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

1. REQUISITION NUMBER	PAGE	OF
211720708S0037	1	42

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
HSTS01-16-A-TCC009		HSTS02-17-J-OIA266		

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	JAKYA BROOKS	5712274873	

9. ISSUED BY — CODE 20

OFFICE OF ACQUISITION
701 S 12TH STREET
Arlington VA 20598

10. THIS ACQUISITION IS — UNRESTRICTED OR X SET ASIDE: 100.00 % FOR:

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

NAICS: 517919
SIZE STANDARD: $32.5

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

15. DELIVER TO — CODE

Multiple Destinations

16. ADMINISTERED BY — CODE 01

HUMAN CAPITAL & FINANCE
701 S 12TH STREET
Arlington VA 20598

17a. CONTRACTOR/ OFFEROR — CODE 872884200 — FACILITY CODE

SYSTEMS INTEGRATION INCORPORATED
Attn: ERIC FUKUCHI
8201 CORPORATE DR STE 300
HYATTSVILLE MD 207857206

TELEPHONE NO. 240-7641103

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

18a. PAYMENT WILL BE MADE BY — CODE TSA1

US Coast Guard Financial Center
TSA Commercial Invoices
P.O. Box 4111
Chesapeake VA 23327-4111

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	GSA Contract #: GS-35F-295DA Tax ID Number: 52-1676018 DUNS Number: 872884200 Base Period + Option Years - Handle Up to 500 Calls per Day Tier 1 Call Center Representative (b)(4) Team Lead (b)(4) Project Manager (b)(4) Surge CLINs - Base Year - Handle 250 Additional Calls per Day *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA
See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*
$1,136,758.90

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.
X 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA — X ARE — ARE NOT ATTACHED.

X 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*
Gloria A. Uria

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
SRINATH NARAYAN, CEO	9/12/17	Gloria A. Uria	09-12-2017

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Tier 1 Call Center Representative (b)(4) Team Lead (b)(4) Period of Performance: 11/01/2017 to 10/31/2022				
00001	Base Period - Handle Up to 500 Calls per Day	1	JB	(b)(4)	
	Monthly Amount (b)(4) x 12 Annual = (b)(4) Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate) Accounting Info: 5OS178A000D2017SWE020GE000025005900590BMO-59000000 00000000-251D-TSA DIRECT-DEF. TASK-D Funded: (b)(4)				
00001A	Additional Funding to support CLIN 00001 Base Period - Handle Up to 500 Calls per Day Monthly Amount (b)(4) /x 12 Annual = (b)(4) Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate) Continued ...	1	JB	(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 ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ 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)*	42d. TOTAL CONTAINERS

NAME OF OFFEROR OR CONTRACTOR
SYSTEMS INTEGRATION INCORPORATED

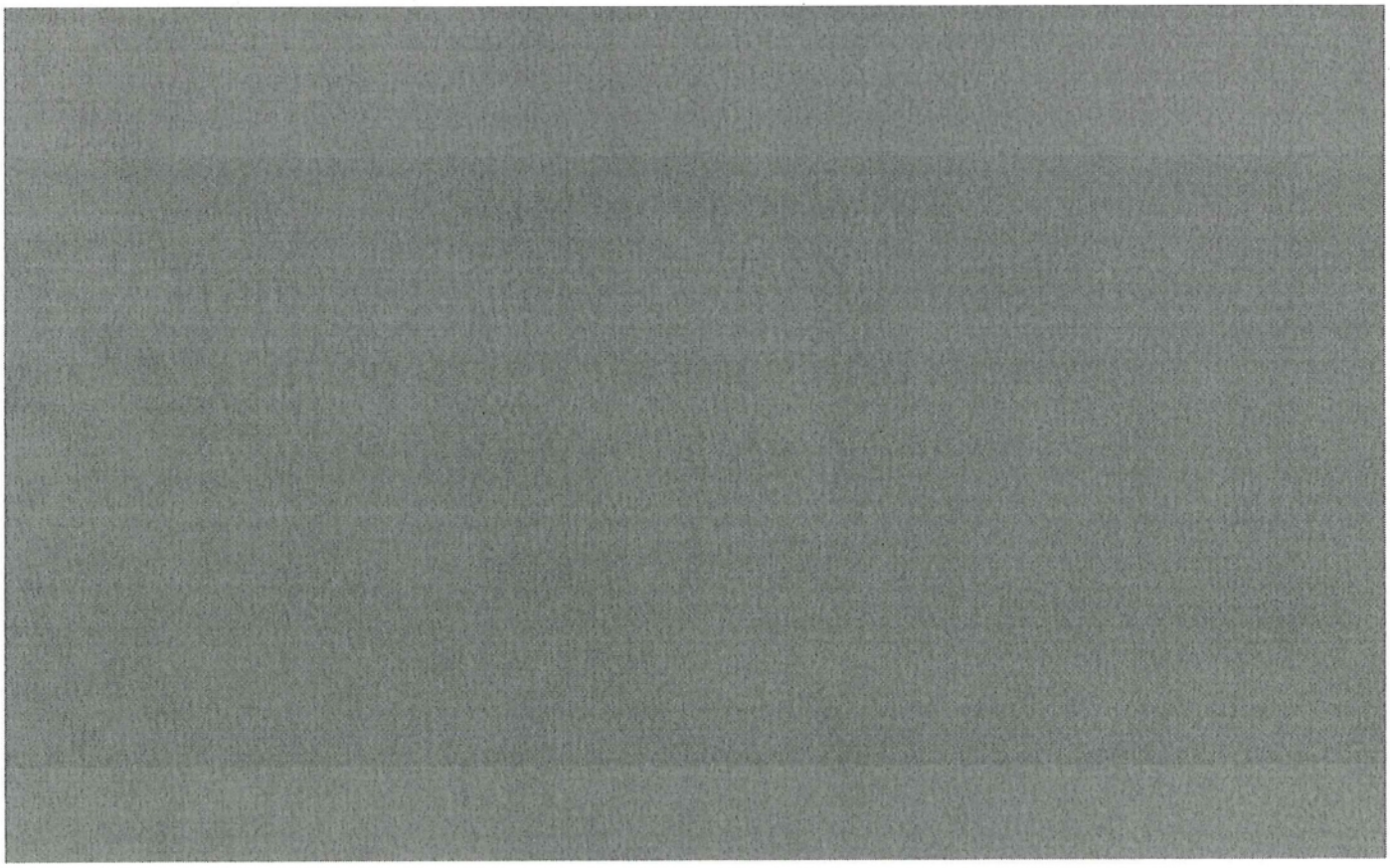
ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: 5OS178A000D2017TVC010GE000023005400540OIA-5400000000000000-251D-TSA DIRECT-DEF. TASK-D Funded: (b)(4)				
00002	Surge CLIN - Base Year - Handle 250 Additional Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 10/31/2018	1	JB	(b)(4)	0.00
10001	Option Year 1 - Handle Up to 500 Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager ((b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 11/01/2018	1	JB	(b)(4)	0.00
10002	Surge CLIN - Option Year 1 - Handle 250 Additional Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 10/31/2019	1	JB	(b)(4)	0.00
20001	Option Year 2 - Handle Up to 500 Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead ((b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 11/01/2019	1	JB	(b)(4)	0.00
20002	Surge CLIN - Option Year 2 - Handle 250 Additional Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 10/31/2020	1	JB	(b)(4)	0.00
30001	Option Year 3 - Handle Up to 500 Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Continued ...	1	JB	(b)(4)	0.00

NAME OF OFFEROR OR CONTRACTOR
SYSTEMS INTEGRATION INCORPORATED

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 11/01/2020				
30002	Surge CLIN - Option Year 3 - Handle 250 Additional Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 10/31/2021	1	JB	(b)(4)	0.00
40001	Option Year 4 - Handle Up to 500 Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate) Amount: (b)(4) (Option Line Item) 11/01/2021	1	JB	(b)(4)	0.00
40002	Surge CLIN - Option Year 4 - Handle 250 Additional Calls per Day Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Amount: (b)(4) Option Line Item) 10/31/2022 All Other Terms and Conditions of Blanket Purchase Agreement HSTS01-16-A-TCC009 remain in full force and effect. The total amount of award: $8,464,308.83. The obligation for this award is shown in box 26.	1	JB	(b)(4)	0.00

Statement of Work
Transportation Security Administration, Office of Intelligence and Analysis, Identity Verification Services

September 2017



1 Overview

The Transportation Security Administration (TSA) is continuing to look for ways to enhance its layered approach to security through new state-of-the-art technologies, expanded use of existing and proven technologies, improved passenger identification techniques, and other developments that will continue to strengthen our anti-terrorism capabilities.

The Vetting Analysis Division within the TSA Office of Intelligence and Analysis is requesting proposals for contact center services to complement existing operations that conducts identity verification for an airline passenger who present themselves to TSA's security checkpoints without government approved identification. Passengers lose or have their identification stolen during their travel and will appear at the security checkpoint without identification. TSA established the Identity Verification Call Center (IVCC) to assist passengers without proper identification. The enforcement of the 2005 Real ID Act and a change in security procedures will cause a significant increase to the IVCC's call volume in the next year.

2 Background

The IVCC was created to assist airline passengers who present themselves at a security checkpoint without approved government issued identification because their identification was either lost or stolen. The center operates 24 hours per day, 365 days per year. The IVCC receives calls from the TSA security checkpoint when a passenger without identification presents themselves at a checkpoint. The IVCC uses knowledge based authentication, via commercial and government database sources with personal identifiable information, in order to derive questions that the IVCC asks the passenger to verify his or her identity. The commercial databases used by the IVCC are aggregators of an individual's transactional data, providing essential information of which only an individual would have knowledge.

The IVCC experienced significant call volume growth over the past years due to increases in passenger air travel. In 2015, the IVCC received 123K calls, a 48% increase over the previous year. The IVCC calls increased another 33% in 2016, receiving 165K calls. The current daily average call volume is 450 calls per day, with peak volume of 865 last Labor Day Holiday. The daily call volume fluctuates by day of week, peak holiday travel, and seasonal travel periods. TSA estimates that contractor staff will be needed to handle an expected call volume increase of approximately 180K annual calls given its plan to limit the types of acceptable alternate identity documents allowed at the security checkpoints.

A challenge to the identity verification process is that certain demographics, such as foreign nationals, refugees, and the 18 – 24-year-old traveler, are difficult to verify identity due to the

limited data in commercial databases. The IVCC uses government databases as the source of information to derive questions.

3 Requirements/Technical Specifications

The purpose of this requirement is to provide contact center services to conduct identity verification for airline passengers complementing the existing IVCC operations, in support of TSA's expected policy change which will increase the demand for identity verification. Since the identity verification process can have challenging passenger populations, the model used by the IVCC and contractor support will be based on a two tier approach; the contractor provides identity verification as the first contact point, with more difficult identity verification calls escalated to the government staffed IVCC. Tier 1 calls include the following two types of calls:

- Identity Verification: A passenger has presented themselves at the Security Checkpoint without the approved government issued identification. A TSA Representative will contact the Identity Verification Call Center identifying them as a TSA employee with a passenger without proper identification. The contractor will request the passenger information, search the available databases for a passenger profile, research the passenger's information that contains personally identifiable information (PII), derive questions to ask the passenger and based on the passenger's successful answering of the questions will be permitted to proceed through screening. The passenger's unsuccessful answering of the questions unverifys the passenger identity. The Checkpoint Staff then follow their procedures for unverified passengers. The contractor uses critical thinking skills to derive the questions and determine if the passenger's knowledge matches the database information verifying their identity. TSA will provide the contractor with training and guidelines that establish if the individual has successfully verified his/her identity.
- Process Assistance Calls: The IVCC receives calls from the Security Checkpoint about various identity verification and security checkpoint procedures. The contractor will assist the TSA representative in clarifying questions they may have regarding security procedures.

The contractor will provide the identity verification call center services based on an average expected call volume of 500 calls per day with the following daily peak variations:

Percent of Daily Average

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
126%	122%	92%	86%	95%	95%	85%

Based on current IVCC call volume, the call volume is expected to be evenly distributed from 7:00am – 7:00pm Eastern Time (ET) with a 20%-30% lower call volume between 5:00am – 7:00am ET and 7:00pm – 9:00pm ET.

The Government is requesting a proposal providing contact center services to conduct identity verification with the following options:

- Providing call center representatives who will be located at TSA facilities, specifically the Colorado Springs Operations Center (CSOC), using existing TSA provided call center technologies, including call center telephone system, call ticketing system, quality assurance and identity verification databases. The proposal must explain best practices used to provide a positive customer experience.

- Hours for call center representatives will be between 5:00am – 9:00pm ET, seven (7) days per week including holidays. The government will provide a detailed schedule closer to the launch date and will plan to adjust the work schedule based on volume and timing of calls received.

- The Government may exercise an optional Contract Line Item Number (CLIN) to increase the number of calls that the Contractor will be expected to handle on a daily basis. The Contractor must provide pricing in increments of 250 calls. If the Contractor consistently experiences an average daily call volume more than 10% above/below expected volumes (e.g., on average, contractor responds to more than 550 calls per day), TSA and the Contractor will determine whether TSA will exercise this optional CLIN or cease to exercise an optional CLIN. After the initial implementation of the identity verification procedural change, TSA will evaluate how estimated call volumes reflect actual call volumes to determine if an optional CLIN needs to be exercised. Following this initial period, TSA and the Contractor will evaluate call volume every quarter.

- A supervisor or team lead must be available at CSOC to oversee contractor staff and address any issues that may arise during contractor hours (Sun-Sat, 5am-9pm). The supervisors may also respond to identity verification calls.

- Training will be provided by the Government on operational procedures and requirements for verifying the passenger's identity.
- Due to the sensitivity of the call type, all representatives will be required to pass a TSA Personnel Security suitability determination and adhere to strict TSA privacy policies.

3.1 Performance Requirements

The service requirements are summarized into performance objectives that relate directly to essential performance measurements. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement.

The Contractor will use the Government's call center software and reporting system to track the following performance metrics.

Performance Standard	Target Metric	Sample Calculation (Actual calculation to be determined)	Assessment Period
Service Level	60% in 20 seconds	Calls answered within 20 seconds + Calls abandoned within 20 seconds)/(Total calls answered + Total calls abandoned)	Weekly
Average Wait Time	3 mins		Weekly
Average Call Handle Time	7.5 mins	Talk time + after call work time	Weekly
Representative Availability	80%	The occupancy of the representative or group of representatives expressed as a percentage of time available to receive calls.	Weekly
Adherence to Escalation Policy	95%	Total calls escalated properly/total calls	Monthly
Call Quality Score (Calibration Score)	97%	The overall rating received by contractor staff measuring performance based on a set of standards. The quality assurance check includes reviewing tickets created in the case management system and listening to call recordings comparing to customer service and quality standards. * Government staff will review ticket and call quality based on standards provided to the contractor	Monthly
Privacy Violations	0 violations	A privacy violation is defined as a compromise or suspected compromise of Personally Identifiable Information (PII) to persons not authorized to receive that information, or a serious failure to comply with the provisions of applicable privacy requirements which is likely to result in compromise. A practice dangerous to privacy is defined as any knowing, willful, or negligent action contrary to the provisions of applicable privacy requirements that does not rise to the level of a privacy violation. A pattern of repeated lesser privacy infractions committed by Contractor personnel may result in a determination of a practice dangerous to privacy.	As soon as the violation is discovered

4 Delivery Order Information

4.1 Period of Performance

The task order will begin November 1, 2017. The contract shall be in effect for five (5) years; Base year plus four (4) one-year option periods.

4.2 Place of Performance

Contractor's personnel will work full-time to provide coverage 5:00am – 9:00pm ET, seven (7) days per week including holidays at TSA Colorado Springs located at 121 South Tejon Street, Colorado Springs, CO 80903.

4.3 Government Points of Contacts:

A. Contracting Officer (CO)

Name: Gloria Uria

Phone: (b)(6)

E-Mail: (b)(6)

B. Contracting Officer Representative (COR)

Name: Birgitta Brady

Phone: (b)(6)

E-Mail: (b)(6)

4.4 Marking of Deliverables

1. All deliverables submitted to the Contracting Officer (CO), the designated Contracting Officer's Representative (COR), shall be accompanied by a packing list or other suitable shipping document that shall clearly indicates the following:
    a. Contract number;
    b. CLIN number;
    c. Name and address of the consignor;
    d. Name and address of the consignee;
    e. Government bill of lading number covering the shipment (if any); and
    f. Description of the item/material shipped, including item number, quantity, number of containers, and package number (if any).
2. The Contractor shall take all necessary precautions to ensure that all sensitive data developed under this contract are delivered to the Government in a secure manner.

4.5 Contract Deliverables

The following table describes the Contract Deliverable Requirements List (CDRLs) that are required for this SOW. The Contractor requires written approval from the Contracting Officer (CO) before executing any change to the scope, content, and/or delivery schedule of the described work products and tasks in this SOW.

In accordance with BPA sections 2.8 "Quality Assurance/Quality Improvement" and 2.9 "Performance Management" the following deliverables are required for this task order:

#	Deliverable	Due Date	Recipient	BPA Ref #	Format/Type
1.	Quality Control Plan (QCP)	Due with Proposal. Final Document Due 45 days after date of award.	COR	2.2.3	Hard copy and/or e-mail
2.	Staffing Plan	Due with Proposal. Final Document Due 45 days after date of award.	COR	2.2.3	Hard copy and/or e-mail
3.	Post-Award Conference/Kick off Meeting	Within seven (7) business days after the Contractors performing work on this contract have passed TSA Personnel Security suitability determination.	CO, COR	2.2.3	Hard copy and/or e-mail
4.	Monthly Program Management Reviews and Reports*	Monthly, Due four days after the last day of each month	CO, COR	2.2.3	Hard copy and/or e-mail
5.	Weekly Status Reports*	Weekly, Every Monday/ in advance of project status meetings.	PM and COR		Hard copy and/or e-mail

* Monthly and weekly reports will include the performance metrics identified in Section 3.1. The monthly report will include a plan to address any performance deficiencies.

The dates shown in the CDRLs table are the required initial delivery date, which initiates the Government acceptance timeline described below.

All plans and documents are intended to provide continuity with previous work performed and to provide a comprehensive set of program management guidance and reporting as well as systems development and management documentation.

All deliverables, existing plans and documents shall be used in their current form where applicable and shall be updated to accommodate deficiencies, program and development changes, as appropriate. Documents listed but not currently existing shall be created and delivered at the time specified in the frequency column above. The Contractor shall prepare and maintain all documentation in accordance with an industry standard best practice for auditable, repeatable engineering process to assure the availability and accuracy of a comprehensive, complete, and current set of plans, reports, and documents.

The Contractor shall use the TSA Systems Development Life Cycle Guidance Document, version 2.0, (or updated version) for updating of systems development documentation form and content.

The Contractor shall take all necessary precautions to ensure that all sensitive data developed under this contract are delivered to the Government in a secure manner.

The list of documents and their content and format may be refined and tailored by mutual agreement between the Government and Contractor to assure quality program management, systems development, and systems operation and management.

The Contractor shall use the TSA Style Guide when preparing all deliverables.

5 Government Furnished Equipment (GFE)

The Government identifies the following GFE and Government Furnished Information (GFI) for this effort when onsite support is requested:

- Use of Government provided facilities for Contractor office space;
- Computer-hosting facilities with appropriate power, space and environment;
- Operating environments to include a workstation;
- Documentation required for facility and system accreditation;
- OIA On/Off-boarding procedures; and
- Access to TSA's Online Learning Center (OLC) – TSA's automated training system used to meet the mandated privacy and security training requirements.

6 Incorporation by Reference

All clauses, terms and conditions included in the base BPA HSTS01-16A-TCC009 are hereby incorporated by reference, and are in full force and effect for the entirety of this task order.

7 Additional Contract Compliance Requirements

Information Assurance Requirements for TSA Government Acquisitions (April 2016)

7.1 A. General Security Requirements

A.1. 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.

A.2. The Contractor shall perform periodic reviews to ensure compliance with all information security and privacy requirements.

A.3. 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.

A.4. 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).

A.5. The Contractor shall ensure all staff has 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.

A.6. The Contractor shall sign a DHS Non-Disclosure Agreement (NDA) within thirty (30) calendar days of the contract start date.

A.7. 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.

A.8. 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.

A.9. The Contractor shall make all system information and documentation produced in support of the contract available to TSA upon request.

7.2 B. Training Requirements

B.1. All Contractor employees, requiring system access, shall receive initial Organizational Security Fundamentals Training within (sixty) 60 days of assignment to the contract via the Online Learning Center (OLC). Refresher training shall be completed annually thereafter.

B.2. The Contractor shall complete annual online training for Organizational Security Fundamentals and TSA Privacy training.

B.3. 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.

B.4. 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 ninety (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.

B.5. Information Security and Privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

B.6. 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.

B.7. 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.

7.3 C. Configuration Management (hardware/software)

C.1. 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.

C.2. 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.

C.3. The Contractor shall ensure all sites impacted by patching are compliant within fourteen (14) days of change approval and release.

C.4. 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.

C.5. 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:

   http://usgcb.nist.gov/usgcb_content.html

2. DHS Sensitive Systems Configuration Guidance:

   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.

C.6. 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.

7.4 D. Risk Management Framework

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

D.1. 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), 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 (RMF). Ongoing Authorization is part of Step 6 "Monitoring" of the RMF. All NIST guidance is publicly available; TSA and DHS security policy is disclosed upon contract award with some exceptions, which are public facing (i.e., DHS Security and Training Requirements for Contractors).

D.2. A written Authorization to Operate (ATO) granted by the TSA Authorizing Official (AO) also known as TSA Chief Information Security Officer (CISO) 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.

D.3. TSA shall assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) Pub 199 *Standards for Security Categorization of Federal Information and Information Systems* impact levels and assign security controls to those systems consistent with FIPS Pub 200 *Minimum Security Requirements for Federal Information and Information Systems* methodology.

D.4. Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation shall be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

D.5. The Security Authorization (SA) 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 shall be reviewed and approved by the CISO and the IAD, and accepted by the CO upon creation and after any subsequent changes, before they go into effect. Ongoing Authorization artifacts include monthly TRigger Accountability Log (TRAL), monthly operating system scan results, application scans as directed, updated control allocation table (CAT), and associated memos as directed. All steps in the DHS Information Assurance Compliance Systems (IACS) shall be completed correctly, thoroughly and in a timely manner for all steps of the RMF.

D.6. The Contractor shall support the successful remediation of all identified system weaknesses and vulnerabilities that are identified as a result of the aforementioned security review process.

D.7. The Contractor shall submit and analyze monthly operating system vulnerability scans for the DHS Information Security Performance Plan FISMA Scorecard. Vulnerabilities not remediated are generated into Plan of Action and Milestone (POA&M) after thirty (30) days.

7.5 E. Contingency Planning

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

E.1. The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations may be disrupted and thus require activation of the CP and/or COOP. are disrupted. The Contractor's CP/COOP responsibility relates only to the system they provide or operate under contract.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in the DHS IACS Tool. If access has not been provided initially, the Contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K *IT Contingency Plan Template*.

E.3. 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.

E.4. The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

E.5. The Contractor shall test their CP annually and retain records of the annual CP testing for review during periodic audits.

E.6. The Contractor shall record, track, and correct any CP deficiency; any deficiency correction that cannot be accomplished within one month of the annual test shall be elevated to IAD.

E.7. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.8. 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.

E.9. 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.

E.10. 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.

E.11. The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

E.12. 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.

E.13. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) shall 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.

E.14. 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 shall be stored at a secondary location determined by the local element disaster recovery plan.

E.15. The Contractor shall ensure that data at the secondary location is current as required by the system's availability security categorization impact rating.

E.16. 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).

E.17. The Contractor shall adhere to the DHS IT 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.

E.18. The Contractor shall adhere to the DHS IT Security Architecture Guidance Volume 1: *Network and System Infrastructure* for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

7.6 F. Program Performance

F.1. The Contractor shall comply with requests to be audited and provide responses within three (3) business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the Contracting Officer (CO).

F.2. The Contractor shall provide support during the IAD audit activities and efforts. These audit activities shall include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

F.3. Upon completion of monthly security scans, findings shall be documented and categorized as High, Moderate, or Low based on their potential impact to the System IT Security posture. The Contractor shall provide TSA with estimates of the total engineering service hours required to support the remediation of open POA&M items. High security findings shall be remediated first in forty-five (45) days or less; Moderate security findings shall be remediated in sixty (60) days or less, and Low security findings shall be remediated in ninety (90) days or less. The Contractor shall work with the TSA System ISSO and the respective CO and/or Contracting Officer's Representative (COR), as well as OIT IAD and the System Owner (as required) to prioritize and plan for the remediation of open POA&Ms. The TSA System ISSO shall maintain all security artifacts and perform Ongoing Authorization (per NIST 800-137 and DHS-TSA requirements) and Continuous Diagnostics and Mitigation (CDM) (per OMB M-14-03) activities to ensure active compliance with security requirements. Specific POA&M guidance and information can be found in the SOP 1401 *Plan of Action and Milestone (POA&M) Process*, as well as the DHS 4300A PD Attachment H *Plan of Action and Milestones (POA&M) Process Guide.*

7.7 G. Federal Risk and Authorization Management Program (FedRAMP)

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

G.1. **FedRAMP Requirements**: Private sector solutions shall be hosted by a Joint Authorization Board (JAB)-approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) (http://cloud.cio.gov/fedramp/cloud-systems) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The CSP 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 properly cleared and vetted U.S. citizens;
- TSA data shall not leave the United States; and
- The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) 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.

G.2. Private Sector System Requirements: TSA shall conduct audits at any time on 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 IACS. The private sector systems are required to go through the Security Authorization Process and the RMF in accordance the Federal Information Systems Management Act (FISMA) and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has E3A deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Management Directive 1400.3 and its Attachment 1 (TSA IA 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 and communicated by the contracting officer representative (COR) or contract security point of contact (POC).

7.8 H. Information Assurance Policy

H.1. All services, hardware and/or software provided under this task order shall be compliant with applicable DHS 4300A Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook, TSA MD 1400.3 Information Technology Security, TSA IA Handbook, Technical Standards (TSs) and standard operating procedures (SOPs).

H.2. The Contractor solution shall follow all current versions of TSA and DHS policies,

procedures, guidelines, and standards, which shall be provided by the Contracting Officer.

H.3. Authorized access and use of TSA IT systems and resources shall be in accordance with the TSA IA Handbook.

H.4. 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 and include a hard copy with the shipment.

7.9 I. Data Stored/Processed at Contractor Site

I.1. Unless otherwise directed by TSA, any storage of data shall 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.

7.10 J. Remote Access

J.1. 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 shall be expressly granted, in writing, by the TSA IAD.

J.2. The Contractor employee(s) remote access connection to TSA networks shall be terminated immediately for unauthorized use, at the sole discretion of TSA.

J.3. The Contractor shall use his or her federal issued personal identifiable verification (PIV) badge to access TSA resources to include IT applications and physical facility.

7.11 K. 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:

K.1. 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 using an interagency agreement; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

K.2. ISAs shall be reissued every (three) 3 years or whenever any significant changes have been made to any of the interconnected systems.

K.3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

7.12 L. SBU Data Privacy and Protection

This section is not applicable if contract has DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

L.1. The Contractor shall satisfy requirements to work with and safeguard Sensitive Security Information (SSI), Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (Sensitive PII). All support personnel shall understand and rigorously follow DHS and TSA requirements, SSI Policies and Procedures Handbook, and Privacy policies, and procedures for safeguarding SSI, PII and SPII.

L.2. 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, SPII, 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.

L.3. TSA shall identify IT systems transmitting unclassified/SSI information that shall 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 DHS 4300A Sensitive Systems Handbook), current version.

L.4. 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 shall comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

L.5. 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 IA Handbook, and applicable IT Security Technical Standards and SOPs.

L.6. The Contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA IA Handbook, applicable Technical Standards, SOPs, and TSA MD 3700.4; *Handling Sensitive Personally Identifiable Information*.

L.7. The Contractor shall ensure that source code is protected from unauthorized access or dissemination (see TSA IA Handbook).

7.13 M. Disposition of Government Resources

M.1 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 IA Handbook, Technical Standards and SOPs. 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, TSA Technical Standard 046 *IT Media Sanitization and Disposition*, and SOP 1400-503 *IT Media Sanitization*. The Contractor shall email a signed, by the Contractor's designated security officer or senior official, proof of sanitization to the COR. In addition, the Contractor shall provide the Contracting Officer a master asset inventory list that reflects all assets, government furnished equipment (GFE) or authorized non-GFE that were used to process TSA information.

7.14 N. Special Considerations and Circumstances (if applicable and when requested)

N.1 For major agency Information Technology (IT) infrastructure support ranging in the total estimated procurement value (TEPV) of about $100 million or above **or** per TSA management's request, the Contractor shall provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA IAD. This plan shall describe the processes and procedures that shall be followed to ensure the appropriate security of IT resources are developed, processed, or used under this contract. At a minimum, the Contractor's SPP shall address the Contractor's compliance with the controls described in NIST SP 800-53 (current version). The security controls contained in the plan shall meet the requirements listed in the TSA IA Handbook, Technical Standards and the DHS Sensitive Systems Policy Directive and Handbook 4300A (current versions).

N.2 The SPP shall be a living document. It shall be reviewed and updated semi-annually, beginning on the effective date of the contract, to address new processes, procedures, technical or federally mandated security controls and other contract requirement modifications or additions that affect the security of IT resources under contract.

N.3 The SPP shall be submitted within thirty (30) days after contract award. The SPP shall be consistent with and further details the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the system security requirements.

N.4 The SPP, as submitted to the Contracting Officer, and accepted by the Information Systems Security Officer (ISSO), shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

7.15 O. Trusted Internet Connection 2.0 Requirements for Managed Trusted Internet Protocol Service Offering (MTIPS)

O.1 MTIPS providers shall comply with the FedRAMP TIC 2.0 Overlay requirements in addition to the basic requirements outlined in the DHS TIC Reference Architecture v2.0.

7.16 P. ISSO Support

P.1 The Contractor Program Manager shall ensure that the Contractor ISSO duties and responsibilities align with the Information Assurance and Cyber Security Division, Governance, Risk, and Compliance (GRC) Branch mission and security responsibilities. The TSA CISO is the authorizing official for ISSO designation.

7.17 Q. Continuous Diagnostics and Mitigation

Q.1 The Government, through a Continuous Monitoring as a Service (CMaaS) vendor, shall provide the Contractor with GFE appliances and tools to support the implementation and maintenance of the Continuous Diagnostics and Mitigation (CDM) Solution. The tools shall be hosted on the DHS' Infrastructure as a Service (IaaS) program. The Government, through the CMaaS vendor, shall provide sensor kits and agents that shall be deployed on all Contractor Information Systems supporting the TSA.

Q.2 The Contractor shall support the installation (including rack and configuration) of the sensor kits and agents on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards.

Q.3 The Contractor shall tune their existing endpoint security products to coexist with the identified products to ensure smooth and cohesive functionalities. Credentials (Service accounts) shall be provided, by the TSA CISO or designee, for vulnerability scans and host interrogation.

Q.4 The Government, through the CMaaS vendor, shall provide the following support for operations and maintenance of the CDM solution sensor kits:

- Patching (Controlled through a CMaaS Windows Server Update Service (WSUS))
- Hardware troubleshooting & Risk Management (RMA)
- Application maintenance (done from the Government/TSA Management Enclave)
- Vulnerability scanning

Q.5 The Contractor shall install TSA-provided CDM Solution patches within two (2) days of issuance, or as directed by TSA, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

Q.6 The TSA Contracting Owner is authorized to provide technical direction to the Contractor for the sole purpose of implementing the CDM Solution. If the technical direction results in any cost incurred by the Contractor, for which the Contractor shall seek

reimbursement from the Government, the Contractor shall identify the following information in any cost/price proposal to the Government: name of system owner, summary of the technical direction, date of the technical direction, purpose of the technical direction, summary of actions taken by the Contractor, any other information the contracting officer may require to further guide the directed change. The Contactor shall receive approval from the Contracting Officer of the directed change prior to incurring costs associated with the technical direction.

7.18 R. Software Guidance

The Contracting Officer shall provide a listing of all TSA approved security software upon contract award. The approved security software listing is maintained by the Information Assurance Division (IAD).

R.1 In support of the CDM objective to protect high value assets (HVAs) and information, the Government has acquired security tools in order to conduct Indicator of Compromise (IOC) scans within the mandated time frame. The Government shall provide the tool license and/or equipment for installation of tool agents on all TSA supported assets.

R.2 The Contractor shall support efforts to allow for the IOC scanning mandate. This may include installation of tool servers and/or agents within each system's environment and on all TSA supported assets. The Government shall provide the Contractor with the tool server(s) that shall not belong to the Contractor's system boundary. The tool server shall be reachable from OneNet/TSANet over the Internet. The tool server(s) shall be properly configured to reach all assets with the tool agent installed on the network. Credentials (service accounts) shall be provided for IOC scans and tool interrogation.

R.3 The Contractor shall support or perform the installation of forensic software servlet agents on supported Operating Systems on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards. The Contractor shall test and upgrade the servlet agents as directed by the IAD.

R.4 The Government shall provide the Contractor with a forensic software server that shall not belong to the Contractor's system boundary. The Contractor shall support or perform the installation of the server. The server shall be reachable from TSANet over the Internet and shall be primarily used for authentication and proxy functions. The server shall be properly configured to reach all assets with the agent installed on the network.

R.5 The Contractor shall support efforts of incident response and forensic investigation. This includes authorization to connect TSA authorized equipment where the forensic software servlet agents are reachable to perform analysis.

R.6 The Contractor shall install TSA-provided solution patches within two (2) days of issuance, or as directed by TSA CIO, and provide evidence of implementation to the TSA Information System Security Officer (ISSO).

7.19 S. Passwords

S.1 The contract ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation. In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.

7.20 T. Personal Identifiable Verification (PIV)

T.1 The Contractor shall use Personal Identity Verification (PIV) as the primary means to access TSA resources to include IT applications and physical facility. TSA network domain user account password expiration function shall be disabled when using PIV Machine Based Enforcement (MBE). PINs for PIV card-enabled users shall not expire, and shall have a minimum six-digit PIN when logging into the network using a PIV card.

T.2 The Contractor shall ensure newly developed information system(s) support PIV smartcard authentication. The information system shall be capable to accept and electronically verify PIV credentials.

T.3 The Contractor shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. http://www.idmanagement.gov/approved-products-list.

T.4 The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the PIV credentials as the common means of authentication for access to TSA's facilities, networks, and information systems.

7.21 U. End-of-Life (EOL) / End-of-Service (EOS)

U.1 The Contractor shall ensure that any hardware or software that is procured develops a full lifecycle plan based on the vendor's established life and service expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within 3 years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the TSA CISO in order to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

7.22 V. Maintenance

V.1 The Contractor shall ensure that the system, once operational, is properly maintained and monitored, to include: immediate response to critical security patches, routine maintenance windows to allow for system updates, and compliance with a defined configuration management process. All patches and system updates shall be properly tested in a development environment before being implemented in the production environment.

V.2 The Contractor shall perform customer support 24 hours, 7 days a week within the continental United States only.

7.23 W. Security in the Agile Development Process

W.1. All TSA systems shall follow the below guidance when delivering system and application solutions to the agency:

- All applications shall be reviewed prior to acceptance by the Contractor;
- Contractor shall implement Threat Modeling;
- Developer shall deliver a defect list;
- Developer shall implement Patching and Configuration Management strategies;
- Developer shall use Component Analysis;
- Developer shall implement build tests;
- Developer shall implement Manual Code Inspection;
- Developer shall implement Security Regression Tests;
- Developer shall implement Pre-Deployment/Post Deployment Automated Tests.
- Developer shall implement industry standard "Every-Sprint Practices", which at a minimum consists of:
  - Threat Modeling;
  - Use of Approved Tools;
  - Deprecate Unsafe Functions;
  - Static Analysis;
  - Conduction Final Security Review;
  - Certify, Release and Archive.
- Developer shall implement industry standard Practices, which at a minimum consists of:
  - Create Quality Gates/Bug Bars;
  - Perform Dynamic Analysis;
  - Perform Fuzz Testing;
  - Conduct Attach Surface Review.
- Developer shall implement industry standard One-Time Practices, which at a minimum consists of:
  - Establish Security Requirements;
  - Perform Security and Privacy Risk Assessments;
  - Establish Design Requirements;
  - Perform Attack Surface Analysis;
  - Create Incident Response Plan.

8 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.

1. All developed solutions and requirements shall be compliant with the HLS EA.
2. 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.
3. 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).
4. 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.
5. 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.

1. 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.
2. 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

3. 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.
4. 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.
5. 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.

9 Sensitive Information Required Special Contract Terms (MARCH 2015)

SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015).

9.1 (a) Applicability.

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

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

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

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

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

1. Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations

thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

2. Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
3. Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
4. Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

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

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

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

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

9.3 (c) *Authorities.*

The Contractor shall follow all current versions of Government policies and guidance accessible at: http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the CO, including but not limited to:

1. DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information;
2. DHS Sensitive Systems Policy Directive 4300A;
3. DHS 4300A Sensitive Systems Handbook and Attachments;
4. DHS Security Authorization Process Guide;
5. DHS Handbook for Safeguarding Sensitive Personally Identifiable Information;
6. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program;
7. DHS Information Security Performance Plan (current fiscal year);
8. DHS Privacy Incident Handling Guidance;
9. Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at: http://csrc.nist.gov/groups/STM/cmvp/standards.html
10. National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at: http://csrc.nist.gov/publications/PubsSPs.html
11. NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at: http://csrc.nist.gov/publications/PubsSPs.html

9.4 (d) Handling of Sensitive Information.

Contractor compliance with this clause, as well as the policies and procedures described below, is required.

1. Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The

DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establish procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

2. The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.
3. All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the COR no later than two (2) days after execution of the form.
4. The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

9.5 (e) Authority to Operate.

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

1. Complete the Security Authorization process. The SA process shall proceed according to the *DHS Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.
    a. Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by

an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the CO shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

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

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

3. Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods:

    a. Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at

least ninety (90) days before the ATO expiration date for review and verification of security controls; or

b. Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least ninety (90) days before the ATO expiration date for review and verification of security controls. The ninety (90) day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

4. *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the CO and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.
5. *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.
6. *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the CO may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive

information from the Internet or other networks or applying additional security controls.

7. *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

9.6 (f) Sensitive Information Incident Reporting Requirements.

1. All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems Handbook Incident Response and Reporting* requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the CO, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the CO's email address is not immediately available, the Contractor shall contact the CO immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.
2. If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *4300A Sensitive Systems Handbook Incident Response and Reporting,* Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

    a. Data Universal Numbering System (DUNS);
    b. Contract numbers affected unless all contracts by the company are affected;
    c. Facility CAGE code if the location of the event is different than the prime Contractor location;
    d. POC if different than the POC recorded in the System for Award Management (address, position, telephone, email);

e. CO POC (address, telephone, email);
f. Contract clearance level;
g. Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
h. Government programs, platforms or systems involved;
i. Location(s) of incident;
j. Date and time the incident was discovered;
k. Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
l. Description of the Government PII and/or SPII contained within the system;
m. Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
n. Any additional information relevant to the incident.

9.7 (g) Sensitive Information Incident Response Requirements.

1. All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the CO in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.
2. The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.
3. Incident response activities determined to be required by the Government may include, but are not limited to, the following:
    a. Inspections;
    b. Investigations;
    c. Forensic reviews; and
    d. Data analyses and processing.
4. The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

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

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

shall not proceed with notification unless the CO, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

    a. A brief description of the incident;
    b. A description of the types of PII and SPII involved;
    c. A statement as to whether the PII or SPII was encrypted or protected by other means;
    d. Steps individuals may take to protect themselves;
    e. What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
    f. Information identifying who individuals may contact for additional information.

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

1. Provide notification to affected individuals as described above; and/or
2. Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

    a. Triple credit bureau monitoring;
    b. Daily customer service;
    c. Alerts provided to the individual for changes and fraud; and
    d. Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

3. Establish a dedicated call center. Call center services shall include:

    a. A dedicated telephone number to contact customer service within a fixed period;
    b. Information necessary for registrants/enrollees to access credit reports and credit scores;

c. Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
d. Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
e. Customized FAQs, approved in writing by the CO in coordination with the Headquarters or Component Chief Privacy Officer; and
f. Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

9.10 (j) Certification of Sanitization of Government and Government-Activity-Related Files and Information.

As part of contract closeout, the Contractor shall submit the certification to the COR and the CO following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization.*

9.11 (k) Security Training Requirements.

1. All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at: http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.
2. The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions

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

9.12 (l) Privacy Training Requirements.

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

10 508 Compliance

10.1 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:

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.

10.2 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the Contractor to fulfill this work statement does not require

compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those Contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

10.3 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.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@hq.dhs.gov.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00001	See Block 16C	2417207OSO037	

6. ISSUED BY CODE 20

OFFICE OF ACQUISITION
701 S 12TH STREET
Arlington VA 20598

7. ADMINISTERED BY *(If other than Item 6)* CODE 01

HUMAN CAPITAL & FINANCE
701 S 12TH STREET
Arlington VA 20598

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

SYSTEMS INTEGRATION INCORPORATED
Attn: ERIC FUKUCHI
8201 CORPORATE DR STE 300
HYATTSVILLE MD 207857206

CODE 872884200 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

X 10A. MODIFICATION OF CONTRACT/ORDER NO.
HSTS01-16-A-TCC009
HSTS02-17-J-OIA266

10B. DATED *(SEE ITEM 13)*
09/08/2017

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.
X	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:
	D. OTHER *(Specify type of modification and authority)*

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-295DA
Tax ID Number: 52-1676018
DUNS Number: 872884200
The purpose of modification P00001 is to add a CLIN chart for the Task Order that outlines each of the CLINs and Surge CLINs
Period of Performance: 11/01/2017 to 10/31/2022
All Other Terms and Condition of the Blanket Purchase Order and Task Order are unchanged and in full force and effect.

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)*	
		Gloria A. Uria	
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
_____ *(Signature of person authorized to sign)*		Gloria A. Uria *(Signature of Contracting Officer)*	9-14-2017

The purpose of modification P00001 is to add a CLIN chart for the Task Order that outlines each of the CLINs and Surge CLINs. The Task Order is modified as follows:

Insert CLIN chart before Statement of Work:

HSTS02-17-F-OSO037 Price Analysis * invoced on a monthly basis*			
CLIN	**Description**	**Monthly Amount**	**Extended Price**
	Base Period 11/01/2017 - 10/31/2018		
00001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
	Surge CLINs - Labor to Handle 250 Additional calls per day		
00002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
	Option Period 1 11/01/2018 - 10/31/2019		
10001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
	Surge CLINs - Labor to Handle 250 Additional calls per day		
10002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
	Option Period 2 11/01/2019 - 10/31/2020		
20001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
	Surge CLINs - Labor to Handle 250 Additional calls per day (b)(4) Hourly Rate)		
20002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
	Option Period 3 11/01/2020 - 10/31/2021		
30001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
	Surge CLINs - Labor to Handle 250 Additional calls per day		
30002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
	Option Period 4 11/01/2021 - 10/31/2022		
40001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
	Surge CLINs - Labor to Handle 250 Additional calls per day		
40002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
	Total Amount at Time of Base Award		**$ 1,136,758.90**
	Total Amount of Task Orders (Options Periods + Surge CLINs)		**$ 8,464,308.83**

These changes do not affect the total funding of this Task Order. There will be no changes to the line items or descriptions on the Task Order.

All Other Terms and Condition of the Blanket Purchase Order and Task Order are unchanged and in full force and effect.

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

1. CONTRACT ID CODE	PAGE OF PAGES
	1 2

2. AMENDMENT/MODIFICATION NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NO.	5. PROJECT NO. *(If applicable)*
P00002	See Block 16C	2417207OSO037	

6. ISSUED BY	CODE	7. ADMINISTERED BY *(If other than Item 6)*	CODE
OFFICE OF ACQUISITION 701 S 12TH STREET Arlington VA 20598	20	HUMAN CAPITAL & FINANCE 701 S 12TH STREET Arlington VA 20598	01

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

SYSTEMS INTEGRATION INCORPORATED
Attn: ERIC FUKUCHI
8201 CORPORATE DR STE 300
HYATTSVILLE MD 207857206

CODE 872884200 FACILITY CODE

(x) 9A. AMENDMENT OF SOLICITATION NO.

9B. DATED *(SEE ITEM 11)*

X 10A. MODIFICATION OF CONTRACT/ORDER NO.
HSTS01-16-A-TCC009
HSTS02-17-J-OIA266

10B. DATED *(SEE ITEM 13)*
09/08/2017

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).
X	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF: FAR 43.103(a)(3) - Bilateral Modification
	D. OTHER *(Specify type of modification and authority)*

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 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-295DA
Tax ID Number: 52-1676018
DUNS Number: 872884200
This bilateral modification:

a. Adjusts and extends the overall Period of Performance FROM: (11/01/2017 to 10/31/2022) TO: (12/04/2017 to 12/03/2022).

b. Updates the Periods of Performance for all base and option CLINs as shown in Attachment I.

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)*
Srinath Narayan, CEO	Steven Santos

15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA	16C. DATE SIGNED
(Signature of person authorized to sign)	November 27, 2017	*(Signature of Contracting Officer)*	11/29/17

NAME OF OFFEROR OR CONTRACTOR
SYSTEMS INTEGRATION INCORPORATED

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	c. Replaces all references of HSTS02-17-F-OSO037 in Attachment I's Contract Line Item Number (CLIN) chart, previously introduced in modification P00001, with the correct BPA call number HSTS02-17-J-OIA266. As a result of this modification, the total obligated amount and total value remains unchanged. Period of Performance: 12/04/2017 to 12/03/2022 Attachments: I. HSTS02-17-J-OIA266 P00002 SF30 Attachment I - CLIN Chart --- END OF P00002 ---				

BPA# HSTS01-16-A-TCC009 / BPA call# HSTS02-17-J-OIA266
Modification P00002

Attachment I: CLIN Chart

The purpose of task order modification P00002 is to shift the period of performance dates and update the below Contract Line Item Number (CLIN) chart from the prior modification (P00001).

HSTS02-17-J-OIA266 Price Analysis *invoiced on a monthly basis*			
Base Period 12/04/2017 - 12/03/2018			
CLIN	**Description**	**Monthly Amount**	**Extended Price**
00001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
Surge CLINs - Labor to Handle 250 Additional calls per day			
00002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
Option Period 1 12/04/2018 - 12/03/2019			
10001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
Surge CLINs - Labor to Handle 250 Additional calls per day			
10002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
Option Period 2 12/04/2019 - 12/03/2020			
20001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
Surge CLINs - Labor to Handle 250 Additional calls per day			
20002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
Option Period 3 12/04/2020 - 12/03/2021			
30001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
Surge CLINs - Labor to Handle 250 Additional calls per day			
30002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
Option Period 4 12/04/2021 - 12/03/2022			
40001	Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate) Project Manager (b)(4) Hourly Rate)	$ (b)(4)	
Surge CLINs - Labor to Handle 250 Additional calls per day			
40002	Surge CLIN - Tier 1 Call Center Representative (b)(4) Hourly Rate) Team Lead (b)(4) Hourly Rate)	$ (b)(4)	
		Total Amount at Time of Base Award	**$ 1,136,758.90**
		Total Amount of Task Order (Option Periods + Surge CLINs)	**$ 8,464,308.83**

These changes do not affect the total funding of this task order. There will be no changes to the line items or descriptions on the task order, only the periods of performance.

BPA# HSTS01-16-A-TCC009 / BPA call# HSTS02-17-J-OIA266
Modification P00002

Attachment I: CLIN Chart

All other Terms and Conditions of the Blanket Purchase Agreement (BPA) and task order remain unchanged, and in full force and effect.

--- End of Attachment I ---