: 609-813-(b)(6)  
EMAIL: (b)(6)

#### **4.2.3 5200. 242.001 CONTRACTING OFFICER'S REPRESENTATIVE (COR) AND TECHNICAL MONITORS**

The principle role of the COR is to support the Contracting Officer in managing the contract. This is done through furnishing technical direction within the confines of the contract, monitoring performance, ensuring requirements are met within the terms of the contract, and maintaining a strong relationship with the Contracting Officer. As a team the Contracting Officer and COR must ensure that program requirements are clearly communicated and that the agreement is performed to meet them. The principle role of the Technical Monitor (TM) is to support the COR on all work orders, tasks, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.

The Contracting Officer hereby designates the individual(s) named below as the Contracting Officer's Representative(s) and Technical Monitor(s). Such designations(s) shall specify the scope and limitations of the authority so delegated.

TSA CORs:  
NAME: Sung Lee  
PHONE NUMBER: 571-227-(b)(6)  
EMAIL: (b)(6)

The COR(s) and TM(s) may be changed at any time by the Government without prior notice to the Contractor, but notification of the change, including the name and phone number of the successor COR, will be promptly provided to the Contractor by the Contracting Officer in writing.

The responsibilities and limitations of the COR are as follows:

- The COR is responsible for the technical aspects of the project and technical liaison with the Contractor. The COR is also responsible for the final inspection and acceptance of all reports and such other responsibilities as may be specified in the contract.
- The COR may designate assistant COR(s) to act for him/her by naming such assistant in writing and transmitting a copy of such designation through the Contracting Officer to the Contractor.
- The COR will maintain communications with the Contractor and the Contracting Officer. The COR must report any observed fraud, waste, or opportunities to improve performance of cost efficiency to the Contracting Officer.
- The COR will immediately alert the Contracting Officer to any possible Contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.

- The COR is not authorized to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract's price, terms or conditions. Any Contractor request for changes shall be referred to the Contracting Officer directly or through the COR. No such changes shall be made without the expressed prior authorization of the Contracting Officer.
- The COR is not authorized to direct the Contractor on how to perform the work.
- The COR is not authorized to issue stop-work orders. The COR may recommend the authorization by the Contracting Officer to issue a stop work order, but the Contracting Officer is the only official authorized to issue such order.
- The COR is not authorized to discuss new proposed efforts or encourage the Contractor to perform additional efforts on an existing contract or order.

The responsibilities and limitations of the TM are as follows:

- Coordinating with the COR on all work orders, task, deliverables and actions that require immediate attention relating to the approved scope and obligated funding of the contract action.
- Monitoring the Contractor's performance in relation to the technical requirements of the assigned functional area of the contract to ensure that the Contractor's performance is strictly within the contract's scope and obligated funding.
- Ensuring that all recommended changes in any work under the contract are coordinated and submitted in writing to the COR for consideration.
- Informing the COR if the Contractor is not meeting performance, cost, schedule milestones.
- Performing technical reviews of the Contractor's proposals as directed by the COR.
- Performing acceptance of the Contractor's deliverables as directed by the COR.
- Reporting any threats to the health and safety of persons or potential for damage to Government property or critical national infrastructure which may result from the Contractor's performance or failure to perform the contract's requirements.

#### **4.2.4 4202.242.002 "SUBMISSION OF INVOICES - Commercial"**

(a) Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the U.S. Coast Guard Finance Center (FinCen).

(b) Invoice Submission Method: Invoices may be submitted via facsimile, U.S. Mail, or email. Contractors shall utilize **ONLY ONE** method per invoice submission. The submission information for each of the methods is as follows in order of preference:

1) Facsimile number is: 757-413-7314

The facsimile number listed above shall be used by contractors for ORIGINAL invoice submission only. If facsimile submission is utilized, contractors shall not submit hard copies of invoices via the U.S. mail. It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed in subparagraph (d) of this clause.

2) U.S. Mail:

United States Coast Guard Finance Center

TSA Commercial Invoices  
P.O. Box 4111  
Chesapeake, VA 23327-4111

3) Email Invoices:

FIN-SMB-TSAInvoices@uscg.mil or www.fincen.uscg.mil

(c) Invoice Process: Upon receipt of contractor invoices, FinCen will electronically route invoices to the appropriate TSA Contracting Officer's Technical Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

Note for discounts offered:

Discounts on invoices. If desired, the Contractor should offer discounts directly upon the invoice submitted, clearly specifying the terms of the discount. Contractors can structure discounted amounts for payment for any time period less than the usual thirty day payment period specified under Prompt Payment requirements; however the Contractor should not structure terms for payment of net amounts invoiced any sooner than the standard period required under FAR Subpart 32.9 regarding prompt payments for the specified deliverables under contract.

Discounts offered after invoice submission. If the Contractor should wish to offer a discount on a specific invoice after its submission for payment, the Contractor should submit a letter to the Finance Center identifying the specific invoice for which a discount is offered and specify the exact terms of the discount offered and what time period the Government should make payment by in order to receive the discount. The Contractor should clearly indicate the contract number, invoice number and date, and the specific terms of the discount offered. Contractors should not structure terms for net amount payments any sooner than the standard period required under FAR Subpart 32.9 regarding prompt payments for the specified deliverables under contract.

(d) Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

(1) Via the internet: <https://www.fincen.uscg.mil>

Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

(2) Via the Payment Inquiry Form: <https://www.fincen.uscg.mil/secure/payment.htm>

(e) Invoice Elements: Invoices will automatically be rejected if the information required in subparagraph (a)(2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and DUNS number are not included in the invoice.

All invoices must clearly correlate invoiced amounts to the corresponding contract line item number and funding citation. The Contractor shall work with the Government to mutually refine the format, content and method of delivery for all invoice submissions during the performance of the Contract. Should an invoice be rejected for any reason, the resulting revised invoice must be submitted for the period covered by the original invoice. The revised invoice shall not be merged or combined with a subsequent invoice.

(f) Supplemental Invoice Documentation: Contractors shall submit all supplemental invoice documentation (e.g. copies of subcontractor invoices, travel vouchers, etc) necessary to approve an invoice along with the original invoice. The Contractor invoice must contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Representative. Note for "time-and-materials" type contracts: The Contractor must submit the following statement with each invoice for labor hours invoiced under a "time-and-materials" type contract, order, or contract line item: "The Contractor hereby certifies in accordance with paragraph (c) of FAR 52.232-7, that each labor hour has been performed by an employee (prime or subcontractor) who meets the contract's specified requirements for the labor category invoiced."

(g) Additional Invoice Preparation Instructions for Software Development and/or Hardware. The Contractor shall clearly include a separate breakdown (by CLIN) for any software development activities (labor costs, subcontractor costs, etc) in accordance with Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10 (Preliminary design costs, Development costs and post implementation costs) and cite payment terms. The contractor shall provide make and model descriptions as well as serial numbers for purchases of hardware and software (where applicable.)

(h) Frequency of Invoice Submission: Invoices shall be submitted on a monthly basis in arrears

#### **4.2.5 5201.204.001 Personnel Access**

All Contractor personnel requiring unescorted access to TSA facilities, information systems, or information will be subject to the security procedures set forth in this contract.

#### **4.2.6 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 Task Order and may, with the consent of the contracting parties, be changed from time to time during the course of the Task Order by adding or deleting personnel or facilities, as appropriate.

(b) Before removing or 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 Task Order. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Task Order:

1) Application Engineer (Intermediate) : (b)(6)

- 2) Project Manager: (b)(6)
- 3) Business Process Reengineering Specialist: (b)(6)

**4.2.7 5200.237.006 SUBSTITUTION OF KEY PERSONNEL**

The Contractor shall notify the Contracting Officer (CO) and the Contracting Officer’s Technical Representative (COR) prior to making any changes in Key Personnel. No changes in Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the Key Personnel being replaced or otherwise meet the standards applicable in the contract. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or forty-five (45) days if either a background investigation for building or information system access and/or a security clearance (due to classified contract requirements that relate specifically to personnel) must be obtained to meet the contract’s requirements, in advance of the proposed substitution. Such notification from the contractor shall include:

- (a) an explanation of the circumstances necessitating the substitution;
- (b) a complete resume of the proposed substitute; and
- (c) any other information requested by the CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The CO and COR will evaluate substitution requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

**4.2.8 5201.242.001 PERIOD OF PERFORMANCE FOR CONTRACTS REQUIRING EMPLOYEE BACKGROUND CHECKS**

The period of performance begins upon the day of award. However, contractor performance may begin up to 60 days after contract award to allow for the Enter On Duty Suitability Determination. Performance may begin sooner if the vetting process takes less than 60 days.

**4.2.9 3052.209-73 LIMITATIONS ON FUTURE CONTRACTING (JUN 2006)**

- (a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR 9.5 – Organizational Conflicts of Interest.
- (b) The restrictions upon future contracting are as follows:
  - (1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production

- contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.
- (2) To the extent that the work under this Contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

#### **4.2.10 General Requirements**

##### **4.2.10.1 Special Delivery Instructions:**

All deliverables shall be created in the *Department of Homeland Security Systems Engineering Life Cycle (DHS SELC)* format whenever an applicable template is available or a format provided by the GPM.

The TSA OASIS II Deliverable Submission Acceptance Form (DSAF) shall be provided to the Government Project Manager (GPM) Technical Monitor (TM), Contracting Officer (CO) and Contracting Officer's Representative (COR). The Contractor shall provide a Letter of Transmittal to the CO. The deliverable shall be one hard copy and one soft copy via iShare site in MS Office format clearly marked with:

- Title of the submittal
- DHS contract number
- TSA work order number, and
- CLIN

The contractor is hereby notified that TSA is a Microsoft based environment for office productivity tools. Document deliveries must be in a Microsoft format (where applicable).

##### **4.2.10.2 Place/ Location of Performance/ Delivery**

1. The Contractor is required to perform the required work at sites specified in the task order.
2. Primary work on this task order will be performed at the Contractor's facility in accordance with the terms and conditions of the Contractor's OASIS II BPA.
3. Local commuting expenses within a fifty (50) mile radius of the TSA Headquarters (currently in or near 601 12th Street, Arlington, VA) and other direct costs (cell phone, etc.) will not be charged to the Government.

Travel outside the local area is not authorized under this task order.

##### **4.2.10.3 Accessibility Requirements (Section 508)**

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

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

#### **4.2.10.4 Section 508 Applicable EIT Accessibility Standards**

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

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

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

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

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

#### **4.2.10.5 Section 508 Applicable Exceptions**

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

#### **4.2.10.6 Section 508 Compliance Requirements**

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

#### **4.2.11 DHS and TSA Enterprise Architecture Compliance**

- a) The Contractor shall ensure that all solutions, products, deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the Federal Enterprise Architecture Framework (OMB Reference Models).
- b) All solutions and services shall meet DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with Homeland Security Enterprise Architecture (HLS EA) requirements.
  - i. All developed solutions and requirements shall be compliant with the HLS EA.
  - ii. The contractor shall align all solutions and services and ensure compliance with applicable TSA and DHS IT Security, Application, System, Network, Data, Information, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.
  - iii. The contractor shall utilize any existing TSA or DHS user interface design standards, style guides, and/or policies and standards for human factors, usability, user experience, or human computer interaction (HCI).
  - iv. All solution architectures and services (Application, System, Network, Security, Information, etc.) shall be reviewed and approved by TSA EA as part of the TSA SELC review process and in accordance with all applicable DHS and TSA IT governance policies, directives, and processes (i.e. TSA IT Governance Management Directive 1400.20). This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. All implementations shall follow the approved solution architecture/design without deviation. Any changes, to either the prior approved solution and/or prior approved design that are identified during subsequent SELC phases, including testing, implementation and deployment, shall undergo additional EA review prior to proceeding.



- v. All IT hardware and software shall be compliant with the TSA and HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to TSA and DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the TSA and HLS EA 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 TSA Enterprise Architecture Data Management Team, who will be responsible for coordination with the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
  - i. 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 and TSA data management architectural guidelines and subject to the TSA Enterprise Architecture Data Management Team (EDM) approval.
  - ii. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – ‘Rights in Data and Copyrights’ and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in an understandable format to TSA. Examples of data structures can be defined as, but not limited to
    - a. Data models depicting relationship mapping and, or linkages
    - b. Metadata information to define data definitions
    - c. Detailed data formats, type, and size
    - d. Delineations of the referential integrity (e.g., primary key/foreign key) of data schemas, structures, and or taxonomies
  - iii. All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within the ‘Requirements for Handling Sensitive, Classified, and/or Proprietary Information’, section of this SOW. This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system. Alternative data delivery techniques may also be defined by TSA Enterprise Data Management (EDM) team.
  - iv. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g. metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered in a TSA approved manner). Metadata shall also provide an indication of historical verses the most current data to be used, as well as frequency of data refreshes.

- v. The contractor shall adhere to providing a Data Management Plan (DMP), as defined by Enterprise Architecture, to the EA design review team before the preliminary/critical design review. The Data Management Plan includes conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data. All data artifacts must adhere to TSA EA data standards defined and published before the design review. Data Standards include but are not limited to, data asset standards, metadata standards, logical/physical naming standards, and information exchange (using the National Information Exchange Model (NIEM)) standards. All required artifacts must be provided to and approved by the EA Design Review team.
- d) 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.

#### **4.2.12 Monthly Burn Report**

On a monthly basis, the Contractor shall provide a monthly burn report to the TM, COR and CO. The report shall provide the Government an accurate report for monthly contract expenses. This monthly report shall be within 5% of the actual monthly total cost. The monthly burn report shall include projected monthly cost vs actual monthly cost; projected hours burned per labor category per CLIN vs actual hours burned per labor category per CLIN; projected level of effort per task vs actual level of effort per task; overall CLIN burn percentage; and overall contractual burn percentage. The report format shall include tasking, labor category, hourly labor cost, hours, and total cost matching the following format. All projected and actual burn per labor category per mobile applications development CLINs shall be associated with the project number from the relevant Project Definition Document, so that burn is directly associated with the related effort in accordance with the approved Project Definition Document.

The Monthly Burn Report is due on the 15th of each month for the previous month's burn rate. (If the 15th falls on a weekend/holiday, then the first business day prior to the 15th).

Burn Rate Example					
Monthly Burn, WP 000, Project Name, Month					
Resource Name	Tasking	Labor Cat	Hourly Labor Cost	Hours	Total
Joe Smith	Data Cleansing	Database Specialist 2	\$153.24	120.0	\$18,388.80
Jack Rabbit	Data Entry Module	Application Programmer 1	\$185.99	60.0	\$11,159.40
Jack Rabbit	Reporting Module	Application Programmer 2	\$225.00	60.0	\$13,500.00
Lucy Jones	PM Support	SME 2	\$150.00	80.0	\$12,000.00
<b>Monthly Total</b>				<b>320.0</b>	<b>\$55,048.20</b>

#### 4.2.13 Information Assurance Requirements for TSA Acquisitions (April 2016)

##### 4.2.13.1 General Security Requirements

The Contractor shall comply with all Federal, Department of Homeland Security (DHS) and Transportation Security Administration (TSA) security and privacy guidelines in effect at the time of the award of the contract, As well as those requirements that may be discretely added during the contract.

The Contractor shall perform periodic reviews to ensure compliance with all information security and privacy requirements.

The Contractor shall comply with all DHS and TSA security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 standards.

The Contractor shall include this guidance in all subcontracts at any tier where the subcontractor is performing the work defined in this statement of work (SOW).

The Contractor shall ensure all staff have the required level of security clearance commensurate with the sensitivity of the information being accessed, stored, processed, transmitted or otherwise handled by the System or required to perform the work stipulated by the contract. At a minimum, all Contractor staff shall be subjected to a Public Trust background check and be granted a Public Trust clearance before access to the System or other TSA resources is granted.

The Contractor shall sign a DHS Non-Disclosure Agreement (NDA) within (30) calendar days of the contract start date.

The Contractor shall not release, publish, or disclose agency information to unauthorized personnel, and shall protect such information in accordance with the provisions of the pertinent laws and regulations governing the confidentiality of sensitive information.

The Contractor shall ensure that its staff follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel shall be responsible for the physical security of their area and government furnished equipment (GFE) issued to the contractor under the terms of the contract.

The Contractor shall make all system information and documentation produced in support of the contract available to TSA upon request.

#### **4.2.12.2 Training Requirements**

All Contractor employees, requiring system access, shall receive initial Organizational Security Fundamentals Training within 60 days of assignment to the contract via the Online Learning Center (OLC). Refresher training shall be completed annually thereafter.

The Contractor shall complete annual online training for Organizational Security Fundamentals and TSA Privacy training.

Role Based training is required for contract employees with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, and shall be in accordance with DHS and TSA policy. The contractor will be notified if they have a position with significant security responsibility.

Individuals with SSR shall have a documented individual training and education plan, which shall ensure currency with position skills requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan shall be refreshed annually or immediately after a change in the individual's position description requirements.

Information Security and Privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

The Contractor shall maintain a list of all employees who have completed training and shall submit this list to the contracting officer representative (COR) upon request, or during DHS/TSA onsite validation visits performed on a periodic basis.

The contractor shall its employees review and sign the TSA Form 1403 Computer and Wireless Mobile Device Access Agreement (CAA) prior to accessing IT systems.

#### **4.2.12.3 Configuration Management (hardware/software)**

Hardware or software configuration changes shall be in accordance with the DHS Information Security Performance Plan (current year and any updates thereafter), the DHS Continuous Diagnostics and Mitigation (CDM) Program to include dashboard reporting requirements and TSA's Configuration Management policy. The TSA Chief Information Security Officer (CISO)/Information Assurance and Cyber Security Division (IAD) shall be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD POC shall approve any request for change prior to any development activity occurring for that change and shall define the security requirements for the requested change. The COR will provide access to the DHS Information Security Performance Plan.

The Contractor shall ensure all application or configuration patches and/or Requests for Change (RFC) have approval by the Technical Discussion Forum (TDF), Systems Configuration Control Board (SCCB) and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 Information Technology Security and TSA Information Assurance (IA) Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA CISO, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.

The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting “sensitive information”) shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/NIST, National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

#### US Government Configuration Baseline and DHS Configuration Guidance

- a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Baseline (USGCB) and in accordance with DHS and TSA guidance.
  1. USGCB Guidelines:
    - a. [http://usgcb.nist.gov/usgcb\\_content.html](http://usgcb.nist.gov/usgcb_content.html)
  2. DHS Sensitive Systems Configuration Guidance
    - a. <http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx>
- b) The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology shall also use the Windows Installer Service for installation to the default “program files” directory and shall be able to discretely install and uninstall.
- c) Applications designed for general end users shall run in the general user context without elevated system administration privileges.

The Contractor shall establish processes and procedures for continuous monitoring of Contractor systems that contain TSA data/information by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). The Contractor shall perform monthly security scans on servers that contain TSA data, and shall send monthly scan results to the TSA IAD.

#### 4.2.13.4 Risk Management Framework

The Security Authorization and Ongoing Authorization Process in accordance with NIST SP 800-37 and SP 800-137 (current versions) is a requirement for all TSA IT systems, including general support systems (e.g., standard TSA desktop, general network infrastructure, electronic mail, etc.), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework. Ongoing Authorization is part of Step 6 “Monitoring” of the Risk Management Framework. All NIST and

DIACAP guidance are publicly available; TSA and DHS security policy is disclosed upon contract award.

A written authority to operate (ATO) granted by the TSA Authorizing Official (AO) is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.

TSA will assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) 199 and assign security controls to those systems consistent with FIPS 200.

Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation will be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

The Security Authorization Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation: 1) Security Assessment Report (SAR) 2) Security Plan (SP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Security Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Assessment Plan (SAP), 9) Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Ongoing Authorization Artifacts as required by the DHS Ongoing Authorization Methodology (current version). The SA package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents will be reviewed and approved by the Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

#### **4.2.13.5 Contingency Planning**

The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations are disrupted in accordance with The Office of Management and Budget (OMB) Circular A-130, Appendix III.

The Contractor shall ensure that contingency plans are consistent with template provided in the DHS Information Assurance Compliance System Tool. If access has not been provided initially, the contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K, *IT Contingency Plan Template*.

The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

The Contractor will test their CP annually.

The Contractor shall record, track, and correct any CP deficiency and any deficiency correction that cannot be accomplished within one month of the annual test will be elevated to the Information Assurance and Cyber Security Division (IAD).

The Contractor shall retain records of the annual CP testing for review during periodic audits.

The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

The Contractor shall have an Emergency Response Plan that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other incident or activity that may endanger lives, property, or the capability to perform essential functions.

The Contractor shall have a Backup Operations Plan that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time as described in the Performance Work Statement.

The Contractor shall have a Post-disaster Recovery Plan that includes procedures and responsibilities to facilitate rapid restoration of normal operations at the primary site or, if necessary, at a new facility following the destruction, major damage, or other major interruption at the primary site.

The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

The Contractor shall ensure a full backup of all network data occurs as required by the system's availability security categorization impact rating per TSA Information Assurance policy.

The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) will be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one hour.

The Contractor shall ensure sufficient backup data to facilitate a full operational recovery within one business day at either the prime operational site or the designated alternate site will be stored at a secondary location determined by the local element disaster recovery plan.

The Contractor shall ensure that data at the secondary location is current as required by the system's availability security categorization impact rating.

The Contractor shall ensure the location of the local backup repository and the secondary backup repository is clearly defined, and access controlled as an Information Security Restricted Area (ISRA).

The Contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure for the layout of the file systems, or partitions, on a system's hard disk impacting the security of the data on the resultant system. File system design shall:

- Separate generalized data from operating system (OS) files

- Compartmentalize differing data types
- Restrict dynamic, growing log files or audit trails from crowding other data.

The contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure Design for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

#### **4.2.13.6 Program Performance**

The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer.

The Contractor shall provide support during the Information Assurance and Cyber Security Division (IAD) audit activities and efforts. These audit activities may include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

#### **4.2.13.7 Federal Risk and Authorization Management Program (FedRAMP)**

**If a vendor is to host a system with a Cloud Service Provider, the following shall apply:**

**FedRAMP Requirements:** Private sector solutions will be hosted by a Joint Authorization Board (JAB) approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) (<http://cloud.cio.gov/fcdramp/cloud-systems>) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The Cloud Service Provider shall adhere to the following in addition to the FedRAMP requirements: Identity and entitlement access management shall be done through Federated Identity; SSI and PII shall be encrypted in storage and in transit as it is dispersed across the cloud; Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS or SaaS levels; Cloud bursting shall not occur; TSA data shall be logically separated from other cloud tenants; All system administrators shall be U.S. citizens; TSA data shall not leave the United States; The cloud internet connection shall be behind a commercial Trusted Internet Connection that has EINSTEIN 3 Accelerated (E3A) capabilities deployed. These include but are not limited to the analysis of network flow records, detecting and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The E3A capability shall use the Domain Name Server Sinkholing capability and Email filtering capability allowing scans to occur destined for .gov networks for malicious attachments, Uniform Resource Locators and other forms of malware before being delivered to .gov end-users.

**Private Sector System Requirements:** TSA shall conduct audits at any time on the private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS Information Assurance Compliance Tool (IACS). The private sector systems are required to go through the Security Authorization Process and the Risk Management Framework in accordance the Federal Information Systems Management Act and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection that has



EINSTEIN 3 Accelerated (E3A) deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Information Assurance 1400.3 Management Directive and Handbook shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS.

#### **4.2.13.8 Information Assurance Policy**

All services, hardware and/or software provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook, TSA MD 1400.3 Information Technology Security Policy, TSA Information Assurance Handbook and Technical Standards.

The Contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which will be provided by the Contracting Officer, including but not limited to:

- DHS Sensitive Systems Policy Directive (PD) 4300A
- DHS 4300A Sensitive Systems Handbook
- DHS National Security Systems Policy Directive (PD) 4300B
- DHS 4300B National Security Systems Handbook
- TSA MD 1400.3 Information Technology Security
- TSA Information Assurance Handbook
- TSA Technical Standards
- DHS IT Security Architecture Guidance Volumes 1, 2 and 3
- DHS/TSA Systems Engineering Lifecycle (SELIC)
- DHS Performance Plan (current fiscal year)
- DHS Ongoing Authorization Methodology (current version)
- OMB M-10-28, M-14-03

Authorized use of TSA IT systems and resources shall be in accordance with the TSA Information Assurance Handbook.

The contractor shall complete TSA Form 251 and TSA Form 251-1 for sensitive or accountable property. The contractor shall email the completed forms to [TSA-Property@dhs.gov](mailto:TSA-Property@dhs.gov) and include a hard copy with the shipment.

#### **4.2.13.9 Data Stored/Processed at Contractor Site**

Unless otherwise directed by TSA, any storage of data must be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

#### **4.2.13.10 Remote Access**

The Contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct sanctioned TSA business. Therefore, remote access rights must be expressly granted, in writing, by the TSA Information Assurance and Cyber Security Division (IAD).

The Contractor remote access connection to TSA networks may be terminated for unauthorized use, at the sole discretion of TSA.

#### **4.2.13.11 Interconnection Security Agreement**

**If the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity, the following shall apply:**

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

#### **4.2.13.12 SBU Data Privacy and Protection**

The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow DHS and TSA requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI and Informational Security, which take one hour each, as well as TSA online Privacy training.

The Contractor shall be responsible for the security of i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor's control. All TSA data, including but not limited to PII, sensitive security information (SSI), sensitive but unclassified (SBU), and critical infrastructure information (CII), shall be protected according to DHS and TSA security policies and mandates.

TSA will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

- FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2. (current version)
- National Security Agency (NSA) Type 2 or Type 1 encryption. (current version)
- Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) 4300IA Sensitive Systems Handbook). (current version)

The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII must comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA Information Assurance Handbook and applicable IT Security Technical Standards.

The contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA Information Assurance Handbook, applicable Technical Standards and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

The Contractor shall ensure that source code is protected from unauthorized access or dissemination.

#### **4.2.13.13 Disposition of Government Resources**

At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA Information Assurance Handbook and Technical Standards. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, and TSA Technical Standard 046 *IT Media Sanitization and Disposition*. The contractor shall email signed proof of sanitization to the COTR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

#### **4.2.14 Security of Systems Handling Personally Identifiable Information and Privacy Incident Response**

(a) Definitions.

“Breach” (may be used interchangeably with “Privacy Incident”) as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have

access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

“Personally Identifiable Information (PII)” as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

“Sensitive Personally Identifiable Information (Sensitive PII)” as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual’s name or other unique identifier plus one or more of the following elements:

1. Driver’s license number, passport number, or truncated SSN (such as last 4 digits)
2. Date of birth (month, day, and year)
3. Citizenship or immigration status
4. Financial information such as account numbers or Electronic Funds Transfer Information
5. Medical Information
6. System authentication information such as mother’s maiden name, account passwords or personal identification numbers (PIN)

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

(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal

Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4

In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the

Contracting officer in coordination with CISO approves written certification by the contractor that the following requirements are met:

1. Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;
2. The contractor has developed and implemented a process to ensure that security and other applications software are kept current;
3. Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
4. When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.
5. The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
6. Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
  - i. Authorized and official use;
  - ii. Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
  - iii. Prohibition against access by unauthorized users and unauthorized use by authorized users; and
  - iv. Protection of Sensitive PII;
7. All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

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

Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

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

(c) Breach Response. The contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Representative (COR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

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

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

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require

written subcontractor acknowledgement of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

#### **4.2.15 Department of Homeland Security ISO Compliance**

##### **A. Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 *Information Technology Systems Security* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information.

Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

##### **B. Security Review**

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

##### **C. Interconnection Security Agreements**

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

##### **D. HSAR 3052.204-70 - Security Requirements for Unclassified Information Technology Resources (JUN 2006)**

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause

applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

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

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

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (41 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 5.5, September 30, 2007) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

**E. HSAR 3052.204-71 - Contractor Employee Access (JUN 2006) Alternate 1**



(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or 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 Representative (COR) 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 COR 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 Performance Work Statement, other terms and conditions in this contract, or as approved in writing by the COR, 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) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(3) 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.

(m) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR 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 performance work statement, other terms and conditions in this contract, or as approved in writing by the COR, 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.

(n) 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).

#### **F. Special Information Technology Contract Security Requirements**

(a) **Identification Badges.** All Contractor employees shall be required to obtain and wear TSA identification badges when working in TSA facilities.

(b) **Computer Access Agreement.** All Contractor employees (users, managers, and operators of the TSA network) must sign TSA Form 1403, *Computer Access Agreement*. A copy of which shall be provided to the TSA contracting officer's technical representative for retention for the duration of the contract.

#### **(c) Personnel Security.**

(1) Privileged access users are individuals who have access to an information technology (IT) system with privileges of Administrator or above and have access to sensitive network infrastructure data. Privileged access users will be appropriately screened on entry into the privileged access position and the initial screening shall be refreshed every two years,

(2) Individuals terminating voluntarily or involuntarily from a Contractor performing under contract at TSA must have an exit briefing, conducted by a supervisory or management-level employee of the Contractor in order to identify and explain their post-employment responsibilities to the TSA.

(3) Records of exit interviews will be signed and maintained by the Contractor as part of the individual employment record for a period of not less than two years following the termination of the individual's employment.

(4) The Contractor shall notify the Contracting Officer's Technical Representative and the Contracting Officer with proposed personnel changes. Written confirmation is required. This includes, but is not limited to, name changes, resignations, terminations, and reassignments to another contract.

(5) The Contractor shall notify the TSA, in writing of any requested change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes,

resignations, terminations, and transfers to other company engagements. The Contractor shall provide the following information to TSA: full name, social security number, effective date, and reason for change.

(6) The Contracting Officer must approve key personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 45 days from the date the completed forms are received (and acknowledged as complete) in the Security Programs Division.

(7) Failure of any Contractor personnel to pass a background investigation, without timely substitution that meets the contracts requirements, may be grounds for termination of the contract.

**(d) Non-Disclosure Agreements.**

(1) All TSA contractor employees and consultants must execute a DHS Form 11000-6, *Sensitive But Unclassified Information Non-Disclosure Agreement (NDA)* upon initial assignment to TSA and before being provided access to TSA “sensitive and/or mission critical information.” The original NDA will be provided to the TSA contracting officer’s technical representative for retention for the duration of the contract.

(2) The Contractor, and those operating on its behalf, shall adhere to the requirements of the nondisclosure agreement unless otherwise authorized in writing by the Contracting Officer.

**(e) Performance Requirements.**

(1) The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

(2) Contracting Officer’s Representative (COR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

**4.2.16 Government Furnished Resources and Information**

**A. Office Space & Equipment**

The Government shall provide on-site office space for Contractor personnel to work at the Government location.

For Contractor personnel performing work on Government premises, the Government will provide furniture, telephone service, workstations, software tools, access to servers and other network components, and any other necessary equipment.

**B. Government Furnished Property**

Work performance shall be performed on-site at the TSA Headquarters, Springfield Annex. The initial location of work will be the Springfield Annex, but the contractor can recommend that some services are completed at the contractor’s office location(s). It is the Government’s decision to accept the contractor’s proposal to complete any portion of this work offsite.

### **C. Expiration of Contract/Data Disposition**

At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with TSA MD 1400.3, related Information Assurance Handbook and Technical Standards.

Proof of sanitation shall be delivered via electronic transmission (soft copy) to the COR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

**(End of Clause)**

### **4.2.17 Third Party OSS Software**

Any third party OSS software furnished by TSA to our team ("OSS GFS"), that our team may install, update, or otherwise use on behalf of TSA under this work order is licensed and distributed to TSA by the third parties, and our team is not a party to such licenses or a distributor of any OSS GFS. Our team provides no warranty, indemnification, or implied or explicit license obligations regarding any OSS GFS delivered by TSA to our team as OSS GFS. Our team is responsible, in accordance with FAR 52.246-4 or FAR 52.246-6 (as applicable), for any modifications and creations of derivative works related to OSS GFS under this task order, and the foregoing does not relieve our team from its performance obligations under this task order.

## **5 Task Order Attachments**

<b>Attachment</b>	<b>Description</b>
<b>A</b>	<b>Performance Work Statement (PWS)</b>



August 2016

**SECTION I: Objective**

**Product, Service or Outcome Needed**

The Transportation Security Administration (TSA) Office of Information Technology (OIT) has implemented Microsoft Office SharePoint 2007 Server (MOSS, commonly known as iShare) as an enterprise-wide collaboration platform to enhance internal productivity, collaboration, and information sharing. iShare includes the TSA intranet for internal content publishing, TSApedia, Enterprise level blogs, interactive discussion forums and employee profile sites known as "My Sites".

This requirement maintains the technical services required to enhance and expand the iShare platform, and may also provide similar services on other Microsoft platforms such as MS Dynamics. For example, on iShare, the Team Site "layer" requires focus to ensure that the enterprise uses sites to share documents and collaborate on programs/projects. Further, this effort will provide application and data integration with key TSA systems such as TSA Operating Platform (TOP) and Microsoft Operating Platform (MOP).

Also as part of iShare, the Office of Global Strategies (OGS) needs SharePoint and Data Environment support for the iShare Team Site to effectively and efficiently maintain and enhance communication, business processes, document collaboration, and information sharing throughout OGS.

As part of iShare, the Office of Law Enforcement, Federal Air Marshal Service (OLE/FAMS), Office of Security (OOS) has asked for additional support to upgrade and enhance their current Facility as Security Data System (FASDS). The FASDS application requires upgrade from SharePoint 2007 and well as enhancements that will add additional functionality and correct issues with the current application. This work will streamline the FASDS business processes and collaboration efforts with the supporting staff from each of the Airport Regions.

As part of iShare, the Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Security Services and Assessments (SSA), Security, Personnel Security (PerSec) has asked for additional support to design, develop and deploy an Enterprise Contractor Database (Contractor Evaluation and Tracking Database (CETS)) application needed to support the tracking and reporting of contractor personnel assigned to TSA contracts. This new application is intended to replace the current manual method of tracking contractor personnel and accurately account for all contractors assigned to TSA contracts. This work will add additional data management capabilities, plus correct issues with the existing application.

The Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), Chief Security Office (CSO), has been mandated by DHS to expand current visitor vetting, to TSA facilities. Visitors are subject to background screening prior to admittance and all non-foreign visitors 18 years and older are required to provide their social security number and date of birth for vetting. The CSO team has asked for support in designing, developing and deploying an enhanced visitor request system that not only provides for request submission but data management and request tracking as well.

As part of iShare, the Office of Intelligence and Analysis (OIA), Strategic Communications Branch, requires technical services to support the enhancement of SharePoint sites for all divisions within OIA. OIA requires SharePoint site development and support to expand the functionalities of existing SharePoint sites for use by OIA divisions/branches.

### **Scope of the Product, Service, or Outcome**

The iShare and Workflow requirement includes leveraging SharePoint 2007, SharePoint 2010, SharePoint 2013, SharePoint 2016, SharePoint Online, and products such as Microsoft Datazen and MS Dynamics CRM versions to provide capabilities at the enterprise, organization/team, and individual-level. TSA's iShare environment is currently utilizing SharePoint 2007, SharePoint 2010, and SharePoint 2013. TSA will continue to use newer versions of the software when it becomes available. The contractor will utilize TSA approved software for iShare/Workflow Development and Technical Support.

This Performance Work Statement (PWS) describes the necessary requirements to assure iShare, SharePoint, and Workflow services. These requirements include those for Data Environment Support for OGS iShare Team Site effectively meeting the requirements of the evolving TSA/OGS mission. The OLE/FAMS OOS objective for enhancing the Facility and Security Data System (FASDS) application (optional task) is to increase efficiency and ensure compliance with TSA policies and procedures. The OLE/FAMS, SSA, Security, PerSec objective for creating the Enterprise Contractor Database application (Contractor Evaluation and Tracking Database (CETS)) (optional task) is to increase efficiency of tracking and reporting on contractor personnel assigned to TSA contracts and to ensure compliance with DHS and TSA policies and procedures. The OLE/FAMS, CSO objective is to create a robust visitor request system (optional task) that will allow them to collect all necessary data for DHS directed screening and ensure that all necessary measures are taken to ensure protection of the visitors' personally identifiable information.

### **SECTION II: Background Information**

The iShare tasks and team members (Federal and Contractor) in this PWS directly support the IT Strategic Goal to "improve information sharing and data collaboration" by leveraging a platform which includes a wiki (TSApedia), internal blogs (Blog Central), discussion forums, enhanced contact pages (MySites), new web content management systems, and document collaboration workspaces.

iShare, TSA's intranet solution, is organized in three layers:

1. Enterprise Layer (Blue) - Containing information published for the benefit of all TSA resources
2. Team Sites Layer (Green) - Contains collaboration sites and information specific to teams and projects
3. MySites Layer (Red) - Contains personal space for document management and information organization

At the Enterprise Layer, there is information and links provided that pertain to all employees within TSA. This layer has a listing of all TSA Offices, Divisions, and Branches, various employee services, a Directives and Forms Library, Blog Central, and TSApedia. At the Team Sites Layer, TSA Offices, Divisions, and Branches build their own collection of workspace sites where employees store and share documents, organize activities, and provide information to members of their organizational units.

My Sites within iShare are a personal/professional space to promote individuals' skills, store images and documents, and house and share information with users. My Sites also allow users to express themselves more creatively and share interests, TSA knowledge, and personal information. Each user has their own personal My Site that is completely customizable. Users can create lists, document/picture libraries and surveys, and can customize the viewing of their personal (My Home) and public (My Profile) views.

TSA has created separate "apps" layers for some SharePoint versions, to allow SharePoint applications to be separated from the mostly content-oriented layers (blue, green, and red). This apps layer creation is not part of the iShare Workflow effort, and if available would be one of the options for accomplishing the requirements described in this document.

In FY11, the iShare team assisted in the migration of the iShare platform to a new data center, and completed the implementation of several applications using custom as well as out-of-the-box features of SharePoint. In FY10, the iShare team migrated 100% of HQ offices staff collaborator sites to iShare team sites and developed several SharePoint-based applications and began planning efforts to respond to TSAs growing demand for collaboration and social networking tools and technologies. FY08-09 activities included the planning, design, and implementation of the initial release of iShare.

In FY12 through FY14, the scope of the team expanded to include business process workflow and related systems, using SharePoint, and Dynamics CRM and similar products as platforms. Use of K2 BlackPoint was envisioned, but the platform was not available. FY15 requirements include enhancing iShare with a focus on full TSA adoption as follows:

- 1) Support the enhancement of iShare team sites to HQ and field offices. This includes meetings with the stakeholders, producing requirements, executing the technical changes within SharePoint to meet these requirements, and providing user acceptance testing/training.
- 2) Enhance iShare Governance. This work includes meeting with stakeholders, including within OIT, to understand current SharePoint-related governance practices.
- 3) Develop and/or integrate into iShare FSD applications identified as important to the field. Candidate applications include: Lost & Found, Uniform tracking, HR Data Tracking, Inventory Management, Supply Purchasing, Dashboards.
- 4) Allow users to access key TSA application data from within iShare (e.g., PIMS, PMIS, OLC). Develop reporting and dashboarding capabilities within iShare and CRM. One example of this type of work was the creation of a web part within iShare which allows the display of user-specific information to each iShare user on their current training requirements, such as overdue training. The information was extracted nightly from OLC, and transferred to the iShare environment.
- 5) Develop a road map for My Sites enhancements and implement these enhancements. The implementation of SharePoint 2013 is currently being worked at the platform level, and potential changes to My Sites under SharePoint 2013 have not yet been completely addressed.
- 6) Provide advanced customizable workflows using Microsoft SharePoint, K2 BlackPoint, and/or Microsoft Dynamics CRM, and other similar products. Users of iShare can create simple workflows, including InfoPath forms routed to internal users. More advanced workflows have been created by the iShare team using SharePoint Designer. An example of a custom application developed by the iShare team, allowing more advance workflows, is CCMS (Controlled Correspondence Management System). CCMS was created by the iShare team as an application to allow routing and tracking of document reviews by and across several TSA offices.



**OGS Background:** The OGS Team Site was created under TSA iShare and tailored or customized to the business needs of OGS and its divisions. Each division's sub-site contains office/division-specific SharePoint out-of-the-box (OOTB) features. The OGS team site is currently operated and managed by the OGS Business Management Office (BMO) and Integrated Plans and Support (IPS) divisions. The IPS division is responsible for building site content, managing data in back-end lists, and developing InfoPath form workflow via the OOTB web front-end SharePoint interface.

In 2011, OGS reached out to the Office of Information Technology (OIT) Application Development Division (ADD) iShare team for requiring support use of the SharePoint Designertool. The support included:

1. Dashboard pages that consolidate data from multiple sources to provide relevant information
2. Enhanced look-and-feel of the site, including menu navigation and layouts
3. Custom workflows associated with existing InfoPath Forms (Microsoft Office 2010)
4. Additional Lists to support data management needs
5. Enhanced data quality and data management capability through list updates, data consolidation, and re-structuring

Since then, the support has gone through four phases:

1. Phase 1 Support Tasks included:
  - a. Creation of the Country Dashboard for Operational Status (OPSTAT). The dashboard displays Profile Information, training, Agreements and the National Information Report
  - b. Development of a search capability for the FAAP Document Library, that allows users to have quick and easy access to relevant documents
  - c. Assisting in lists cleanup activities to ensure data integrity
2. Phase 2 Support Tasks included:
  - a. Employed further assistance in list cleanup activities that ensure data integrity
  - b. Enhanced country dashboard with the addition of new tabs containing risk and compliance information.
  - c. Developed the Airport dashboard. The airport dashboard consolidates and synthesizes information stored across the OGS Team Site. Specifically it displays the following information associated with airports:
    - Risk data: Air Carrier Inspections, associated FAAP Documents, and SARP Assessments
    - Screening Equipment compliance information for passengers and cargo
    - Flight Data: Average weekly flights, BTS Data and carriers with direct flights to the US
  - d. Developed Air Carrier dashboard. The air carrier dashboard displays Air Carrier profile information, Inspections, IIR and GPE Assignments, as well as Amendments and Alternate procedures.
3. Phase 3 support tasks consisted of creating SharePoint workflows for lists and InfoPath enhancing the OPSTAT dashboards
  - a. Migrate FAAP Report Documents to new document library and improved the FAAP search capability for easy information finding.
  - b. Create workflows that cascade fields to maintain data integrity.
  - c. Update OPSTAT Dashboards by adding contacts to the Air Carrier and updating data sources for Agreements and Capacity Development

4. Phase 4 Support Tasks include reorganization, redesign of OGS Team Site pages for some OGS divisions and Operational and Maintenance (O&M) tasks using only SharePoint Out-of-The-Box (OOTB) functionalities. Specific Phase 4 tasks include launching pilot for redesign using the sub-site for Integrated Plans and Support (IPS) and follow with the complete OGS Data Environment.

**OLE/FAMS, OOS Background:** The OLE/FAMS OOS created the FASDS application on TSA's SharePoint applications infrastructure. FASDS is a robust, non-proprietary, integrated case management and risk assessment solution implemented in 2014. I know

Based on the initial implementation the stakeholders have requested enhancements and fixes to increase efficiency and ensure compliance with TSA policies and procedures. In December on 2014 OLE/FAMS OOS approved a Functional Requirements Document (FRD) that notes the changes required to enhance the OOS's ability to meet mission requirements by standardizing processes, procedures, checklists, and reports concerning physical security assessments. The enhancements will also provide specialized support for all types of assessments (including new construction/renovations, data network rooms, burn facilities, and office spaces).

**OLE/FAMS, SSA, Security, PerSec Background:** The OLE/FAMS, SSA, Security, PerSec and Physical Security (PhySec), Office of Information Technology (OIT) and Office of Acquisition (OA) are stakeholders in the tracking and reporting of contactor personnel for contractors assigned to TSA contracts. TSA Contracting Officer Representatives (CORs) need the capability to input and manage contractor personnel data for actions relating to adding, deleting and changing TSA contractor personnel data. A function is needed to notify the appropriate organizations of the any changes via email. Currently all TSA offices are without the capability of centrally tracking and reporting information related to: onboarding, off boarding, changes of contractor information, and COR related information. A Functional Requirements Document (FRD) was created in December 2014 detailing associated requirements.

**OLE/FAMS, Chief Security Office Background:** The OLE/FAMS, Chief Security Office, Security Appointment Center has been using a SharePoint InfoPath form for Visitor Request submissions. These requests contain professional personally identifiable information (PII) information that is submitted as a text file formatted for submission to the PassagePoint system used by the Security Guards. This data is not maintained in any system other than PassagePoint and does not provide the CSO with a repository for managing repetitive visitors. A Functional Requirements Document (FRD) was signed off on in February 2015 detailing the requirements need to design, develop and implement a more comprehensive system to meet the CSO and DHS requirements.

**OIA Background:** The mission of the TSA Office of Intelligence is to predict and assess threats to various transportation modes. Various systems currently in operation allow TSA OIA to plan, trace, review, and report on financials needed to support the mission. OIA has a need to enhance its OIA iShare presence, architecture, and capability to enhance communications and collaboration efforts in support of the OIA Strategic Plan initiatives.

### **SECTION III: Basic Requirements**

All applications will be hosted at a DHS Enterprise Data Center, unless TSA has an approved waiver from the DHS CIO or the application will be migrated to a DHS Enterprise Data Center and is listed in the TSA Data Center Migration Plan provided to DHS CIO.

The contractor will architect solutions per the ADD playbook (provided previously to all DASIS II contractors). All applications will follow an approved architecture prior to design and development.

Specifically, TSA requires the vendor to perform the following tasks:

## **A. REQUIREMENTS:**

### **TASK 1: iShare/Workflow Development & Technical Support**

This task provides development of new functionality, changes to existing functionality, and technical support and guidance. The technical support is generally related to the developed functionality and standard SharePoint functionality available to end-users, rather than support for the platform (hardware and operating systems) which is provided through a separate contract. The Government estimates the level of effort to be approximately 2,000 hours/month.

#### **Management and technical oversight:**

Management and technical oversight consists of the following activities:

- Maintain the overall iShare team schedule, staffing plan, pipeline forecast of upcoming projects and impacts.
- Provide direction and oversight for each project, ensuring quality and consistency between all projects and within projects.
- Provide support for knowledge transition from the outgoing iShare service provider to the future incoming iShare / Workflow service providers.
- Maintain the project status and other project information (currently stored in the internal TSA iShare repository), updating on at least a weekly basis.
- Attend meetings as-scheduled to discuss overall project issues, possible new projects and initiatives, and inter-project discussions. Examples of these meetings are weekly status meetings, meetings within TSA to understand emerging requirements in order to assess how (or if) the team can provide the services required, and meetings with the TSA OIT Enterprise Architecture (EA) staff.

#### **Technical activities:**

- The activities for this task refer to the customized content and applications. This scope is not expected to include any infrastructure (server, communications, etc.), which is separately maintained outside the scope of this effort.
- The project mix includes from 10 to 20 simultaneous separate taskings, including maintenance efforts. The approximate project mix active *at any time* is expected to require 10 non-managerial oversight resources, and may be:
  - **Small** (historically less than half-time attention for one intermediate-level person, with 1-4 hours per week management/senior technical oversight) – 10-20 projects (averaging an estimated 60% of total active projects). These projects may last from 2 to 8 weeks, requiring mostly requirements-gathering, browser-based customization, content editing, and testing. Examples of a small project include (1)

site enhancements for the iShare pages belonging to a TSA office such as Office of Human Capital (OHC), and (2) performing initial project scoping and planning for a medium or large project under consideration.

- **Medium** (historically full-time attention for about one intermediate or senior-level person, with 1-5 hours per week management/senior technical oversight) – 3 to 6 projects (averaging an estimated 25% of total active projects). These projects may last from 3 to 12 weeks, requiring the same skills as small projects, with potential for analysis and system design. An example of a medium-sized project is completing a small development bug-fix to a custom-coded app, and working the change through the standard testing process before promoting to production deployment.
- **Large** (historically small teams of two to three people, junior to senior level, with part-time management/senior technical oversight) – 2 to 4 projects (averaging an estimated 15% of total active projects). These projects may last 6 to 24 weeks, requiring the same skills as medium projects. An example of a large-sized project is a tasking historically requiring 2 to 3 people for an important initiative which was originally created by the end-user via browser-based techniques, but now requires multiple enhancements using SharePoint Designer via work in a development environment which is tested and promoted to production deployment. Work done to create CCMS was a large project lasting several months, including analysis of the old system (non-SharePoint), requirements gathering and refinement, designing and developing the new (now current) CCMS, extensive user testing, migration planning, final data migration and cutover, and post-migration support.
- Perform software development and customization work for DIT-approved iShare projects, or as directed in time-sensitive or critical initiatives. The primary method of OIT approval are tasking documents, which define the scope and estimated resources required for the tasking to complete.
- Perform software development, analysis, and customization work for these on-going areas of responsibility as available work load allows:
  1. Maintain and enhance **TSApedia** – a wiki (collaboratively built encyclopedia) that will become the “encyclopedia of TSA knowledge”. Maintenance activities are expected to be infrequent updates to user-contributed content, along with enhancing the look-and-feel (such as navigation, web parts, and permissions) of this part of the existing iShare site.
  2. Maintain and enhance **Blog Central** – a collection of enterprise blogs (web journal that contains commentary, opinions or other material which allow readers to respond via open comments) that will enable employees to share their current thoughts, experiences, and opinions on areas for which they have some authoritative knowledge.
  3. Maintain and enhance the **Directives & Forms Library** – a central repository of official TSA policy documents and forms.

4. Maintain and enhance **My Site** (SharePoint personal sites, internal to TSA) capabilities—including the ability to organize content and dashboards, maintain profile/contact information, blog, and share information to others with both a public view and private view.
5. Develop iShare **Team Sites** (team-level collaboration sites, internal to TSA) for HQ and field office communities/organizations including:
  - a. Developing a structured and prioritized approach for the roll out of team sites to TSA HQ and the field. Team sites exist for TSA offices, and Team Site development will be needed as existing office priorities and focus evolve, and as a result of any TSA office reorganizations in the future.
  - b. Developing team site templates.
  - c. Supporting the development and delivery of iShare training, to allow the iShare Team Site users and administrators to use and maintain the site (such as best practices for content updates). Typically, training is conducted live in one or two sessions as a new Team Site is completed. The training sessions usually have an estimated 1 to 10 attendees. The iShare training development frequently is accomplished by creating user guides which are used as a reference during (and after) training. Additional slides or presentation materials may also be created. The nature of the training is not a formal course-type, and typically does not involve quiz or test material.
6. Enhance iShare **Governance** including:
  - a. Supporting the establishment of and adherence to policies and procedures for governance. This support is generally the contribution of knowledge to existing governance documentation, and to apply this knowledge to the functional (user) and technical operation of iShare.
  - b. Design, implement, and enhance capabilities to monitor iShare for compliance and conducting audits.
7. Implement **Record Management** capabilities. As TSA migrates from SharePoint 2007 and SharePoint 2010 to the use of SharePoint 2013 and newer versions, it is anticipated that the use of the SharePoint records management features will be utilized within iShare, most likely using SharePoint 2013's features. This effort will require the iShare team to provide knowledge on implementation aspects, and to update some sites to incorporate records management.
8. Design and develop custom SharePoint applications and web parts, including integration with external systems and data sources to enable true portal functionality and dashboarding. Examples of data sources include SQL databases (some of these are used to more effectively manage SharePoint 2007/2010 list sizes above a few thousand items). An example of external integration is creating interaction with external mapping services (Bing, Google/Google Earth).
9. Design and develop custom applications on products like .NET, including integration with internal and external systems, for advanced workflow (business process) requirements.

10. Subject to EA (Enterprise Architecture) guidance and platform availability, design and develop custom Dynamics CRM information system applications, including integration with SharePoint and other internal and external systems.
11. Perform other necessary activities related to the successful design, development, operation, and maintenance of iShare and other iShare related platforms as needed.

## **TASK 2: OGS SHAREPOINT TEAM SITE SUPPORT**

The overall objective of this task is to provide SharePoint development, operation & maintenance support and business process improvement services across the OGS data environment, improving information sharing and data collaboration. Historically, the work has been performed by a team of 2.5 FTE. Consolidating common information across OGS divisions will make data more accessible and provide business insight for better-informed decisions. The improvement of the OGS data environment will support the OGS mission: to develop and promote the implementation of effective/enhanced global transportation security processes and structures worldwide, while ensuring compliance with international and TSA standards.

### **1. Data Consolidation**

- 1.1. Current – The current data sources include information collected and stored within the OGS Team SharePoint (SharePoint Lists, Calendars, InfoPath Forms and mission oriented information from Capacity Development/Training, Outreach activities, Compliance Inspections/Assessments, Reference Lists/Look-up Lists, and data from other systems). The data solution, internally referred as OPSTAT dashboards, was created as an integrated information sharing platform designed to share OGS program data with all OGS employees. This tool standardizes answers to routine data calls and provides staff with information from which they can conduct meaningful analysis.
- 1.2. Enhanced Capability – Expand and Integrate Data Sources from both external and internal locations to provide a more robust and comprehensive data collection, consolidation, and analysis system. Additionally, the system will continue consolidating more data sources as they are available from both public and private sectors as well as from other TSA or DHS systems.

### **2. Process and Program Automation**

- 2.1. Current – OGS Activities and Mission areas are tracked in a variety of formats depending on projects identified. The formats include, but are not limited to: Microsoft Excel, InfoPath and SharePoint.
- 2.2. Enhanced Capability – Provide process and program tools for automation of data collection for items such as National Information Report (NIR), OGS Trip Tracker, International Agreements Process, Protocol Forms, BMO Personnel Tracker, OGS Contact Form Process, Equipment Loan Request Form, OGS Activity Sandbox, and other mission related data collection efforts.

### **3. Reporting**

- 3.1. Current – The service provided the creation of reporting dashboards, internally titled “OPSTAT”, created through the SharePoint Designer interface. SharePoint provides dashboard with data from several SharePoint Lists, Document Libraries, and Form Libraries.
- 3.2. Future Capability – The services will continue to provide development of custom reporting. Reports will be customized to the user’s needs and will create timely, accurate reporting across all directorates. The services will continue to leverage collected data and other relevant data sources as inputs into centralized reporting dashboards which provide leadership decision-making tools, predictive analysis, and resource management capabilities.

### **4. User Interface Enhancement**

- 4.1. Current – The Office of Global Strategies Team Site was redesigned in phase 4 (initiated with a pilot launch for redesign using the sub-site for Integrated Plans and Support (IPS) and follow with OGS Team Site.)
- 4.2. Future Capability – Redesign OGS Team Site based on the progressive elaboration of business requirements, and additional mission needs. Provide enhanced access to information and processes based on user requirements.

### **5. iShare application development initiatives: support the redesign of office, directorate, and team-based iShare sites and pages, as well as on maintaining the OGS site structure and contents and collaborating with OGS representatives to guide users towards system and application best practices.**

- 5.1. Development initiatives will include a variety of tools and design efforts that will automate tasks and leverage large amounts of information through iShare to make informed decisions driving the OGS mission. Tasks that will be served include but not limited to directorate site redesign efforts (five directorates), developing a series of Community Sites designed to provide a forum for OGS employees on particular topics (Cognos, etc), performing a large amount of data migration to repurpose the OGS Expansion iShare site and consolidate overlapping workstreams, the completion of TSA PreClearance dashboards, the development of a Risk Working Group site.
- 5.2. Additional initiatives include process optimization, further development of site analytics, guidance documentation for new and redeveloped tools, and the migration and deployment of an office-wide travel request system.

### **TASK 3: OLE/FAMS, OOS FASDS ENHANCMENTS SUPPORT**

This task provides OLE/FAMS OOS with support for their continued efforts to upgrade, design and deploy enhancements and additional features needed for the Facility and Security Data System (FASDS) application. The OOS intends to enhance and fix the FASDS application to increase efficiency and ensure compliance with current DHS/TSA policies.

The FASDS development support (an optional task) is dependent on funding availability. If approved, it is

anticipated that this task will be exercised in October 2016.

TSA requires the vendor to perform the following:

**Management and technical oversight:**

- Maintain the overall team schedule, staffing plan, and pipeline forecast of upcoming efforts and impacts.
- Provide direction and oversight of project, ensuring quality and consistency of the development effort.
- Maintain the status and other project information (currently stored in the internal TSA iShare repository), updating on at least a weekly basis.
- Attend as-scheduled meetings to discuss overall project issues. Examples of these meetings include weekly status meetings as well as meetings with the TSA OIT Enterprise Architecture (EA) staff.

**Technical activities:**

- Continue design, development, and coordination efforts for the deployment of a flexible – SharePoint solution that can be updated and maintained by the customer
- This scope is not expected to include any infrastructure (server, communications, etc.), which is separately maintained outside the scope of this effort.

**Enhancement activities:**

- Upgrade application from SharePoint 2007 to current TSA SharePoint platform
- Enhance current user roles and permissions
- Enhance and correct current email notifications
- Modify fields to include adding, deleting, editing and relocating to relevant areas
- Enhance the Risk Assessment capabilities to meet DHS/TSA policy requirements
- Add Risk Identification Calculator to derive Risk Scores based on ISC established Risk Assessment Event Areas.

**TASK 4: OLE/FAMS, SSA, SECURITY, PERSEC, ENTERPRISE CONTRACTOR DATABASE SUPPORT**

This task provides OLE/FAMS, SSA, Security, PerSec with continued support to complete the SharePoint design, development and deployment of an application needed to support the tracking and reporting of contractor personnel assigned to TSA contracts. OLE/FAMS, SSA, Security, PerSec intends to create, deploy, enhance and fix the Enterprise Contractor Database (Contractor Evaluation and Tracking Database (CETS)) application to increase efficiency of tracking and reporting of TSA contractor personnel and ensure compliance with current DHS and TSA policies and procedures.

The Enterprise Contractor Database (Contractor Evaluation and Tracking Database (CETS)) development support (an optional task) is dependent on funding availability. If approved, it is anticipated that this task will be exercised in October 2016. TSA requires the vendor to perform the following:

**Management and technical oversight:**



- Maintain the overall team schedule, staffing plan, and pipeline forecast of upcoming efforts and impacts.
- Provide direction and oversight of project, ensuring quality and consistency of the development effort.
- Maintain the status and other project information (currently stored in the internal TSA iShare repository), updating on at least a weekly basis.
- Attend as-scheduled meetings to discuss overall project issues. Examples of these meetings include weekly status meetings as well as meetings with the TSA OIT Enterprise Architecture (EA) staff.

#### **Technical activities:**

- Complete the design, development, and coordination for the deployment of a flexible solution in a centralized location that can be updated and maintained as contractor personnel are added, changed and deleted and as office reorganizations are implemented.
- The solution should be easy for TSA Contractor Officer Representatives (CORs) to use without requiring training and provide all stakeholders the ability to access and report on contractor personnel information.
- Automate the reconciliation process for contract data from the OADB into CETS and develop a web service interface into the DHS Integrated Security Management System (ISMS). Provide Operations and Maintenance (O&M) support for the Contractors Evaluation Tracking System (CETS) to include answering help questions, troubleshooting, code break/fix, minor enhancements and data refresh for the Office of Acquisition Database (OADB) contract export. The OADB export will be provided in a standard Excel spreadsheet and should be imported into the CETS contracts list.
- This scope is not expected to include any infrastructure (server, communications, etc.), which is separately maintained outside the scope of this effort.

#### **TASK 5: [RESERVED]**

#### **Task 6: OIA Strategic Communications (Optional Task)**

OIA requires SharePoint site development and support to expand the functionalities of existing SharePoint sites for use by the following OIA divisions/branches:

- OIA Strategic Communications Branch
- OIA Business Management Office (BMO) Division
  - Budget, Finance, and Acquisitions (BFA) Branch
  - Human Capital & Workforce Development and Training Branch
  - Mission Readiness Branch
- Screening Portfolio Branch
- Counter Terrorism Branch
- Threat Analysis Division (TAD)
- Vetting Analysis Division (VAD)
- Field Intelligence Division (FID)
- Program Management Division (PMD)
- Risk Analysis Division (RAD)

- Mission Architecture & Process Innovation (MAPI)

#### **Management and technical oversight**

- Knowledge and experience in project management (PM) principles such as planning, tracking, and requirements solicitation
- Experience with program and process development
- Ability to evaluate procedures and provide methodologies to develop reliable processes
- Ability to develop evaluate current requirements and provide modernized technical solutions to enhance digital processes

#### **Technical activities**

- Ability to develop in a unique SharePoint environment
- The Contractor shall provide the application development skillsets to support iShare development. Contractor must have knowledge of the following skills:
  - JQuery
  - JavaScript
  - HTML
  - CSS
  - SharePoint Designer
  - Current SharePoint environment and object model
  - C#
  - SQL Server
  - Linq
- Site development unique to each OIA division, prioritized by government Project Manager
- Manage solicited requirements and prioritize based upon system development complexity and level of effort for TSA management acceptance
- Develop Standard Operating Procedures to assist users
- Develop unique site capabilities according to requirements and site capabilities
  - Site capabilities should include but not limited to site layout, graphics, navigation, lists, calendars, surveys, and customer workflows
  - Out of the box site development within site collections using webparts, HTML, Javascript, and JQuery
- Develop and document process to gain OIT approval of unique custom automation, and execute that process for any requirements needed
- Establish a requirements intake and review process
  - Establish and document Requirement Review Board charter
  - Develop and automate requirement intake process for all OIA iShare requirements
  - Establish weekly review of all new and current requirement/project statuses
  - Establish and automate the ability to track requirement/project statuses
- Establish a user testing and acceptance process
  - Establish, document, and execute a user testing and acceptance process for all user requirements implemented
  - Include in all project plans a reasonable amount of time for user testing
  - Develop and document a user testing plan/manual
- Enable access to external data
  - Enable links within SharePoint environment to external data
  - Import and maintain access to external data

- Ability to conduct Site Management and Maintenance
  - Ability to manage and maintain site content
  - Ability to manage users and user permissions
  - Provide site administrator support

#### **Training**

- Provide on-site user testing for customer acceptance and approval
- Develop and maintain user manuals, instructions, and training materials
- Develop and facilitate classroom and desk-side user training

### **B. PROGRAM MANAGEMENT REQUIREMENTS**

#### **1. Program Management Service**

- 1.1. Provide program management services that assist the government in planning, executing, controlling and delivering the support taskings on time and within cost. Provide timely and accurately programmatic, cost, schedule and performance information to the Government.
- 1.2. Develop Integrated Master Project Plan (update weekly), minimum coordination requirements :
  - 1.2.1. Release Configuration and Change Management (RCCM) for release planning, Application Support Team (AST) Testing and Request for Change (RFC) support
  - 1.2.2. Operational Engineering Division (OED) for deployment support
  - 1.2.3. Section 508 Testing support.
  - 1.2.4. Enterprise Architecture Division (EAD) for design review
  - 1.2.5. IT Security Division for security review and scanning
- 1.3. Establish a sound risk management system. Identify and mitigate risks.

### **C. APPLICATION ENGINEERING REQUIREMENTS**

#### **1. Requirement Definition**

- 1.1. Work with application users and other OIT stakeholders to gather, analyze, and document detail requirements that are accurate, unambiguous and verifiable.
- 1.2. Requirements include functional and non-functional requirements, such as security compliance, section 508 compliance, system performance, design constraints, environment constraints and data requirements.
- 1.3. Analyze business process that results in improvement of business operations
- 1.4. Identify requirements from any appropriate external source, including GAO findings, current applicable business processes, TSA & DHS technical requirements/policy/guidance.
- 1.5. From all gathered requirements, establish the baseline for a given business target date or a target scope.

## **2. Design:**

- 2.1. Transform the baseline requirements into comprehensive, logical and detailed designs to efficiently and effectively guide for implementation.
- 2.2. For complex changes that require design review, work with the OIT Enterprise Architecture Division (EAD) to plan and execute Preliminary Design Review (PDR) and Critical Design Review (CDR) for the solution.
  - 2.2.1. Create, submit, brief all design artifacts for the designed solution that are required at PDR and CDR (System Design Document, Data Management Plan, Data Asset Profile, Conceptual Data Model, Logical Data Model, Physical Data Model, Data Dictionary, Entity Relationship Diagram, Data Migration Plan, Data Quality Plan).
  - 2.2.2. Remediate and update design artifacts as required for final design approval

## **3. Development**

- 3.1. Use the OIT approved development tools and development environments to perform development and SharePoint customization activities.
- 3.2. Develop reliable, efficient, secure and maintainable codes.
- 3.3. Use the approved Configuration Management (CM) tools (TSA OIT is currently using CollabNet and subversion) to manage source code control and timely check in development artifacts, such as script, platform pages, or codes.
- 3.4. Incrementally develop functionalities in iterations, allowing the government to review and provide feedbacks.

## **4. Integration and Testing**

- 4.1. Testing shall be in accordance with TSA guidance (coordinate with other IT environment service providers as required)
- 4.2. Testing shall be completed using the Office of Information Technology (OIT) development and test environment and infrastructure resources (work with other Testing Infrastructure support groups as required)
- 4.3. Support the stand-up of the testing applications in the Development Test Environment (DTE), Integrated Test Environment (ITE).
- 4.4. Work with appropriate release management groups, including but not limited to Application Development Division (ADD) Release Change and Configuration Management (RCCM), TSA Release Management, to submit required artifacts for promoting the applications into test environments.
- 4.5. Perform the end-to-end testing to demonstrate that the solution developed satisfied the requirements. Provide Test Analysis Report (TAR) to report test results.
- 4.6. Plan and conduct the User Acceptance Testing (UAT) with the government
- 4.7. Work with appropriate groups to support their independent testing, verify the findings and provide remediation's for valid findings in these testing's, minimum including:
  - 4.7.1. The Application Support Team (AST) independent testing of functional requirements.
  - 4.7.2. OIT IAD (Information Assurance Division) and iShare ISSO : security testing and scanning.
  - 4.7.3. Section 508 Coordinator: 508 Accessibility testing.
  - 4.7.4. Other testing as directed by the government, such as load testing, performance testing.
- 4.8. Collect, document, track and report defect data.

## **5. Implementation:**

- 5.1. Provide services to implement the required changes into a production state
- 5.2. If the changes require approval from release management, work with appropriate release management groups and participate in the Change Control Process to submit required artifacts and obtain the approval of the software promotion into Production. Activities include but not limited to:
  - 5.2.1. Coordinate with Release Management for resource, to support the preparation of operational sites and the deployment of solution to production environment
  - 5.2.2. Submit Request for Change (RFC)
  - 5.2.3. Attend Change Control Board (CCB) meetings to brief CCB stakeholders on the solution deployments
- 5.3. Work with other IT infrastructure support groups to implement changes into production as needed.
- 5.4. Perform “smoke testing” to verify the changes after the implementation
- 5.5. Support communication to all stakeholders on the deployment
- 5.6. Transition the implemented changes to the application administrators.

## **6. Training**

- 6.1. The training historically has been a mix of:
  - interactive one-on-one for short time periods (one hour)
  - a conference-room 5-25 attendee presentation style (for one to two hour time periods)
  - online screen-sharing training of 1 to 10 people, which did not require in-person attendees (for one to two hours).
- 6.2. Historically, there has not been a dedicated training resource or specific course-development resources. Material has been developed in minutes to hours, mostly using existing project resources and documentation.
- 6.3. The training historically has been primarily associated with a release (new functionality), or with training users who started using a system after it was released. The number of training sessions occurred as one time sessions, or as a cluster of 2-4 sessions within a few weeks.
- 6.4. The overall LOE for training needs historically has not been tracked, but is estimated to have been less than ¼ of an FTE.
- 6.5. Projected training needs for the type and frequency of sessions are similar to historical patterns. The training activities will require providing live user training/instruction sessions, typically including a User Guide or summary presentation materials if there are more than one or two attendees.

## **7. Configuration Management:**

Use the approved Configuration Management (CM) tools to:

- 7.1. Maintain proper configuration management for System Engineering Life-Cycle (SELC) artifacts under TSA guidance.

- 7.2. Perform timely and accurate document and source code control for applications: ensure all code and document artifacts that were developed for the applications are checked in the code repository.

#### **D. KNOWLEDGE TRANSFER REQUIREMENTS**

1. At contract termination, effectively coordinate transfer of knowledge to the new contractor.
  - 1.1. Implement an orderly and efficient transition with new contractor within 45 days of the contract termination, to ensure that the required services are performed without interruption.

#### **E. OPERATIONS AND MAINTENANCE REQUIREMENTS**

1. Present an operations and maintenance (O&M) support plan that addresses the key areas of the applications.
2. Maintenance support includes Break fixes that all activities require for diagnosing, debugging, development/coding, assisting with promoting the software to production, and performance quality assurance on software defects after the software becomes operational.
3. The TSA Application Support Team (AST) provides some O&M support but not all. The contractor shall coordinate all O&M activities with the AST to ensure reduced/elimination of duplicative O&M.
4. Post Production/Deployment Software Support:
  - 4.1. Provide a minimum 30-day maintenance support for the applications in production after the deployment of changes until the site has been transitioned to Application Support Team (AST).
  - 4.2. Under Release Change and Configuration Management (RCCM) process, provide knowledge transfer to AST, to transition the applications to AST for production issues support.
  - 4.3. Work with COTS vendors and other TSA IT support groups such as TSA help desk (SPOC), Application Support Team (AST), Information Technology Infrastructure Program (ITIP) support teams to log, investigate, troubleshoot and resolve applications issues.
5. Provide assistance to applications trainers or application administrator users on application use and functionality.
6. Develop and implement remediation for security Plan of Action and Milestones (POA&Ms) and Section 508 Accessibility POA&Ms as needed.
7. Perform regression tests, system validation for applications against scheduled or unscheduled infrastructure maintenance (SharePoint, Windows Operating System) and for system recoveries after major outage in test and production environments (DTE, ITE and PROD)
8. As the operational production environments and technologies are upgraded to SharePoint 2013, SharePoint 2016, Windows 10, etc., support the upgrade of the supported applications into these new environments. Perform regression tests and other updates to resolve issues and make the applications operational in these new upgraded environments.

### **SECTION IV: Deliverables and Performance Metrics**

#### **A. DELIVERABLES**

The deliverables shall be delivered to the COR and CO in accordance with the deliverables schedule. All deliverables will be provided in DHS SELC where templates are available.

The initial format for most deliverables will be a standard Microsoft Office format. However, ADD is continuing to evolve its application development process and practices including the adoption of new

technologies to enhance the management of applications development efforts. The contractor shall use these new technologies including in the submission of deliverables.

Specifically, the use of the OIT Project Tracker will be used for project management and status reporting. CollabNet will be used for configuration management and the submission of source code and associated artifacts including functional requirements, design documents, test scripts, etc.

The TSA TimeTracker application will be used by contractors to record time spent on any given task or project. The TSA TimeTracker application is not an official time keeping mechanism for the Government, but it will be used for reporting purposes and for invoice verification.

Variances reported will be tracked in accordance with current ADD reporting requirements; significant variances on a tasking (i.e. planned vs. actual labor hours) will be reported with an explanation for the cause of the variance.

**The following apply to all tasks:**

#	Deliverable	Due Date	Deliverable Recipient	Deliverable Format*	Reference (specify CDRL, attachments, etc.)
1	Weekly Status Report (by task)	Weekly, by COB Monday, for the prior week.	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
2	Project Mgmt Plan & Project Schedule (by task)	2 Weeks after Kickoff Meeting, Updated Weekly	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
3	Weekly Burn (by task)	Weekly, by COB Monday, for the prior week.	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
4	Monthly Burn (by task)	Monthly, by COB of the second Monday of the month, for the prior month.	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
5	Requirements Document– signed off	Per Release, as determined in Project Plan, updated if needed	CO,COR, TM	MS Office	(1) Hard Copy; (1) Soft Copy
6	Systems Designs Document (SDD) and Design Approval	Per Release, as determined in Project Plan,	CO,COR, TM	MS Word	(1) Hard Copy; (1) Soft Copy

#	Deliverable	Due Date	Deliverable Recipient	Deliverable Format*	Reference (specify CDRL, attachments, etc.)
		updated if needed			
7	User Guide or Manual for end users and application admin.	Per Release, 5 business days before UAT	CO,COR, TM	MS Word / MS Visio	(1) Hard Copy; (1) Soft Copy
8	User Acceptance Testing (UAT) Session	Per Release, as determined in Project Plan.	TM, customer (OGS for OGS task, FAMS for FAMS task)	Session	UAT artifacts
9	User Acceptance Testing sign-off document	5 business days after UAT completed	CO,COR, TM	Word document	(1) Hard Copy; (1) Soft Copy
10	Developed releases, including all source code, build scripts and configurations that are needed to construct, build the applications.	Per release, 5 business days before release in production, updated if needed	CO,COR, TM	In CollabNet & Subversion or other T5A CM repositories. Provided links to locations.	(1) Hard Copy; (1) Soft Copy
11	Software Deployment Document (describe how to deploy, configure and install the built software package onto different environment)	Per release, 5 business days after release in production, updated if needed	CO,COR, TM	In CollabNet & Subversion or other T5A CM repositories. Provided links to locations.	(1) Hard Copy; (1) Soft Copy
12	User Training Sessions	1-6 weeks before or after deployment, as determined in Project Plan	TM, customer (OGS for OGS task, FAMS for FAMS task)	Demo, Presentation Slides, Training Session	Training Meeting Minutes. Training Materials.
13	AST Knowledge Transfer Sessions	Per release, 4-8 weeks before and after deployment.	AST, TM, customer (OGS for OGS task, FAMS for FAMS task)	Sessions & Knowledge Transfer artifacts.	Knowledge transfer artifacts.



#	Deliverable	Due Date	Deliverable Recipient	Deliverable Format*	Reference (specify CDRL, attachments, etc.)
14	Transition-Out Plan (to the new contractor)	60 days from Contract Termination	CO, COR, TM	MS Office	(1) Hard Copy; (1) Soft Copy

**The following applies to task 1:**

#	Deliverable	Due Date	Deliverable Recipient	Deliverable Format*	Reference (specify CDRL, attachments, etc.)
15	iShare Governance Documentation	Updated as needed	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy

**The following applies to tasks 1, 2, and 4:**

#	Deliverable	Due Date	Deliverable Recipient	Deliverable Format*	Reference (specify CDRL, attachments, etc.)
16	Test Plan & Test Scripts	Updated as needed	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
17	Test Results Document	Updated as needed	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
18	RFC and CCB Documentation	Updated as needed	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy
19	Data Management Plan**	90 days after first team member is cleared to begin work.	TM/ CO/ COR	MS Office	(1) Hard Copy; (1) Soft Copy

\*\* In accordance with the DHS SELC and guidance from the Enterprise Architecture Division (EAD, see Section IV, E.), the contractor will develop a Data Management Plan to address the management of data

in accordance with TSA policies and standards.

**The following applies to task 3:**

20	Defects and backlog List	5 business days after UAT completed	OGS, TM	Word document	(1) Hard Copy; (1) Soft Copy
----	--------------------------	-------------------------------------	---------	---------------	---------------------------------

**B. PERFORMANCE METRICS**

#	Performance Metrics
1	Did contractor deliver all required reports, document artifacts within one week of due date?
2	Did contractor deliver code that was 80% free of bugs and defects?
3	Did contractor develop test plans, test the developed apps and produce the TAR?
4	Did contractor build enterprise SharePoint/K2/CRM apps that did not exceed platform operating capabilities (CPU utilization)?
5	Was the contractor proficient in the use of Microsoft's SharePoint when coding SharePoint development projects? Demonstration of this for code is an average of less than 2 deployments to the ITE (pre-production integration) environment for each release.
6	Was the contractor proficient in the use of Microsoft's Dynamic CRM when coding CRM development projects? Demonstration of this for code is an average of less than 2 deployments to the ITE (pre-production integration) environment for each release.
7	Did contractor manage projects using a "tasking model" whereby hours and deliverables were tracked accordingly and entered into DIT's Time Tracker?
8	Did contractor coordinate with TSA IT security personnel (as needed) to evaluate security findings and made recommendations to GPM within specified timeframe?
9	Application deliverables should be delivered no later than two(2) week as specified in Project Schedule in individual tasking project plans and RCCM Release Plans
10	Did contractor manage requirements, artifacts and code using TSA's CollabNet and Subversion service?

The *Performance Metrics*, shown in the table above, documents the Government's expectations concerning performance under this Work Order. *Rating values equate to: 5 = Always performed by due date; 4 = Always performed within one week (7 calendar days) of due date; 3 = Always performed within 10 calendar days of due date; 2 = Always performed within two weeks (14 calendar days) of due date; 1*

*= Did not perform or occasionally performed by due date.*

The consequences of the inability to meet these metrics will result in a Contractor Performance Report from the COR to the CO, for CPAR (Contractor Performance Assessment Reporting) consideration.

### **C. Transition Support**

At the completion of performance of this task order, the contractor shall fully support the transition of the work identified to be transitioned to another entity, either government or a successor offeror(s). The contractor shall assist with transition planning and shall comply with established milestones and schedules of events.

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

- Inventory and orderly transfer of all GFP, to include hardware, software, and licenses, Contractor Acquired Government Property, and Government Furnished Information (GFI)
- Transfer of documentation currently in process
- Transfer of all software analysis & design in process
- Certification that all non-public DHS information has been purged from any contractor-owned system
- Exchange of accounts to access software and hosted infrastructure components
- Participate in knowledge transfer activities in accordance with the transition plan
- Provide members to and participate in transition management team

If the government provides a Transition Plan template, the contractor shall complete this template as assigned, otherwise the contractor shall submit a Transition Plan at the direction of the government. The Transition Plan shall:

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

A Transition Plan shall be delivered 30 calendar days prior to the task order expiration date or, if directed by the government, 30 days prior to the end of each option period. The Transition Plan shall include support activities for all transition efforts for follow-on requirements to minimize disruption of services. The contractor shall account for a 10-business day Government review process prior to transition execution. The 10-day review and approval process is not included in the 30-day transition activities.

Transition support shall commence 30 business days prior to expiration of the Task Order. Upon award of a follow-on contract, the incumbent contractor will work with the new contractor to provide knowledge transfer and transition support, as required by the COR and PM.

**AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT**

2. AMENDMENT/MODIFICATION NO. PG0001		3. EFFECTIVE DATE See Block 16C	4. REQUISITION/PURCHASE REF. NO. 2416206CT0631	1. CONTRACT ID CODE	PAGE OF PAGES 1 / 1
6. ISSUED BY OFFICE OF ACQUISITION 701 S 12TH STREET ARLINGTON VA 20598	CODE 20	7. ADMINISTERED BY (If other than Item 6) TSA INFRASTRUCTURE 701 S 12th St. ARLINGTON VA 20598		5. PROJECT NO. (If applicable)	CODE 03

B. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code) INTERNATIONAL BUSINESS MACHINES CORPORATION Attn: (b)(6) 6710 ROCKLEDGE DR BETHESDA MD 208171826		(x) 9A. AMENDMENT OF SOLICITATION NO.
CODE 935130485		9B. DATED (SEE ITEM 11)
FACILITY CODE		(x) 10A. MODIFICATION OF CONTRACT/ORDER NO. HSTS03-13-A-CT0549 HSTS03-16-J-CT0631
		10B. DATED (SEE ITEM 13) 09/30/2016

**11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS**

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

12. ACCOUNTING AND APPROPRIATION DATA (If required)  
See Schedule

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

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
X	D OTHER (Specify type of modification and authority) 5200.237-004 Contractor Responsibility, Conduct and Performance under TSA Service Contracts (Jan 2016)

E. IMPORTANT: Contractor  is not,  is required to sign this document and return \_\_\_\_\_ copies to the issuing office.

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

GSA Contract #: GS-35F-4984H

Tax ID Number: 13-0871985

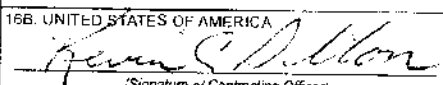
DUNS Number: 835130485

The purpose of the subject modification is to change Key Personnel.

Key Personnel position of Project Manager is hereby changed from (b)(6) to (b)(6)

All other terms and conditions remain unchanged.

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

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print) Kevin C. Dillon	
15B. CONTRACTOR/OFFEROR  (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA  (Signature of Contracting Officer)	16C. DATE SIGNED 10/22/16

**AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT**

1. CONTRACT ID CODE

PAGE OF PAGES

2. AMENDMENT/MODIFICATION NO.

3. EFFECTIVE DATE

4. REQUISITION/PURCHASE REQ. NO.

5. PROJECT NO. (if applicable)

6. ISSUED BY

CODE

20

7. ADMINISTERED BY (if other than Item 6)

CODE

03

OFFICE OF ACQUISITION  
701 S 12TH STREET  
ARLINGTON VA 20598

TSA INFRASTRUCTURE  
701 S 12th St.  
ARLINGTON VA 20598

8. NAME AND ADDRESS OF CONTRACTOR (No., street, county, State and ZIP Code)

INTERNATIONAL BUSINESS MACHINES CORPORATION  
Attn: (b)(6)  
6710 ROCKLEDGE DR  
BETHESDA MD 208171826

9A. AMENDMENT OF SOLICITATION NO.

9B. DATED (SEE ITEM 11)

10A. MODIFICATION OF CONTRACT/ORDER NO.

HSTS03-13-A-CIO549  
HSTS03-16-J-CIO631

10B. DATED (SEE ITEM 13)

09/30/2016

CODE 835130485

FACILITY CODE

**11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS**

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

12. ACCOUNTING AND APPROPRIATION DATA (if required)

See Schedule

Net Increase:

\$781,749.40

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

CHECK ONE	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF _____.
X	D. OTHER (Specify type of modification and authority) FAR 52.217-9 - Option to Extend the Term of the Contract.

E. IMPORTANT: Contractor  is not.  is required to sign this document and return \_\_\_\_\_ copies to the issuing office.

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

GSA Contract #: GS-35F-4984H

Tax ID Number: 13-0871985

DUNS Number: 835130485

The purpose of the subject modification is to exercise CLINs 10001 and 10002 Option Period One.

The period of performance is hereby extended from February 3, 2017 through June 3, 2017.

The total funding under the Task Order is increased from \$1,083,574.07 by \$781,749.40 to \$1,865,323.47.

Continued ...

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

15A. NAME AND TITLE OF SIGNER (Type or print)

16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)

Kevin C. Dillon

15B. CONTRACTOR/OFFICER

15C. DATE SIGNED

15B. UNITED STATES OF AMERICA

16C. DATE SIGNED

(Signature of person authorized to sign)

(Signature of Contracting Officer)

1/12/17

NSN 7540-01-152-8070

Previous edition unusable

STANDARD FORM 30 (REV. 10-93)

Prescribed by GSA

FAR (48 CFR) 93.243

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
 HSTSC3-13-A-C10549/HSTS03-16-J-C10631/P00002

PAGE 2 OF 3

NAME OF OFFEROR OR CONTRACTOR  
 INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
10001	<p>All other terms and conditions remain unchanged.                      Discount Terms:                          Net 30                      FOB: Destination</p> <p>Change Item 10001 to read as follows (amount shown is the obligated amount):</p> <p>CHIN 10001 - iShare/workflow Development &amp; Technical Support - Option Period</p> <p>Delivery Location Code: TSA11                      OFFICE OF INFORMATION TECHNOLOGY                      701 S 12TH STREET                      Attn: Akoua Enow                      Arlington VA 20598                      Accounting Info:                      5CST178A000D201VMSPO10GE000075006700679020-67050000                      00000000-251D-TSA DIRECT-DEF. TASK-D                      Funded: (b)(4)                      Period of Performance: 02/04/2017 to 06/03/2017</p> <p>Authorized Labor Categories:</p> <p>Project Manager (b)(4) /hour and (b)(4) /hour                      Subject Matter Expert (Government) (b)(4) /hour and (b)(4) /hour                      Subject Matter Expert (Contractor) (b)(4) /hour and (b)(4) /hour                      Systems Architect (b)(4) /hour and (b)(4) /hour                      Project Manager (b)(4) /hour and (b)(4) /hour                      Business Process Reengineering Specialist (b)(4) /hour and (b)(4) /hour                      Application Developer/Programmer (b)(4) /hour and (b)(4) /hour                      Applications Engineer (Intermediate) (b)(4) /hour and (b)(4) /hour</p> <p>NTE Hours 4,466                      NTE Dollars (b)(4)</p>	1	CB	(b)(4)	
10002	<p>Change Item 10002 to read as follows (amount shown is the obligated amount):</p> <p>CHIN 10002 - OGS Sharepoint Team Site Support - Option Period</p> <p>Delivery Location Code: TSA38                      OFFICE OF GLOBAL STRATEGIES                      701 S 12TH STREET                      Continued ...</p>	1	CB	(b)(4)	

**CONTINUATION SHEET**

REFERENCE NO. OF DOCUMENT BEING CONTINUED  
 HSTS03-13-A-CIO549/HSTS03-16-J-CIO631/P00002

PAGE OF  
 3 3

NAME OF OFFEROR OR CONTRACTOR  
 INTERNATIONAL BUSINESS MACHINES CORPORATION

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Attn: LEA KAPLAN Arlington VA 20598 Accounting Info: Funded: \$0.00 Accounting Info: 50S178A000D2017AD2080GE000C250066006600GS-66010003 00000000-2520-TSA DIRECT-DEF. TASK-D Funded: (b)(4) Period of Performance: 02/04/2017 to 06/03/2017  Authorized Labor Categories:  Project Manager (b)(4)/hour and (b)(4)/hour Business Process Reengineering Specialist (b)(4)/hour and (b)(4)/hour Application Developer/Programmer (b)(4)/hour and (b)(4)/hour  NTE Hours 1,737 NTE Dollars (b)(4)				