REQUEST FOR QUOTATION

(THIS IS NOT AN ORDER)

THIS RFQ ☐ IS ☒ IS NOT A SMALL BUSINESS SET ASIDE

PAGE 1 OF PAGES 72

1. REQUEST NO.	2. DATE ISSUED	3. REQUISITION/PURCHASE REQUEST NO.	4. CERT. FOR NAT. DEF. UNDER BDSA REG. 2 AND/OR DMS REG.1	RATING
70RDAD19Q00000101	10/30/2019			

5a. ISSUED BY

U.S. Dept. of Homeland Security
Office of Procurement Operations
Dept. Operations Acquisition Div.
245 Murray Lane, SW, #0115
Washington DC 20528-0115

6. DELIVERY BY *(Date)*: Multiple

7. DELIVERY: ☒ FOB DESTINATION ☐ OTHER *(See Schedule)*

9. DESTINATION

a. NAME OF CONSIGNEE

b. STREET ADDRESS

c. CITY

d. STATE e. ZIP CODE

5b. FOR INFORMATION CALL: *(No collect calls)*

NAME	TELEPHONE NUMBER	
	AREA CODE	NUMBER
W. Paul Barrett	202	447-5464

8. TO:

a. NAME b. COMPANY

c. STREET ADDRESS

d. CITY e. STATE f. ZIP CODE

10. PLEASE FURNISH QUOTATIONS TO THE ISSUING OFFICE IN BLOCK 5a ON OR BEFORE CLOSE OF BUSINESS *(Date)*: 11/26/2019 1200 ET

IMPORTANT: This is a request for information, and quotations furnished are not offers. If you are unable to quote, please so indicate on this form and return it to the address in Block 5a. This request does not commit the Government to pay any costs incurred in the preparation of the submission of this quotation or to contract for supplies or services. Supplies are of domestic origin unless otherwise indicated by quoter. Any representations and/or certifications attached to this Request for Quotations must be completed by the quoter.

11. SCHEDULE *(Include applicable Federal, State and local taxes)*

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)
	The purpose of this solicitation is to establish multiple Blanket Purchase Agreements (BPAs) to support the Department of Homeland Security (DHS) Office of the Chief Financial Officer (OCFO) for Enterprise Financial System Integrator (EFSI) Support Services, with an estimated value of $1,000,000,000.00.				

12. DISCOUNT FOR PROMPT PAYMENT ▶

a. 10 CALENDAR DAYS (%)	b. 20 CALENDAR DAYS (%)	c. 30 CALENDAR DAYS (%)	d. CALENDAR DAYS NUMBER	d. CALENDAR DAYS PERCENTAGE

NOTE: Additional provisions and representations ☐ are ☐ are not attached

13. NAME AND ADDRESS OF QUOTER

a. NAME OF QUOTER

b. STREET ADDRESS

c. COUNTY

d. CITY e. STATE f. ZIP CODE

14. SIGNATURE OF PERSON AUTHORIZED TO SIGN QUOTATION

15. DATE OF QUOTATION

16. SIGNER

a. NAME *(Type or print)*

b. TELEPHONE AREA CODE NUMBER

c. TITLE *(Type or print)*

AUTHORIZED FOR LOCAL REPRODUCTION
Previous edition not usable

STANDARD FORM 18 (REV. 6-95)
Prescribed by GSA - FAR (48 CFR) 53.215-1(a)

REQUEST FOR QUOTATION (RFQ)

70RDAD19Q00000101

for

Enterprise Financial System Integrator (EFSI)

Support Services

DHS Office of Procurement Operations
245 Murray Lane, SW
Mailstop #0115
Washington, D.C. 20528

BLANKET PURCHASE AGREEMENT (BPA)

In the spirit of the Federal Acquisition Streamlining Act, the Department of Homeland Security and

(Insert Contractor's Name)

enter into a Blanket Purchase Agreement (BPA) (multiple award anticipated) to support the U.S. Department of Homeland Security (DHS) Headquarters Office of the Chief Financial Officer (OCFO). The intent is to acquire a financial system integration support services through the General Services Administration (GSA) Multiple Award Schedule (MAS) 70, General Purpose Commercial Information Technology Equipment, Software, and Services. The following Special Item Number (SIN) applicable to the Contractor's GSA contract shall include in the BPA:

- SIN 132-51 (IT Professional Services); and
- SIN 132-50 (Training)

Note: The terms Quoter, Contractor, and BPA Holder are used interchangeably in this agreement. As appropriate for the context, the terms contract and contract award are understood to mean BPA and BPA establishment.

Signatures:

DHS Office of Procurement Operations (OPO) BPA Contracting Officer

Printed Name	OPO Title	Signature	Date

Contractor

Printed Name	Company Title	Signature	Date

SECTION I – BPA TERMS AND CONDITIONS

1 GENERAL

This section presents the general requirements applicable to the *Blanket Purchase Agreement (BPA)* Contractor(s).

It is the responsibility of the Contractor to notify the BPA Contracting Officer of GSA Schedule price changes affecting line items and services listed in this BPA prior to award of any Task Order. Discounts shall be in terms of a flat percentage to be applied against the GSA Schedule price for the product or service. If discounts are conditional on a given dollar volume or other condition, the Contractors' assumptions applicable to each conditional discount must be clearly stated. Contractors are strongly encouraged to offer further price reductions in accordance with their commercial practice. For Task Orders issued under this BPA, the price paid shall be the GSA Schedule price in effect at the time the order is issued less applicable discounts under this BPA or any further discounts that may be offered for any task orders. The relationship between the current price in the GSA Schedule and the price offered in the Contractors' Quotation shall remain constant; i.e., the discount shall remain the same throughout the term of the BPA. If the GSA pricing is adjusted lower due to a reduction, the BPA price shall reflect the new price. In the event of a GSA price increase, the BPA price discount shall apply to the new price. All Task Orders are subject to the terms and conditions of the underlying GSA contract and to the additional terms and conditions provided below.

2 SCOPE OF SERVICES

The following services can be ordered under this BPA:

Program Management; Discovery support services; System Integration and Implementation; Data Cleansing, Preparation and Staging; Service Desk Operations; System Operations and Maintenance; and Training services.

Note: All EFiMS software application suites to be integrated as part of this BPA are excluded from procurement under this BPA and task orders issued under this BPA. Advisory and/or recommendation services related to any potential selection of EFiMS software suites are excluded from this BPA and task orders issued under this BPA.

2.1 Types of Task Orders

Task Order types will be specified at the Task Order Level. This BPA provides for Firm Fixed Priced (FFP), Time and Material (T&M), Labor Hour (LH), and any combination of the three.

3 BPA ESTIMATED VOLUME

The estimated value of Task Orders to be placed under this BPA may be $1,000,000,000.00 over the course of One Hundred Twenty (120) months (10 years). The combined cumulative dollar amount that may potentially be awarded is $1,000,000,000.00.

3.1 Obligation

This BPA does not obligate any funds. The individual Task Orders placed against the BPA will obligate funds.

3.2 Off-Ramping (BPA Cancellation)

The Government reserves the unilateral right to cancel a BPA if it is determined to be in the Government's best interest. Examples of why the Government may elect to cancel a BPA include but are not limited to the following:

1. Contractors who fail to maintain a GSA FSS Schedule 70 Contract.
2. Contractors who fail to maintain BPA awarded labor categories on the Contractor's GSA Schedule.
3. Contractors Debarred, Suspended, or Ineligible as defined in FAR 9.4
4. Contractors who fail to consistently provide a response to Requests for Quotations.
5. Contractors who fail to complete BPA task order objectives.

The BPA is not a contract. Either the BPA Contracting Officer or a BPA holder may cancel the BPA upon 30 days' written notice to the other party. The placement of BPA task orders is not guaranteed.

If a Contractor's GSA contract expires or is cancelled, their BPA shall also be cancelled. Upon cancellation of a BPA, no new orders shall be awarded after the effective date of the cancellation. However, BPA cancellation does not release the BPA Contractor from the duty to continue performance on existing task orders or complete BPA level reporting requirements. Ongoing BPA task orders shall continue in accordance with their own periods of performance provided the Contractor's GSA Schedule contract remains valid.

3.3 On-Ramping (New BPA Awards)

The Government reserves the right to reopen this RFQ in order to establish additional BPAs if the Contracting Officer determines it to be in the best interest of the Government. Reopening the solicitation may be conducted in order to increase competition or achieve other Government interests or requirements.

The reopening of the solicitation (on-ramping) shall be achieved via a solicitation amendment through GSA eBuy. The amended solicitation may have a reduced term in order to permit co-termination of any new BPAs with existing BPAs in the FSM portfolio. It is the Government's intent to evaluate quotations received in response to the reissued/reopened BPA RFQ in

accordance with the evaluation criteria in this original BPA RFQ; those evaluation criteria and other instructions if any shall be detailed in the reissued/reopened RFQ. Quoters responding to the reissued/reopened RFQ shall have a valid GSA Schedule for the duration of the proposed BPA term and a period of 24 months beyond the end of the last ordering period. Quotations submitted in response to the solicitation amendment for on-ramping must be rated equal to or higher than the lowest rated contractor originally awarded a BPA in order to be considered or an award. Quotations submitted in response to a previous solicitation shall not be evaluated. Contractors must respond to the solicitation amendment in order to be considered for an on-ramp award.

4 REFERENCED FEDERAL ACQUISITION REGULATION (FAR) AND HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES/PROVISIONS

The Contractor's General Services Administration (GSA) Schedule 70 General Purpose Commercial Information Technology Equipment, Software, and Services contract clauses are incorporated into this BPA. In addition, all clauses referenced below are applicable to the resulting BPA and all Task Orders unless otherwise stated.

4.1 CONTRACT CLAUSES INCORPORATED BY REFERENCE

A. 52.252-2 Clauses Incorporated by Reference (Feb 1998)

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

Federal Acquisition Regulation (FAR) Clauses / Provisions		
Clause	**Title**	**Date**
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights.	Apr 2014
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.204-19	Incorporation by Reference of Representations and Certifications	Dec 2014
52.222-50	Combating Trafficking in Persons	Jan 2019
52.224-2	Privacy Act	Apr 1984
52.227-14	Rights in Data – General Alt IV	Dec 2007
52.228-7	Insurance – Liability to Third Persons	Mar 1996
52.244-6	Subcontracts for Commercial Items	Aug 2019
52.243-3	Changes – Time and Materials or Labor Hours	Sep 2000
52.245-1	Government Property	Jan 2017
52.246-6	Inspection – Time and Material or Labor Hour	May 2001

B. FAR PROVISIONS INCORPORATED IN FULL TEXT

FAR 52.209-2 Prohibition on Contracting with Inverted Domestic Corporations-Representation (NOV 2015)

(a) *Definitions*. "Inverted domestic corporation" and "subsidiary" have the meaning given in the clause of this contract entitled Prohibition on Contracting with Inverted Domestic Corporations (52.209-10).

(b) Government agencies are not permitted to use appropriated (or otherwise made available) funds for contracts with either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation, unless the exception at 9.108-2(b) applies or the requirement is waived in accordance with the procedures at 9.108-4.

(c) *Representation*. The Offeror represents that-

(1) It □is, □is not an inverted domestic corporation; and

(2) It □is, □is not a subsidiary of an inverted domestic corporation. (End of provision)

C. FAR CLAUSES INCORPORATED IN FULL TEXT

FAR 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (NOV 2015)

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

"Inverted domestic corporation" means a foreign incorporated entity that meets the definition of an inverted domestic corporation under 6 U.S.C. 395(b), applied in accordance with the rules and definitions of 6 U.S.C. 395(c).

"Subsidiary" means an entity in which more than 50 percent of the entity is owned-

(1) Directly by a parent corporation; or

(2) Through another subsidiary of a parent corporation.

(b) If the contractor reorganizes as an inverted domestic corporation or becomes a subsidiary of an inverted domestic corporation at any time during the period of performance of this contract, the Government may be prohibited from paying for Contractor activities performed after the date when it becomes an inverted domestic corporation or subsidiary. The Government may seek any available remedies in the event the Contractor fails to perform in accordance with the terms and conditions of the contract as a result of Government action under this clause.

(c) Exceptions to this prohibition are located at 9.108-2.

(d) In the event the Contractor becomes either an inverted domestic corporation, or a subsidiary of an inverted domestic corporation during contract performance, the Contractor shall give written notice to the Contracting Officer within five business days from the date of the inversion event. (End of clause)

Homeland Security Acquisition Regulation (HSAR) Clauses/ Provisions		
Clause	**Title**	**Date**
3052.203-70	Instructions for Contractor Disclosure of Violations	Sep 2012
3052.205-70	Advertisements, Publicizing Awards, and Release – Alternate 1	Sep 2012
3052.242-72	Contracting Officer's Technical Representative	Dec 2003

C. HSAR CLAUSES INCORPORATED IN FULL TEXT

HSAR 3052.204-71 Contractor Employee Access. (Sep 2012)

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

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

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

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

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

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

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

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

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

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

ALTERNATE I (Sep 2012)

When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

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

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of

work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

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

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

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

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

(2) The waiver must be in the best interest of the Government.

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

HSAR 3052.209-72 Organizational Conflict of Interest (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting may be identified at the BPA task order level, if applicable.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

____ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

HSAR 3052.209-73 Limitation of future contracting (Jun 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5--Organizational Conflicts of Interest.

(b) The nature of this conflict may be identified at the BPA task order level, as applicable.

(c) The restrictions upon future contracting are as follows:

> (1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

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

(End of clause)

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

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

(b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, no less than 15 business days in advance before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel under this Contract:

- BPA Account Manager
- Additional Key Personnel will be identified at the BPA task order level.

(End of Clause)

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

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

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing

this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

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

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

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

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

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

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

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or

unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

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

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

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

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

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

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

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

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

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

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

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

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

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

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

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

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

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

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy

Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

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

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

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

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

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

(f) Sensitive Information Incident Reporting Requirements.

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

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

(i) Data Universal Numbering System (DUNS);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

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

(g) Sensitive Information Incident Response Requirements.

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

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

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

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

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

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

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

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

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

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

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

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

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

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

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

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

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall

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

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

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

4.2 BPA Expiration

This BPA shall consist of one (1) base period and nine (9) ordering periods as shown below. Task Orders may have a Period of Performance of 24 months beyond the last day of Ordering

Period Nine of this BPA. The extension may not exceed more than 60 months after the GSA Schedule contract expired.

BPA Period	Ordering Period
Base Period	12 months
Ordering Period One	12 months
Ordering Period Two	12 months
Ordering Period Three	12 months
Ordering Period Four	12 months
Ordering Period Five	12 months
Ordering Period Six	12 months
Ordering Period Seven	12 months
Ordering Period Eight	12 months
Ordering Period Nine	12 months

This BPA expires at the end of the current period, or on the end date of the Contractor's GSA Schedule contract, or on the end date of each subsequent contract period for which GSA extends the GSA Schedule contract by modification, in which case this BPA will be comparably extended by modification not to exceed a total period of performance of one hundred twenty (120) months. Task Orders may be placed against this BPA on or before the last day of Option Period Nine if all of the ordering periods are exercised.

The Government may exercise an optional ordering period in accordance with the clause at FAR 52.217-9, *Option to Extend the Term of the Contract*, in the parent GSA schedule contract. For this purpose, the fill-ins for that clause are:

a) 30 days after the end of the current period
b) 60
c) 10 years

The BPA Holder is required to immediately notify, in writing, the BPA Contracting Officer if at any time the GSA Contract upon which the BPA is based, is no longer in force.

This BPA is not a contract. If the BPA Holder fails to perform in a manner satisfactory to the BPA Contracting Officer, this BPA may be canceled at any time with written notice to the BPA Holder by the BPA Contracting Officer. BPA cancellation does not simultaneously cancel existing orders written against the BPA.

4.3 Ordering Officers

DHS Warranted Contracting Officers.

4.4 Task Orders

Task Orders will be placed against this BPA by DHS Contracting Activities in accordance with the Ordering Procedures in Section 4.15.

4.5 Award of Task Orders under the BPA

Each Task Order issued under this BPA will include, at a minimum, the following information as applicable:

1. BPA and Task Order Number;
2. Date of the order;
3. Description of the service(s) to be acquired and/or work to be performed;
4. Period of performance or required completion date;
5. Place of performance;
6. Deliverables;
7. CLIN/SLIN number and description, quantity, unit price and extended price.
8. The security requirements;
9. The payment schedule; and
10. Accounting and appropriation data.

4.6 Task Order Period of Performance

The period of performance will be designated at the Task Order level. Task Orders may have a Period of Performance extending 24 months beyond the final ordering period of this BPA.

4.7 Invoicing

Invoicing procedures will be specified in each individual Task Order. The "remit to" address to which payment must be sent is applicable at the Task Order level. At a minimum, each invoice shall include the following information:

(i) Name and address of the Contractor;

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

(iii) BPA and Task Order number and period of performance or other authorization for supplies delivered or services performed (including order number and contract line item number);

(iv) Description of services;

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

4.8 Order of Precedence

The terms and conditions apply to all Task Orders pursuant to the BPA. In the event of an inconsistency between the provisions of this BPA and the terms and conditions of the Contractor's Schedule 70 contract, the latter shall take precedence.

4.9 Place of Performance

The place of performance will be designed at the Task Order level.

4.10 Travel

Travel requirements will be specified at the Task Order level.

4.11 Security Considerations

Security requirements will be specified at the Task Order level.

4.12 Hours of Operation

The hours of operation will be specified at the Task Order level.

4.13 Post Award Conference

The Contractor shall attend a Post-Award Conference with the BPA Contracting Officer (BPA CO) and the BPA Contracting Officer's Representative (BPA COR) no later than 10 business days after the date of award. The purpose of the Post-Award Conference, which will be chaired by the BPA CO is to discuss contracting requirements. The Post-Award Conference will be held at 301 7th Street, SW, Washington, DC 20407 or via teleconference as determined by the BPA CO.

Post award conferences at the BPA task order level shall be held at the discretion of the awarding task order Contracting Officer (TO CO) if that TO CO determines one to be necessary.

Inasmuch as this BPA does not obligate funds, the Government will not make payment to the BPA holder for attendance at the Post-Award Conference. Attendance at the Post-Award Conference is a subsidiary obligation of the BPA holder.

4.14 Past Performance

Contractor Performance Assessment Reporting System (CPARS) will be utilized to record a Contractor's past performance information on individual Task Orders when applicable.

4.15 Ordering Procedures

4.15.1 General

The DHS Task Order Contracting Officer (TOCO) will award and administer Task Orders in accordance with the ordering procedures set forth in the BPA and the procedures outlined in FAR 8.405-3(c)(2), Blanket Purchase Agreements.

4.15.2 Task Order Request for Quotation (TORQ)

Task Orders will be within the scope, issued within the period of performance, and be within the maximum value of the BPA. Only the Contracting Officer for the BPA may modify the agreement to change the scope, period, or maximum value as allowed by law.

The Task Order Request for Quote (TORQ) will be in writing (via mail, e-mail, or fax) and include a description of the required services, the evaluation or review criteria, and the evaluation or review procedure.

Information obtained from other than the BPA Holder's quotation may be used to determine the quality of the product or service, schedule, cost control, business relations, management, and utilization of small business.

The BPA Holder shall submit a quotation in accordance with the TOCO's TORQ instructions. The information that the TOCO requests from the BPA Holder shall be the minimum needed.

No payment will be made to the BPA Holder for the cost to prepare or submit a Task Order quote.

A TORQ may include clauses applicable to that order.

4.16 Commencing Work

The BPA Holder must not commence work until authorized by the TOCO.

4.17 Annual Review of the BPA

In accordance with FAR 8.405-3(e), the Department of Homeland Security, Office of Procurement Operations, Departmental Operations Acquisition Division which has established this BPA will conduct an annual review to determine whether the underlying Schedule contract is still in effect, whether the BPA still represents best value, and whether the estimated quantities/amounts have been exceeded and additional price reductions can be obtained. The results of this review will be documented in accordance with the Federal Acquisition Regulation.

4.18 BPA Administration

The Contracting Officer (CO) for this BPA is:

Name:	Cynthia Aki
Agency:	Office of Procurement Operations (OPO) Department of Homeland Security (DHS)
Address:	245 Murray Lane, SW, Mailstop #0115 Washington, DC 20528-0115
Voice:	(202) 447-5542
Email:	Cynthia.aki@hq.dhs.gov

The Contract Specialist (CS) for this BPA is:

Name:	Paul Barrett
Agency:	Office of Procurement Operations (OPO) Department of Homeland Security (DHS)
Address:	245 Murray Lane, SW, Mailstop #0115 Washington, DC 20528-0115
Voice:	(202) 447-5464
Email:	Paul.barrett@hq.dhs.gov

The Contracting Officer's Representative (COR) for this BPA is:

Name:	TBD
Agency:	TBD
Address:	TBD
Voice:	TBD
Email:	TBD

SECTION II - STATEMENT OF WORK

1 GENERAL

The Department of Homeland Security (DHS) was officially created in January 2003, merging 22 formerly independent agencies into one cabinet-level department. DHS currently includes fourteen (14) component operational and support organizations. One of the original drivers behind the establishment of the Department was to realize cost benefits and operational efficiencies through business standardization and transformation. When DHS was first established, there were 13 separate core financial systems across its Components, operating under legacy policies and disparate business processes. These systems were comprised of outdated technology, and did not fully support DHS operational requirements. DHS and its Components continue to rely on partially integrated IT platforms, tools, and applications to perform financial management, procurement management, and asset valuation functions. These individual systems provide varying, limited levels of capability with respect to criteria including: interoperability, security, reliability, adaptability and maintainability for standards developed by the Department (e.g., DHS Accounting Classification Structure (ACS)) and/or other Federal laws and mandates (e.g., DATA Act). Enterprise-level solutions that comply with developed DHS standards are needed to aggregate Department-wide financial data for management, oversight, and decision-making purposes.

2 FINANCIAL SYSTEMS MODERNIZATION (FSM) PROGRAM

DHS established the FSM Program in accordance with the Under Secretary for Management (USM) September 2011 memorandum, *"Moving Forward with Financial Systems Projects"*. DHS leadership and Components work together to ensure the FSM Program is planned and executed to meet key financial management requirements, to minimize investment in duplicative systems, to meet Federal guidance, and to deliver financial management information to leadership to support the DHS mission.

To comply with Executive Order 13781, "Comprehensive Plan for Reorganizing the Executive Branch", DHS issued the *"DHS Agency Reform Plan (DARP)"* to guide the improvement of effectiveness, accountability and efficiency. The DARP identifies key outcomes to be sought, in part, through the FSM initiative and its constituent contracts:

- IT Acquisition – Leveraging the Department's buying power, reduce IT procurement costs;
- DHS Procurement Delivery Model – Implement efficient and effective procurement delivery structure and business processes;
- Financial Transactions – Reduce cost, improve efficiency and data quality, and strengthen internal controls through standardizing processes and streamlining systems and services.

At the Department level, the FSM Program is coordinated by the Office of the Chief Financial Officer through the Joint Program Management Office (JPMO). FSM provides a joint framework for coordinating financial, procurement, and asset valuation systems modernization initiatives across the Department and its constituent organizations, and is implemented by means of separate contract vehicles for:

- Competitive selection of commercial off-the-shelf (COTS) software by DHS customers under the Enterprise Financial Management Software (EFiMS) contract vehicle;
- Systems integration, testing, implementation, operations and maintenance support, and disposition of IT under this (EFSI) contract vehicle; and
- Other related services under additional, separate contract(s) (e.g., program management office support, infrastructure hosting).

The integrated FSM IT solution is intended to: enable timely and accurate reporting; be sustainable and effective, scalable, secure and auditable; adhere to federal regulations, Treasury Financial Innovation and Transformation (FIT) and DHS policies; and fully standardize business processes for finance, procurement, and asset valuation according to the DHS Financial Management Systems Standard (FMSS). Standard business processes are to include: "Budget Formulation to Execution", "Record to Report", "Request to Procure", "Procure to Pay", "Bill to Collect", "Reimbursable Management", "Acquire to Dispose", Business Intelligence and Decision Support Reporting", and "Cost Management".

DHS intends to transition all DHS headquarters (HQ) and Components to standard business processes implemented using as few separate solutions as is practicable and cost effective. This effort is intended to reduce cost, improve efficiency and data quality and strengthen internal controls through standardizing processes and streamlining systems and services.

2.1 FSM Program Governance

The OCFO FSM JPMO is responsible for coordinating all efforts to support the FSM Program. JPMO functions include program management, information technology management, and business transformation. The JPMO works with the DHS Component agencies, DHS leadership, and external stakeholders from the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Unified Shared Services Management (USSM) to manage and govern the Program in accordance with the DHS Acquisition Lifecycle Framework and Systems Engineering Lifecycle (SELC). Further, JPMO coordinates governance of financial management shared services in compliance with OMB Memorandum M-19-16 with the Department of Treasury (the designated Quality Service Management Office).

The JPMO supports the implementation and governance of the Financial Systems Modernization (FSM) Program for meeting mission needs and closing capability gaps identified in the FSM Concept of Operations (CONOPS). To date, the JPMO has initiated the first phase of the FSM Program for three Components: U.S. Coast Guard (USCG), Transportation Safety Administration (TSA), and the Countering Weapons of Mass Destruction Directorate (CWMD). The "current state" for the purposes of the EFSI BPA consists of existing legacy systems implemented independently for all DHS Components and directorates, and a developmental target solution for USCG, TSA and CWMD.

The FSM JPMO uses a Portfolio-Program-Project model to ensure proper management of DHS financial system modernization efforts across the Department. Generally, the JPMO funds and manages the FSM portfolio, whereas the Components align Programs and Projects to the Portfolio. The JPMO operates under a charter to the FSM Executive Steering Committee (ESC),

and utilizes standard DHS SELC documents to govern the conduct of all FSM activities. The FSM governance structure is shown below in Figure 1.

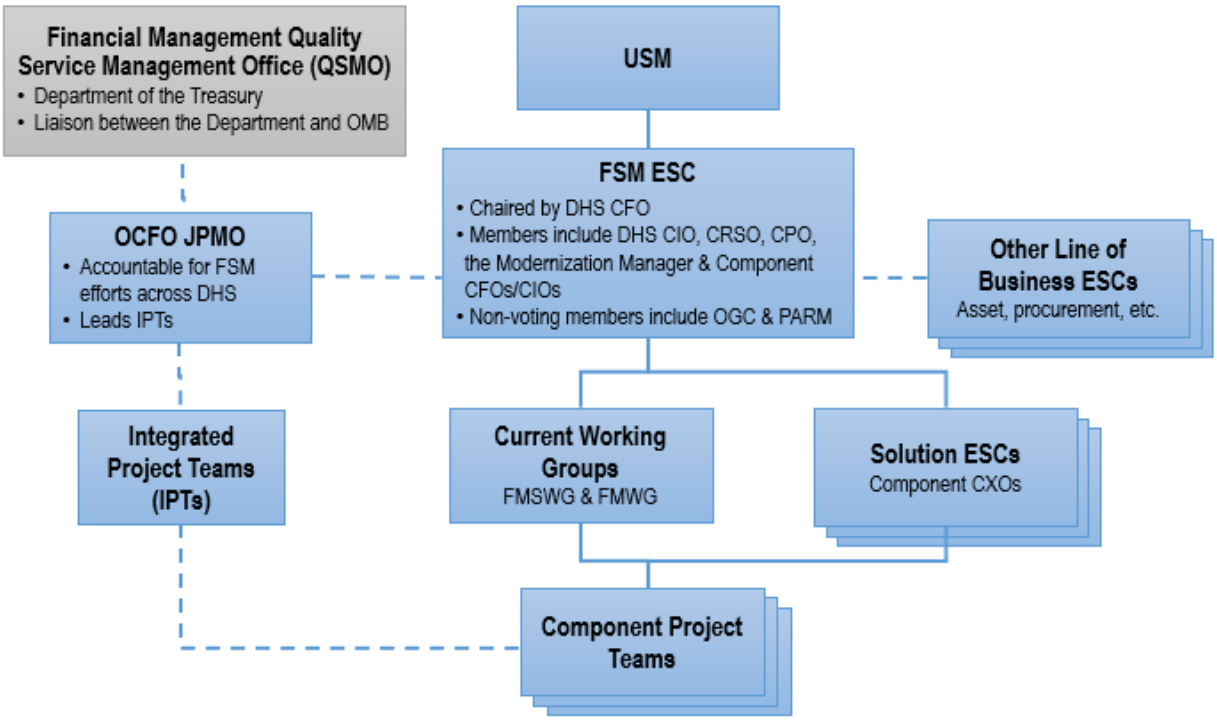

Figure 1: Financial Systems Modernization Governance Structure

2.2 Current State

The current "as is" state consists of multiple "legacy" standalone financial systems and a developmental system being configured for three Components. Transition to a future state target solution for the FSM Program requires systems engineering and integration in order to achieve shared, joint FSM objectives without imposing a singular, pre-determined design. Instead, integration of qualified COTS business application software is intended to streamline and standardize business processes and procedures across the entire organization providing more accurate, timely, and useful financial, procurement, and asset data to managers.

An integrated business software application layer implemented on as few EFiMS systems as is practicable shall enable DHS to more efficiently derive and report on financial statement data both at the consolidated and Component levels. Additionally, the COTS software shall provide procurement community users the capability to meet all mandatory requirements of the Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulations (HSAR). By optimizing the use of shared infrastructure for EFiMS system(s), DHS aims to improve organizational performance and aid all Components in addressing financial audit material weaknesses in internal controls, accounting standards, and system security. Department directorates and Components procure and operate separate information systems to fulfill financial management, asset valuation and procurement management (including contract writing)

business functions. Business applications software is typically licensed and operated as part of IT systems that are provisioned either in Government furnished facilities (data centers) or commercially furnished facilities (service providers). Regardless of how infrastructure is provisioned (deployment model), such IT systems are governed by DHS information security polices and are required to be Authorized to Operate by a DHS/Component Designated Authorizing Official.

Table 1: Current State of DHS Components, below, lists the as-is "legacy" information systems used by DHS and Components to perform financial management, asset valuation and procurement business functions. The shaded cells indicate systems that provide a degree of interoperability for a given Component, either by means of integration native to a COTS software suite or by custom interfaces between standalone applications.

NOTE: Green indicates the system/module is **integrated** with the financial management system. Tan indicates the system/module is **interfaced** with the financial management system. Blue indicates the system/module is **NOT integrated or interfaced** with the financial management system.

Table 1: Current State of DHS Components

Component	Financial Management System	Acquisition Management System	Asset Management System
Federal Emergency Management Agency (FEMA)	Integrated Financial Management Information Systems (WebIFMIS)	PRISM (HQ)	Sunflower Assets (HQ)
U.S. Coast Guard (USCG)	Core Accounting System (CAS) Oracle Federal Financials 11.5.10	Contract Information Management System (CIMS), Financial and Procurement Desktop (FPD)	Oracle Fixed Assets
			Shore Asset Management System (SAMS) (w/Tririga) Housing Management Information System (HMIS), Aids to Navigation System (ATONIS), Asset Logistics Management Information System (***ALMIS***), Naval and Electronic Supply Support System (NESSS)
Transportation Security Administration (TSA)	Core Accounting System (CAS) Oracle Federal Financials 11.5.10 (USCG)	Contract Information Management System (CIMS), Financial and Procurement Desktop (FPD)	Oracle Fixed Assets
			Sunflower Assets (TSA)
Countering Weapons of Mass Destruction (CWMD)	DHS HQ Oracle Federal Financials 12.2	Contract Lifecycle Management (CLM)	Oracle Fixed Assets
			Sunflower Assets (HQ)
U.S. Immigration and Customs Enforcement (ICE)	Federal Financial Management System (FFMS) Release 3.6.1	PRISM (HQ)	Sunflower Assets (HQ) (Personal Property) Vehicle Management Information System (VMIS) Tririga

Component	Financial Management System	Acquisition Management System	Asset Management System
U.S. Citizenship and Immigration Services (USCIS)	Federal Financial Management System (FFMS) Release 3.6.1 (ICE)	PRISM (HQ)	Sunflower Assets (HQ)
Cybersecurity and Infrastructure Security Agency (CISA)	Federal Financial Management System (FFMS) Release 3.6.1 (ICE)	PRISM (HQ)	Sunflower Assets (HQ)
Science & Technology Directorate (S&T)	Federal Financial Management System (FFMS) Release 3.6.1 (ICE)	PRISM (HQ)	Sunflower Assets (HQ)
Office of the Secretary & Under Secretary for Management	Federal Financial Management System (FFMS) Release 3.6.1 (ICE)	PRISM (HQ)	Sunflower Assets (HQ)
Federal Law Enforcement Training Center (FLETC)	Momentum 7.1.2	PRISM (HQ)	Sunflower Assets (HQ)
Office of Intelligence and Analysis (I&A)	Momentum 7.1.2 (FLETC)	PRISM (HQ) (Classified actions are manual, outside of PRISM)	FileMakerPro
Office of Operations Coordination and Planning (OPS)	Momentum 7.1.2 (FLETC)	PRISM (HQ)	Sunflower Assets (HQ)
U.S. Secret Service (USSS)	Enterprise Financial Management System (TOPS) Oracle Federal Financials version 12	PRISM (USSS)	Sunflower Assets (USSS)
Customs and Border Protection (CBP)	SAP Business Suite 7 SAP NetWeaver 7.5	SAP Procurement for Public Sector	Seized Currency and Asset Tracking System (SEACATS) Tririga
			Firearms, Armor, & Credentials Management System (FACTS) Computerized Aircraft Reporting & Material Control (CARMAC) Customs Automated Marine Inventory Tracking System (CAMITS) Maximo Vehicle Management Information System (VMIS)

Table 2: Current State of DHS Components, below, lists the scale, annual budget, operations and funding environments of identified Components:

Table 2 – Scale, Budget, Operations and Funding

Immigration & Customs Enforcement (ICE)	**Scale:** 20,000 Federal Personnel, over 400 offices in United States and foreign countries.
	Annual Budget: $7.9B; 104 Funds/Treasury symbols
	Financial Operations: Provides a financial system and financial transaction services for DHS-HQ, USCIS, S&T, and CISA
Citizenship & Immigration Services (USCIS)	**Scale:** 17,830 Federal and 13,228 contractor employees
	Operations: Field offices in every state and Territory, plus 20 international field offices
	Funding: $4.484B annual budget, 34 funds/Treasury symbols
Cyber & Infrastructure Security Agency (CISA)	**Scale:** 3,542 Federal and 1,833 contractor employees
	Operations: include National Risk Management Center, and Divisions for Cybersecurity, Emergency Communications, and Infrastructure Security
	Funding: $3.387B annual budget, 30 funds/Treasury symbols
Departmental Management Operations (DMO)	**Scale:** 2,346 Federal and 628 contractor employees
	Operations: Financial Operations Division oversees budget formulation and execution, financial transaction processing, financial reporting, and internal controls
	Funding: $1.144B annual budget, 17 funds/Treasury symbols
Science & Technology Directorate (S&T)	**Scale:** 513 Federal and 600 contractor employees
	Operations: Mission & Capability Support, Science & Engineering, Innovation & Collaboration and Enterprise Services
	Funding: $820M annual budget, 28 funds/Treasury symbols
Federal Law Enforcement Training Center (FLETC)	**Scale:** 1,106 Federal and 2,464 contractor employees
	Operations: Facilities in Georgia, New Mexico, South Carolina, and Maryland. Support for International Law Enforcement Academies in Botswana, El Salvador, Thailand and Hungary. Accounting service provider for DHS Office of Intelligence & Analysis (IA) and DHS Office of Operations Coordination (OPS)
	Funding: FLETC: $260M annual direct, ~$120M annual reimbursable. IA/OPS: $260M annual direct. 32 funds/treasury symbols

2.3 Future State

The future state for an "enterprise" Department-wide solution for FSM is described by the FSM CONOPS and refined in the FSM Operational Requirements Document (ORD). All Components are guided by the set of joint requirements for FSM and other Departmental policies including the Department of Homeland Security Agency Reform Plan (DARP). Such policies determine program objectives and constrain the set of alternatives that may achieve the CONOPS. The future state "FSM solution" will consist of materiel and non-materiel solutions that are selected in compliance with Federal Acquisition Regulations, the DHS Acquisition Lifecycle, DHS Systems Engineering Lifecycle, and related legal, regulatory, and policy authorities. FSM Full Operating Capability (FOC) will result from related and coordinated acquisition and systems engineering efforts rather than determined by a single predetermined system design.

The "FSM solution" is a system of systems, the materiel solutions of which are to be specified and procured by DHS headquarters and Components to optimize multiple tradeoffs, including but not limited to: maximizing interoperability and data portability while minimizing duplicative infrastructure, standardizing business operations while allowing for flexibility to accommodate Component-specific operations, and minimizing audit risk while maximizing information security. Generally, the goal is to maximize the probability of providing the required capabilities at the identified service levels under stated conditions while minimizing risks presented from all sources and minimizing the total lifecycle cost of the FSM solution.

3 HOSTING SCENARIOS

Hosting services are not included in the scope of this BPA; however, BPA holders will be required to work collaboratively with DHS hosting providers. The following scenarios are indicative but not prescriptive of the range of outcomes that may follow from the selection of EFiMS software by multiple DHS customers at different times under the separate EFiMS contract vehicle:

- ***"New Software and Platform" Scenario*** - Implementation of a hosting solution that meets requirements without using existing DHS infrastructure to efficiently support the EFiMS software (a new implementation).
- ***"Existing Software, Shared Infrastructure, Separate Instance"*** **Scenario** - Integration/co-location of EFiMS software into an existing hosting solution, located in the same hosted environment as a separate instance, but operated separately at the operating system level. The existing hosting provider will provision a separate independent instance for the implementation of the EFiMS software in an environment that is supported by a different contractor.
- ***"Existing Software, Shared Infrastructure, Separate Books"*** **Scenario** - Utilization of EFiMS software in an existing hosting solution in the same hosted environment and instance as another Component's solution, configured with a separate set of general ledger accounts and/or sub-ledger accounts and operations. Migration of the Component customer into an environment with the same selected EFiMS software, utilizing the same system environment, but as separate "set of books" and operating unit.
- ***"Software as a Service (SaaS)" Scenario*** – EFiMS software is hosted as a service by the EFiMS software vendor. The EFSI Contractor may support customer-specific configuration.

4 OBJECTIVE

Services to be provided under this BPA are intended to achieve the following key objectives:

- Achieve FSM Initial Operating Capability for DHS Components and directorates;
- Achieve FSM interoperability and data portability through configuration, integration and implementation of EFiMS COTS software suites, including as necessary the development and modification of interfaces, extensions, process workflows, and reusable data queries and reports;

- Coordinate service planning, design, transition and operations activities among software vendor(s) and service providers to ensure service levels meet or exceed operational requirements identified in the *Operational Requirements Document for Financial Systems Modernization* (ORD) potentially, for multiple systems in multiple host environments;
- Ensure compliance with public laws, regulations, DHS policies and procedures through systems engineering lifecycle management support, information security technical support, accessibility support and related services for each system;
- Achieve FSM Full Operating Capability, including the conduct of systems operation, maintenance and disposition to required service levels for all DHS Components and directorates.

5 APPLICABLE GOVERNANCE DOCUMENTS

All services provided under this BPA shall comply with DHS policies and procedures, public laws, Executive Orders, federal regulations, and standards in order to support timely performance of DHS and Components' governance processes, including:

1. Chief Financial Officer (CFO) Act
2. Clinger-Cohen Act of 1996
3. Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIG)
4. DHS Acquisition Lifecycle Framework (ALF)
5. DHS Acquisition Management Directive 102-01
6. DHS Enterprise Architecture (EA) framework
7. DHS Financial Accountability Act
8. DHS Homeland Security Enterprise Architecture (HLS EA)
9. DHS Information Security Policy
10. DHS Sensitive Systems Policy Directive 4300A
11. DHS System Engineering Life Cycle (SELC)
12. DHS MD 026-06 Test and Evaluation
13. DHS Instruction 026-06-001, Test and Evaluation
14. DHS Test and Evaluation Master Plan (TEMP) Instruction Guide 0026-06-001-01
15. DHS MD 103-01 Data Management policy
16. DHS MD 139-05 Accessible Systems and Technology Program
17. DHS MD 140-05 Privacy Technology Implementation Guide
18. DHS MD 259-01 Providing Reasonable Accommodations for Employees and Applicants with Disabilities
19. DHS MD 3210 Training
20. DHS Instruction 102-01-004 Agile Development and Delivery for IT
21. DHS Directive 138-01 Enterprise Information Technology Configuration Management
22. DHS Privacy Policy
23. DHS Technical Reference Model (TRM) of approved software
24. Defense Information Security Agency (DISA) Security Technical Implementation Guide (STIG)
25. E-Government Act of 2002
26. Federal Acquisition Regulations (FAR)

27. Federal Information Security Management Act (FISMA)
28. Federal Information Processing Standards (FIPS) 199
29. Federal Information Technology Acquisition Reform Act (FITARA);
30. Federal Managers' Financial Integrity Act (FMFIA)
31. FSM Operational Requirements Document (ORD)
32. Government Management Reform Act (GMRA)
33. Government Performance and Results Act (GPRA)
34. ITIL Service Management v3
35. NIST Special Publication (SP) 800 series guidelines
36. Office of Management and Budget (OMB) Circulars
37. OCFO Financial Systems Modernization Concept of Operations
38. Risk Management Guide for Information Technology Systems
39. Section 508 of the Rehabilitation Act of 1973 as amended
40. Treasury Financial Manual (TFM)
41. The Privacy Act of 1974.

6 SCOPE

The Department of Homeland Security (DHS) requires services to support modernization and transformation of information technology (IT) systems and business processes used for: financial management; procurement and contract writing system management; and asset management and valuation.

The scope of this requirement includes the set of services needed to support the modernization and integration of financial management systems, procurement and contract writing systems, and asset management/valuation systems using EFiMS software. The scope includes technological maturation and evolution of the FSM solution over the lifespan of the BPA. This BPA may be used by all DHS headquarters, directorate, and Component organizations to achieve requirements in the following service areas:

- Program Management Support Services– Manage the services to be provided under this BPA in multi-vendor service provider and shared service environment(s) for Financial Systems Modernization;
- System Life Cycle Management Services – Provide technical and management support for the tasks and sub-tasks under Service Strategy, Service Design, Service Operations, Service Transition, Continuous Service Improvement categories to carry out ordered discovery, systems integration/implementation and operations and maintenance phases in coordination and collaboration with third party(ies) specified at the order level;
- Training Services– Prepare training plan(s) and curricula for software and system use, and provide training via agreed media and instructional methods to identified audiences for all types of system roles.

The scope may include the procurement of tools (including software applications other than EFiMS suites), testing and quality control, configuration management, and training support for

the EFiMS system(s). All EFiMS software application suites to be integrated as part of this BPA are excluded from procurement under this BPA.

The scope includes standardization of data interfaces (logical data exchanges) between the EFiMS system(s) and external "feeder" systems. Whereas the specific interfaces to be integrated under a given order will be specified in each order solicitation, the set of external systems may include but are not limited to the following:

- Payroll (National Finance Center)
- Travel systems (e.g., FedTraveler)
- Treasury systems:
  - Secure Payment System (SPS)
  - Do Not Pay
  - Electronic invoicing (Invoice Processing Platform IPP)
  - Central Accounting and Reporting System (CARS)
  - Intra-Governmental Payment and Collection System (IPACS)
  - G-Invoicing
  - Government-wide Financial Reporting System (GFRS)
  - Government-wide Treasury Account Symbol Adjusted Trial Balance System (GTAS)
  - Treasury Reporting System (TRS)
  - Treasury Offset Program (TOP)
- Grants systems
- Government Services Administration systems:
  - Vendors: System for Award Management (SAM)
  - Federal Business Opportunities (FedBizOps)
  - Federal Procurement Data System – Next Generation (FPDS-NG)
  - GSAxcess.gov and GSA AAMS
- Within DHS:
  - Treasury Information Executive Repository (TIER)
  - DHS Sunflower Asset valuation System (SAMS)
  - Consolidated Asset Portfolio and Sustainability System (CAPSIS)
  - Real Property Data Warehouse (RPDW)
  - Asset valuation Data Warehouse (AMDW)
  - Management Cube
- Bank Cards.

The potential complexity of this requirement stems from multiple criteria including but not limited to: the diversity of legacy systems from which to migrate; the nature of business relationships between Components, in which some Components currently act as service providers to other Components and may do so in the future; the extent to which existing business processes must be adapted to DHS-wide standard FMSS processes; the extent to which Components require interfaces with different external systems and/or integration with internal systems; the potential diversity of infrastructure hosting scenarios; and the joint program governance methodology DHS intends to use for financial systems modernization over the life of the EFSI BPA.

Note: All EFiMS software application suites to be integrated as part of this BPA are excluded from procurement under this BPA and task orders issued under this BPA. Advisory, review and/or recommendation services related to any potential selection of EFiMS software suites are excluded from this BPA and task orders issued under this BPA.

7 REQUIREMENTS

The Contractor shall provide qualified personnel to support the services identified below, as required at the task order level.

7.1 Task 1: Program Management

DHS requires expert program management skills and abilities to seamlessly deliver the full range of program management services to support DHS customer requirements consistent with system lifecycle phase. The anticipated scale and complexity of the FSM program involves near-term transition of Component(s) to target solution(s) as well as long-term technological evolution to a Full Operating Capability for FSM, which may require the Contractor to manage multiple simultaneous projects across multiple customers over a multi-year timeframe. Services under this section are to include orders placed for program and project management during the SELC "Obtain Phase", and program management for orders placed during the SELC Operations and Maintenance Phase.

The Contractor shall:

a) Manage all services provided to support the achievement of the FSM program objectives;
b) Plan, schedule, and coordinate EFSI services with FSM stakeholders and customers;
c) Work collaboratively and cooperate with EFiMS and EFSI related support service contractor personnel;
d) Coordinate and provide informed recommendations to Government personnel regarding program performance, quality, schedule, cost and risk minimally consistent Project Management Institute's Project Management Body of Knowledge (PMBOK) (6th edition or latest published version).
e) Provide quantitative and qualitative risk management using industry standard risk management guidelines (e.g., the Project Management Institute (PMI))
f) Implement a comprehensive communications management strategy that supports the FSM Program across all customers supported by the EFSI contractor;
g) Provide an organizational change management strategy that ensures changes are smoothly and seamlessly implemented;
h) Develop and implement quality management for all areas of program performance in accordance with a Responsible, Accountable, Consulted and Informed (RACI) model;
i) Develop and maintain an Integrated Master Schedule for EFSI contractor's order(s);
j) Establish and provide metrics of value in accordance with ANSI/EIA-748 standard for all work performed under the BPA by applying standard EVM techniques; and
k) Manage projects and provide task order deliverables as defined at the task order level.

7.2 Task 2: Service Strategy Management

DHS requires service strategy management services for meeting DHS and Component FSM business objectives and outcomes. The following sub-sections apply when specified at the task order level:

7.2.1 Requirements Management

The Contractor shall:

a) Prepare and implement a methodology for documenting, tracing, prioritizing and agreeing on FMS requirements for: financial management; procurement and contract writing; and asset valuation processes;
b) Provide technical/governance reviews, evaluation, and recommendation of creation and changes to the Requirements Traceability Matrix (RTM);
c) Translate user requirements into system specifications, data management plans, program life cycle management documentation, integrated logistics support plans and related operational summaries; and
d) Provide a Requirements Management Plan, as required and defined at the task order level.

7.2.2 Performance Management

The Contractor shall:

a) Research, plan and document a performance management strategy consistent with DHS policies;
b) Deliver a performance management strategy that supports timely performance monitoring and reporting of work performed under EFSI order(s);
c) Design, develop and implement a performance management strategy that facilitates reporting on FSM metrics using EVM reporting techniques.

7.2.3 Availability Management

The Contractor shall:

a) Review and recommend changes to current availability requirements defined in the ORD
b) Ensure that all IT infrastructure, processes, and tools are appropriate for the agreed level of EFiMS system availability as described in the ORD;
c) As defined at the task order level, provide an Availability Management Strategy document that addresses the approach for achieving reliability growth through progressive reduction of mean time between failures (MTBF), mean time to restore system (MTRS) and root cause analysis.

7.2.4 Data Management

The Contractor shall:

a) Provide data management services that account for interoperability with external systems listed as identified in task orders;
b) Plan and Implement methods for database management, administration, and documentation for the EFiMS, to include creation, installation, and maintenance of databases;
c) Deliver a Data Management Plan documenting data migration activities, as required and defined at the task order level;
d) Deliver a Data Security Management Plan, as required and defined at the task order level.

7.2.5 Security- System Access Control, Data, Governance Regulation Control

The Contractor shall:

a) Research, plan and document a methodology to establish and maintain user access controls, implement partitioning, and establish Governance Regulation Controls (GRC) in accordance with public laws, regulations, standards and DHS directives and policies;
b) Deliver a GRC that ensures secure access to DHS data and business rules for use by other Component or enterprise-wide composite applications and/or extended multi-application business processes;
c) Provide a Security Access Plan, as required and defined at the task order level.

7.2.6 Data Preparation and Staging

a) Develop a data cleansing plan to ensure (1) the quality of the migrated data; (2) the ability of the operational community to use the migrated data; (3) that all the data sent from the government is fully loaded; and (4) that the data accuracy and validation is acceptable;
b) Support mock conversion, dress rehearsal, and dry-run activities, as required;
c) Perform data cleansing processes in accordance with applicable government and industry best practices for data quality management. Verify that the data is consistent with applicable DHS policies and in accordance with all applicable federal government regulations, requirements, and pertinent industry standards;
d) Ensure the quality of EFiMS data for integrity, availability, accuracy, completeness, uniqueness, timeliness, validity, and consistency;
e) Assist or lead, perform and execute cleansing and extraction of data from legacy data systems into an intermediate data staging area for transformation and loading by the EFSI system integrator into the “target system(s)” and data warehouse (as applicable);
f) Review, update and complete the legacy systems and data analysis strategy and Work Plan for collecting and analyzing legacy systems’ artifacts;
g) Develop and submit legacy systems analysis reports and participate in the disposition recommendation of legacy systems;

h) Assist legacy systems data cleansing and extraction to the staging area in collaboration with DHS components;
i) Provide a data analysis report from the data audit (e.g., description of problem, data source, number of occurrences, impact on production data, type of fix that was applied, number of records fixed, and #of records unable to be fixed);
j) Coordinate and schedule data staging and preparation activities, as required at the task order level, with the specified EFSI system integrator when the integrator is a separate party.

7.2.7 Migration Management

The Contractor shall:

a) Deliver for government approval a Migration Management Strategy document, as defined at the task order level; data migration strategy section shall address gathering the data requirements for all feeder systems, mock data conversions, and coordination with any third-party contractor(s) as required;
b) Manage, schedule and coordinate FSM migration activities and implementation with all parties;
c) Set up the staging environment(s);
d) Load, test and validate converted data in the solution;
e) Adapt the migration strategy to make use of new technologies as EFiMS evolves from Initial Operating Capability to Full Operating Capability.

7.2.8 Software License and Asset Valuation

The Contractor shall:

a) Develop a strategy to manage the EFiMS software license and Asset valuation life cycle to analysis, recommendations and migration management of current financial, procurement and contract writing system, and asset valuation software licenses;
b) Deliver Software License and Asset Valuation Strategy document, as required and defined at the task order level.

7.2.9 Integration Management

The Contractor shall:

a) Research, plan, and document a strategy for supplier coordination, collaboration, interoperability and delivery of standard and non-standard integrations;
b) Provide an integration strategy encompassing interoperability with external systems; incorporate hardware and infrastructure components with business application and software designs;
c) Test newly developed software with existing components;
d) Develop software prototypes required for system design or capability analysis;

e) Document system integration testing, including interface testing in a User Acceptance Test (UAT) Plan, as required and defined at the task order level;
f) Provide an Integration Management Strategy document, as required and defined at the task order level;

7.2.10 Demand Management

The Contractor shall:

a) As specified at the order level, prepare a Demand Management Plan for the customer to forecast, analyze, predict and control the demand for services under the BPA;
b) As specified at the order level, implement a government-approved Demand Management Plan.

7.2.11 Testing - Quality Assurance

The Contractor shall:

a) Research, plan, and document an EFiMS Functional, Non-functional and Security Testing Strategy using an industry standard and best practice, repeatable test methodology, and automated testing tools;
b) In accordance with the DHS Test and Evaluation Master Plan Instruction Guide, provide for government approval an overall Contractor Test and Evaluation (T&E) plan detailing the test methodology, and support requirements to support the plan as required and defined at the task order level; and
c) Deliver a Quality Assurance Strategy document, as required and defined at the task order level.

7.2.12 Service Portfolio Management

The Contractor shall:

a) Define and analyze new or changed services within a portfolio. Develop a complete list of the services managed by the service provider, and make recommendations regarding the government's review and approval of new/changed services.

7.2.13 Business Relationship Management

The Contractor shall:

a) Research, plan and document a strategy to manage current and anticipate planned customer needs by exploring new technologies that may be relevant to the DHS FSM Program, and to refresh existing technologies;
b) Deliver a Business Relationship Management Strategy document, as required and defined at the task order level.

7.2.14 Service Catalog Management

The Contractor shall:

a) Develop a strategy for service catalog management that encompasses an integration strategy with other service management capabilities.

7.2.15 System and Application Monitoring

The Contractor shall:

a) Provide continuous system and application monitoring plan for the EFiMS system integrated into the agency's SELC and IT Security processes.

7.2.16 Configuration Management Plan

The Contractor shall:

a) Provide a Configuration Management Plan that describes specific procedures and the extent of their application during the life cycle; and identifies roles and responsibilities for carrying out configuration management;
b) Support effective, predictable and repeatable configuration management processes.

7.2.17 Physical Security Plan

The Contractor shall

a) Establish and maintain a physical security and conduct a periodic physical security audit consistent with security controls appropriate for the relevant FIPS 199 rating;
b) Tailor and integrate physical security controls with DHS data center security processes and procedures;
c) Integrate physical security controls with FSM logical controls.

7.2.18 Privacy

The Contractor shall:

a) Establish and maintain a privacy plan and conduct a periodic privacy audit;
b) Make recommendations for modifications or improvements in privacy;
c) Ensure that an approved Privacy Policy has been established, all Personally Identified Information is identified within FSM;
d) Ensure that privacy controls have been established and are monitored.

7.3 Task 3: Service Design Management

DHS requires service design management in support of the FSM effort for one or more of the following phases: discovery, transition, implementation, and operations and maintenance. The following sections apply when specified at the task order level:

7.3.1 Solution Architecture and Design Management

The Contractor shall:

a) Design, document and maintain a solution architecture that meets all operational requirements, functional requirements and non-functional requirements as specified at the task order level;
b) Identify and provide all artifacts required to specify the conceptual, logical and physical solution architectures as relates to services, data, enterprise architecture, security and system-level architecture;
c) Prepare and deliver the EFiMS system design, and maintain documentation of all approved changes;
d) Review, recommend, and update EFiMS architecture;
e) Ensure proposed architecture is in conformance to HLS Enterprise Architecture Standards and all DHS and its Components governing documents associated
f) Identify non-conformance, risk and estimated cost of non-conformance and recommend strategy for achieving conformance;
g) Evaluate as-is architecture for Business, Application, Enterprise, and Infrastructure services;
h) Review, recommend, and update architecture for middleware integration such as Service Oriented Architecture (SOA)/Enterprise Service Bus integration and other integration requirements;
i) Describe how they plan to implement middleware integration for the EFiMS interfaces; and

j) Prepare and deliver detailed EFiMS system/solution architecture documentation to support all system configuration, design verification, and implementation of reports, interfaces, extensions, conversions, forms and workflows;
k) Prepare the test design framework, test case specification(s), acceptance test procedures, test scripts, and test reports;

7.3.2 Fit Gap Analysis

The Contractor shall:

a) Conduct fit/gap analysis, evaluate design alternatives and recommend design based on established alternative analysis methodology;
b) Evaluate as-is service architecture(s) and design;
c) Evaluate and update EFiMS architecture and design based on industry best practices, evolution of new architectures and design patterns; and

d) Prepare and deliver EFiMS solution design documentation as Service Design Package(s) to include: requirements, service design, organizational readiness assessment, and service lifecycle plan;
e) Conduct a fit-gap assessment to evaluate how customer requirements will be met and what tailored solutions will be required;
f) Document and analyze the service architecture and design of the as-is system and target system/services, including expected performance capabilities
g) \Document, ensure accuracy and completeness and maintain all requirements in the Requirements Traceability Matrix (RTM)
h) Validate interfaces and functional configurations against customer requirements and existing documentation;
i) Elicit and document customer's prioritization for implementing functionality of the target system/service; and
j) Provide Custom Reports addressing custom configurations and software such as interfaces, extensions, forms and workflow requirements as required and defined at the task order level.

7.3.3 Security Management

The Contractor shall:

a) Develop and manage Order customer's EFiMS security architecture;
b) Recommend role-based access control design for access to the EFiMS system;
c) Assist in role-based access control implementation and management;
d) Evaluate impact of changes to EFiMS system security architecture and design due the EFiMS software updates/system upgrades;
e) Provide security documentation and/or input to the Order customer's Information Systems Security Officer (ISSO) to obtain the EFiMS system Authority to Operate (ATO) according to FISMA Assessment and Authorization (A&A) requirements;
f) Maintain and update the Data Security Management Plan for the EFiMS (see 5.3.4.5);
g) Develop and submit a Security Test and Evaluation (ST&E) plan for Government approval prior to conducting ST&E activities;
h) Support EFiMS system ATO as required within the timeframes established;
i) Prepare documentation and provide information to support the certification (authorization) / accreditation process requested by the DHS or Component CISO, Information System Security Manager or Information Security Officer; and
j) Coordinate to complete all required certification (authorization) and accreditation documentation, actions and approvals necessary to obtain an interim ATO prior to deployment of the system.

7.3.4 Integration Architecture, Design and Management

The Contractor shall:

a) Develop, recommend, implement, update and manage Service Oriented Architecture (SOA)/Interface/Third-party system integration architecture and design;

b) Provide EFiMS system integration architecture(s) and design(s) documentation;
c) Support middleware integration, such as SOA/Enterprise Service Bus integration, that are defined in the Order customer's solicitation;
d) Support the sharing of data between various Government and Commercial entities using standard protocols.

7.3.5 Data Architecture and Design

The Contractor shall

a) Develop a data management plan to ensure (1) the quality of the migrated data; (2) the ability of the operational community to use the migrated data; (3) that all the data sent from the government is fully loaded; and (4) that the General Ledger data accuracy and validation is acceptable

7.3.6 System Performance Management

The Contractor shall:

a) Define, recommend, develop, implement, update and manage EFiMS System Performance Metrics and Reporting;
b) Provide EFiMS system(s) that meet or exceed the service related Key Performance Parameters (KPPs) and corresponding Measures of Performance (MOPs)
c) Conduct performance testing to ensure these metrics are continuously being met;
d) Coordinate and collaborate with the hosting provider to conduct this testing and remediate any identified issues;
e) Conduct customer surveys to ensure the users are receiving the expected response times and remediation for issues that arise on a consistent basis;
f) Work with the appropriate responsible party to remediate the issues;
g) Work with the hosting provider to meet KPPs.

7.3.7 Service Validation/Testing Design

The Contractor shall:

a) Develop and deliver EFSI Test Management Plans prior to conducting ST&E activities;
b) Develop and manage testing framework;
c) Develop Test Design Specifications;
d) Develop Test Cases and test scripts;
e) Provide document updates to the RTM;
f) Design, develop and document a User Acceptance Test Plan according to user requirements;
g) Manage EFiMS System UAT, Regression, Performance, Scalability, Non-functional, Integration, Performance (Load/Stress) and Security Testing;
h) Prepare EFiMS System Test and Acceptance Reports;
i) Develop Integration test design framework;

j) Define, develop, implement and manage Service Design to support Federal, DHS, and Component compliance requirements.

7.3.8 Design Coordination

The Contractor shall:

a) Coordinate development of solution architecture and design, including Third party system integration architecture and design.

7.3.9 Service Level Agreement (SLA) Management

The Contractor shall:

a) Define, develop, and design performance SLAs based on KPPs, MOPs and Measures of Suitability (MOSs).

7.3.10 Availability Management

The Contractor shall:

a) Review and recommend changes if any to current availability requirements
b) Manage relevant MOSs defined in the ORD.

7.3.11 Demand Management

The Contractor shall analyze, recommend, implement architecture and design to support capacity requirements.

7.3.12 IT Service Continuity Management

The Contractor shall:

a) Define, develop, and manage Disaster Recovery and Continuity of Operations (COOP) system architecture and design for EFiMS;
b) Develop specific contingency and disaster recovery plans relevant to each business application, and shall incorporate those plans into the DHS's overall Disaster Recovery/Business Continuity (DRBC) planning structure;
c) Coordinate full testing and tabletop testing of each plan with the target infrastructure hosting provider and business operations subject matter experts (SMEs) at least annually, or more frequently if so required by the plan, and shall perform a full evaluation of each test at its completion, making recommendations for improvements or modifications to existing plans, infrastructure (hosting agreements) or procedures as appropriate; and
d) Maintain business application processes, policies and procedures related to preparing for recovery or continuation of critical business application functionality;

e) Plan and implement the DRBC program and shall coordinate with the DHS Component business operations subject matter experts (SMEs) and infrastructure hosting provider to ensure the DRBC program is defined, documented, and exercised in accordance with DHS policy.

7.3.13 Supplier Management

The Contractor shall:

a) Manage the procurement and provision of all goods and services the Contractor obtains from one or more third parties by outsourcing, sub-contracting, application service provision or other means;
b) Provide, record, and track all information for Configuration Items including items sourced from third-parties.

7.3.14 Business Process Reengineering

The Contractor shall:

a) Review and analyze the customer's needs for transforming current business processes to EFiMS processes; evaluate tradeoffs between organizational changes and customizations/extensions of EFiMS solution; demonstrate the product(s) being proposed to meet the solution, both pre- and post- design; and coordinate with organizational change management processes and vendors to implement new business processes.

7.3.15 Service Desk Planning

The Contractor shall:

a) Prepare a plan for a service desk function to ensure EFiMS users receive appropriate assistance in a timely manner according to service levels specified at the task order level. The Service Desk Plan shall address the following minimum requirements:
    - Provision of live support services via phone, email, and online chat Monday through Friday (excluding holidays) from 8:00AM until 5:00PM Eastern time. Outside of these standard business hours, the Contractor shall provide on-call support via phone. Self-help services shall be available at all times (24x7). Tier levels are defined in the Glossary.
    - Staffing, managing, and equipping the service desk sufficiently to ensure compliance with the service desk performance standards;
    - Logging severity levels for all incidents opened by the service desk according to defined severity levels;
b) Develop and implement training materials, triage processes, and service desk tools necessary to provide end users support.

7.4 Task 4: Service Operations Management

DHS requires service operations management for developmental and/or operational EFiMS system environment(s) including but not limited to: development, test, system integration, sandbox/demonstration, training, and production. The following sections apply when specified at the task order level:

7.4.1 Service Operations

The Contractor shall:

a) Maintain the availability, functionality, operability, compliance, responsiveness and operations of the EFiMS system;
b) Provide services under this section in accordance with Service Level Agreement(s) established at the task order level.

7.4.2 System and Application Monitoring

The Contractor shall:

a) Perform and report on the continuous monitoring of the EFiMS;
b) Prepare and deliver a System and Application Monitoring Plan;
c) Provide System and Application Monitoring Summary Report;
d) Provide system and application monitoring log data;
e) Produce all required/pertinent documentation to comply with FISMA and DHS security requirements for maintaining the authority to operate the EFiMS system;
f) Monitor system storage including total capacity; availability; utilization with projections based on current use;
g) Monitor Application performance system, application, and module availability; average response time to the system, application and modules; error rates; user utilization (maximum, mean, and median numbers licensed); and application system utilization (CPU, Memory, Storage and Network);
h) Contractor shall perform preventive, corrective, perfective and adaptive sustainment engineering, and corrective maintenance for all business applications and associated databases.

7.4.3 System Administration

The Contractor shall:

a) Perform preventive, corrective, perfective and adaptive sustainment engineering, and corrective maintenance for all business applications and associated databases in the EFiMS system;
b) Maintain a catalog of user roles and access profiles defined as user listings and functional hierarchies of all the roles in the EFiMS system, including types of users;

c) Provision user access requests including verifying the user authorization and access; creating and maintaining user profiles; providing access rights; monitoring the identity status; removing or restricting access; and logging and tracking users' access;
d) Review all roles periodically to support security and audit compliance requirements in coordination with the ISSO.
e) Manage and control user access to each application, module, function, and report a user can access;
f) Monitor, operate, configure and maintain the operating system(s) of the EFiMS system;
g) Install and configure all software per the Configuration Management and Change Management guidance and Contractor's Government-approved Configuration Management Plan;
h) Lead and execute all system security activities within the EFiMS system environment;
i) Document all current and proposed system designs and settings according to Government approved content and format requirements;
j) Prepare and execute an interface plan that provides comprehensive and error-free support for all interfaces in order to ensure interoperability between EFiMS system(s) and other Government specified systems;
k) Perform system performance tuning as required;
l) Troubleshoot all system issues, and document and record the issue, status, resolutions and follow-up actions.

7.4.4 Performance Management

The Contractor shall:

a) Conduct performance testing to ensure the system is meeting performance standards.
b) Conduct customer surveys to ensure the users are receiving the expected performance (e.g., response times and remediation for issues that arise on a consistent basis).
c) Coordinate and collaborate with other responsible parties (Government and Contractor) to analyze performance issues reported by users by utilizing tools/ appliances to determine where issues exist either in the hardware, network, application, etc., and shall work with the appropriate responsible party to remediate the issue.
d) Collaborate with the hosting provider to meet the KPPs, MOPs and MOSs.
e) Report downtime for the business application, databases and system interfaces. The Contractor shall coordinate this reporting with the hosting provider.
f) Coordinate with the hosting provider support personnel in executing any downtime event and report consolidated downtime for business application, databases and system interfaces supported by the Contractor as well as hardware and network components support by the hosting provider through a single downtime reporting system
g) Provide Performance Management Reports, Customer Survey Reports, and Downtime reports as required and defined at the task order level.

7.4.5 Configuration Management

The Contractor shall:

a) Ensure all changes to configuration items are documented and identify/document the interrelationships between configuration items;
b) Track the status of a configuration, providing traceability of configuration items throughout their development and operation covering the entire change management lifecycle.

7.4.6 Source Code and Documentation

The Contractor shall:

a) Create and maintain all EFSI Contractor-created source code and documentation, including COTS software items in DHS approved repositories.

7.4.7 Change Management

The Contractor shall:

a) Develop, manage and execute a communication strategy, a communication plan, change management guidance, activities and reporting;
b) Propose, implement and facilitate a structure for a change control process, change review board, and change control board.
c) Plan, design, develop, and implement of all EFSI program and project communications initiatives and materials;
d) Develop and deliver oral and written presentations and reports to multiple levels of management, including executive leadership regarding change management.
e) Define measurable stakeholder aims and create a business case for their achievement
f) Monitor assumptions, risks, dependencies, costs, resource impacts, and rate of change acceptance;
g) Recommend an effective education, training and/or skills upgrading strategy for the organization;
h) Monitor implementation and refine the change management process as required.

7.4.8 Software Updates Installation

The Contractor shall:

a) Install major and minor updates of COTS applications to the latest Government approved version, in the time period required;
b) Proactively manage the application of software updates to include ensuring appropriate system restoration plans are in place prior to beginning any patch cycle.

7.4.9 Patch Management

The Contractor shall:

a) Proactively manage the application of software patches to include ensuring appropriate system restoration plans are in place prior to beginning any patch cycle;
b) Ensure the entire patch management process and procedures are documented in the Configuration Management plan;
c) Implement a system test environment that mirrors the production environment to test all patches and updates;
d) Monitor and evaluate the implementation of all patches and evaluate their performance in the production environment.

7.4.10 Test Management

The Contractor shall:

a) Conduct testing and evaluation to support all phases of configuration management, and provide planning, development, test and O&M support to investigate, resolve, track and report EFiMS application performance (issues and errors);
b) Coordinate with the infrastructure hosting provider, DHS Office of the Chief Information Officer (OCIO) and the Component OCIOs to investigate and resolve network issues that degrade or affect the EFiMS user's ability to access and use the system.
c) Plan, prepare for, and conduct test readiness reviews;
d) Develop, update, and perform configuration management of test plans; ensure that test plans prioritize regression tests based on risks and resources; and maximize the use of automated testing;
e) Develop, update, and perform configuration management of test scripts; ensure the scripts contain the steps and data necessary to verify cited requirements and design use cases;
f) Execute tests in accordance with government-approved test plans and provide in-person and remote access to DHS, Components, and Operational Test Agent (OTA) representatives;
g) Develop test reports and perform other post-test activities in accordance with the test plan;
h) Ensure defects that are also applicable to the production instance can be readily tracked following the test event;
i) Review test reports to gauge the potential for past issues to impact the instance received and avoid similar problems; and
j) Track and manage open and resolved issues, ensure audit capabilities are enacted to collect and log security audit and application performance data, and review audit and performance logs.

7.4.11 Capacity Management

The Contractor shall:

a) Coordinate with the infrastructure hosting provider to manage EFiMS system capacity consistent with demand plan(s), and to ensure reliability, availability and maintainability performance requirements are met under normal and surge operating conditions;

b) Provide system performance tools, techniques, and processes to optimize system throughput and user response time.

7.4.12 System Backups

The Contractor shall:

a) Create and execute a backup, offsite storage, and recovery plan that guarantees the security of financial data consistent with the FIPS 199 rating of the EFiMS;
b) Implement a backup policy and process for all elements of the system to ensure backups of all data and configurations are routinely stored and viable;
c) Periodically test the backups and restore process to ensure it operates entirely.

7.4.13 Service Desk Operations

The Contractor shall:

a) Perform all activities needed to provide Tier 1, 2, and 3 service desk support for the EFiMS system;
b) Provide statistical and performance reporting based on service desk activities;
c) Provide a monthly Service Desk Performance Report, as required and defined at the task order level.

7.4.14 Data Management

The Contractor shall:

a) Perform database management, administration, and documentation for EFiMS system, to include creation, installation, and maintenance of databases for project and mission support, configuration of accounts per mission-specific requirements, and verification of application and database backup processes for system recovery purposes;
b) Coordinate with the infrastructure hosting provider to document the standard operating procedures, as required and defined at the task order level;
c) Transmit required information through authorized systems interfaces and make that information available to users via Contractor furnished or Government furnished data analysis and reporting capabilities (e.g., data warehouse, business intelligence application(s)).

7.4.15 License Management

The Contractor shall:

a) Proactively manage the licenses for EFiMS software to ensure appropriate levels of support, feeding data as necessary into the monitoring and control and problem management functions

b) Provide and manage software licenses required for EFiMS infrastructure excluding EFiMS software suite(s);
c) Support the management of EFiMS software suite licenses by coordinating with and providing required information to EFiMS software vendor(s) to optimize availability to users while minimizing cost
d) Validate the license requirements for the Component on an annual basis and forecast the projected Component licensing requirements for three years; not including the current year.

7.4.16 Event, Incident and Problem Management

The Contractor shall:

a) Develop, implement, and manage effective ITIL-based event, incident, and problem management including content standards; format standards; nomenclature standards; government approved escalation process/entities; and reporting standards;
b) Develop and manage effective ITIL based incident management techniques to ensure the restoration of service to normal levels with a minimum of impact to users or systems;
c) Track, manage and report on problem resolution to ensure the root cause is addressed.

7.4.17 Compliance Management

The Contractor shall:

a) Develop and operationally support compliance management to ensure compliance with all requirements, regulations and laws;
b) Ensure that all compliance requirements are adhered to;
c) Support all Government sanctioned audit activities.

7.4.18 System Security

The Contractor shall:

a) Provide certification documentation and training for the System Security Plan and conduct periodic reevaluation and auditing of the plan
b) Provide recommendations to DHS for modifications or improvements in overall system security
c) Document and manage controls such that the ATO is maintained.

7.4.19 Disaster Recovery

The Contractor shall:

a) Coordinate with the DHS Component business operations subject matter experts (SMEs) and infrastructure hosting provider to ensure the DRBC program is defined, documented, and exercised;

b) Support exercising annual Contingency Plans for each system developed, deployed and maintained by DHS;
c) Develop specific contingency and disaster recovery plans relevant to each business application, and incorporate those plans into the DHS's overall DRBC planning structure;
d) Coordinate testing of each plan with the future infrastructure hosting provider and business operations subject matter experts (SMEs)
e) Perform a full evaluation of each test at its completion, making recommendations for improvements or modifications to existing plans, infrastructure (hosting agreements) or procedures as appropriate.
f) Maintain business application processes, policies and procedures related to preparing for recovery or continuation of critical business application functionality, with amount of time to cutover not to exceed Government specified time limit;
g) Ensure a system recovery capability that will support Government goals and objectives in accordance with established system availability requirements;
h) Provide the capability for primary and backup systems to support recovery of all critical software programs and sensitive Government information;

7.5 Task 5: Service Transition Management

DHS requires contractor performance of ITIL service transition management. The following sections apply when specified at the task order level:

7.5.1 Service Transition

The Contractor shall:

a) Develop a project management plan that articulates how the transition from the current state to the future state will be planned, coordinated communicated, managed, executed, monitored and controlled and updated to reflect any relevant changes throughout project's lifecycle.
b) Review and manage the Government's Functional Requirements for EFiMS service delivery;
c) Review and manage the Government's Requirements Traceability Matrix updates;
d) Develop a Vendor interoperability plan to define the roles and responsibilities and interactions with all relevant vendors and service providers to ensure a successful transition to EFiMS system;
e) Analyze, recommend and manage migration of current financial, procurement and contract writing system (s), and asset valuation COTS software licenses/subscriptions to support the development of a license/subscription management plan;
f) Develop an Operational Readiness Assessment and Plan to validate and propose controls necessary to deliver consistent, efficient services in a secure and effective manner;
g) Conduct a hosting environment assessment;
h) Develop and implement a Transition Risk management plan that identifies risk, assess risk, develops migration strategies, monitors risk, monitors mitigations strategies, documents and reports the status of risk;

i) Develop, update and maintain a Transition Plan that support the successful migration to the target EFiMS;
j) Develop a Quality Control Plan describing how the contractor will achieve and maintain acceptable quality levels for all transition activities, deliverables and work processes
k) Implement quality monitoring capability that will verify that project deliverables meet defined quality standards;
l) Develop and implement a Transition Master Test Plan identifies the scope, strategy, objectives, approach, and details all testing phases including the testing methodology, schedule, constraints, resources, environment requirements, and mechanisms for documenting and tracking test results.
m) Maintain a testing risk registry that describes the risks, impact levels and risk mitigation strategies. The Contractor shall develop, update, and review Test Management Plan for Functional, System, Performance, Regression, and Security Testing;
n) Develop and execute Knowledge Management;
o) Develop and implement an organizational change management process based upon an industry standard change model acceptable to the Government (e.g., ADKAR)
p) Execute, update and maintain a Data Management Plan;
q) Provide an Order Phase-Out Plan for transitioning work from one Contractor to another as required and defined at the task order level.

7.5.2 Transition In/Out Services

The Contractor shall:

a) Provide “Transition in” support to transfer/migrate services from current “as is” financial, asset and procurement system and contract writing systems(s) to the EFSI services;
b) Provide “Transition out” support to transfer/migrate services from EFiMS system(s) to other Government specified solution(s).

7.6 Task 6: Training Services

DHS requires services to support planning, preparation and delivery of training for EFiMS system(s) to achieve Initial Operating Capability (IOC) and to achieve and maintain Full Operating Capability (FOC). For the IOC phase, DHS requires full service including curriculum development and training delivery to support organizational change goals. During FOC phase, DHS requires steady state service to include training delivery to support goals for workforce skills maintenance.

The Contractor shall:

a) Prepare and deliver a Training Plan for government acceptance;
b) Deliver, maintain and update end-user training, ongoing/refresher training, and system administrator training;
c) Deliver training via multiple different modes to accommodate different audience sizes, locations within the continental U.S., and availability of internet access;

d) Conduct trainee pre- and post- assessments according to standard methodologies and tools (e.g., Sharable Content Object Reference Model);
e) Develop, distribute, and update training reference materials (e.g., desk reference, “handy” guide, Frequently Asked Questions (FAQs), etc.) and delivery media;
f) Ensure all e-training delivery is accomplished via a user interface compliant with the Rehabilitation Act Section 508 for a scalable audience size.

SECTION III - INSTRUCTIONS TO QUOTERS

(This section will be removed upon award)

1 INTRODUCTION

This acquisition will be conducted under the auspices of the DHS Procurement Innovation Lab (PIL). The PIL is a virtual lab that experiments with innovative techniques for increasing efficiencies in the procurement process and institutionalizing best practices. There is nothing you need to do differently for this requirement. The PIL project team may reach out to successful and unsuccessful Quoters to assess effectiveness of the procurement process and the innovative techniques applied. The anonymous feedback will be used to further refine DHS procurement practices. Additional information on the PIL may be found at *www.dhs.gov/pil*.

This RFQ is issued under the General Services Administration (GSA) Multiple Award Schedule (MAS) 70, *General Purpose Commercial Information Technology Equipment, Software, and Services* contract. Only prime contractors under GSA MAS 70 may submit an offer for this requirement. This procurement will be conducted in accordance with FAR 8.405.

2 GENERAL QUOTATION PREPARATION INSTRUCTIONS

Quoters shall submit their quotations via email in accordance with the instructions contained herein. Quoters shall submit their signed quotations as "PDF" documents except when specified otherwise.

Each electronic file shall be clearly named in accordance with the solicitation provisions. The Quoter's electronic quotation shall be submitted according to the requirements set forth below:

1) The entire quotation shall be submitted in .pdf format, with the exception of any pricing documents which shall be submitted in MS Excel format.
2) Adobe Acrobat shall be used to create the .pdf files.
3) All submissions shall include 70RDAD19Q00000101 in the subject line of the conveying email.

Quotations submitted electronically will be considered late unless the Quoter completes the entire transmission of the Quotation before the closing date and time for receipt of Quotations under this solicitation. Late Quotations will not be eligible for award. Quotation transmission must be completed by the date and time indicated below. Please Note: As applicable, these submission instructions will also apply to any future correspondence related to this solicitation.

2.1 Errors, Omissions or Ambiguities

If a Quoter believes the solicitation, including the instructions to Quoters, contains an error, omission or ambiguity, or is otherwise unsound, the Quoter shall immediately notify the Contracting Officer in writing with supporting rationale.

2.2 False Statements in Offers

Quoters must provide full, accurate and complete information as required by this solicitation and its attachments. The penalty for making false statements in offers is prescribed in 18 U.S.C. 1001.

2.3 Authorized Personnel

The Quoter shall provide the name, title, address, e-mail, and phone number of the company representative(s) who can obligate the Quoter contractually. Also, the Quoter shall identify the individual(s) authorized to negotiate with the Government by providing the name, title, address, e-mail, and phone number of the individual(s).

2.4 No Prior Knowledge

Quoters shall assume the Government has no prior knowledge of their experience and will base its evaluation on the information presented in the Quoter's Quotation.

2.5 Confidential or Proprietary Information

In the event a Quoter is concerned that information submitted in response to this solicitation contains confidential financial and proprietary information, including trade secrets, then the information must be clearly marked. In the event a Quoter considers specific information to be confidential, they shall provide a written declaration to the Contracting Officer containing the supporting rationale for their contention that the information constitutes an exception to release under Federal Law. The Quotation shall clearly demonstrate the Quoter's understanding of the overall and specific requirements of the Statement of Work (SOW); convey the Quoter's capabilities for transforming their understanding into accomplishments for performing the requirements.

2.6 Quotation Preparation Costs

The Government will not pay any costs incurred by any Quoter in the preparation and submission of a Quotation in response to this RFQ.

2.7 Quotation Validity Period

Quotations shall be valid for a minimum of one hundred twenty (120) days.

3 ADVISORY DOWN-SELECTION NOTIFICATION

After the Government completes evaluation of Criteria 1, 2, and 3, Quoters will receive an advisory notification via e-mail from the Contracting Officer. This notification will advise the Quoter of the Government's advisory recommendation to proceed or not to proceed with Phase II submission. Quoters who are rated most highly for criteria 1, 2, and 3 will be advised to proceed to Phase II of the quote submission process. Quoters who were not among the most highly rated

will be advised that they are unlikely to be viable competitors, along with the general basis for the Government's advisory recommendation. The intent of this advice is to minimize quote development costs for those Quoters with little to no chance of receiving an award. Quoters should note that Phase I evaluation criteria are more important than Phase II evaluation criteria.

The down-select notifications will include information regarding the submission due date and time of Phase II quotation submission. The Government intends to provide appropriate lead time for quoters to decide whether it wishes to proceed with a Phase II submission

The Government anticipates providing no more than 8 Quoters with an advisory notification to proceed. However, the Government's advice will be a recommendation only, and those Quoters who are advised not to proceed may elect to continue their participation in the procurement.

Failure to participate in Phase I of the procurement precludes further consideration of a Quoter. Phase II submissions will not be accepted from Quoters who have not submitted Phase I quotes by the due date and time stated in this solicitation. For those Quoters that are rated most highly and advised to proceed to Phase II of the quote submission process, the Contracting Officer will include the Phase II submission instructions in the advisory notification, including the date, time and exact location of the Quoter's scheduled oral presentation, as well as the due date for the written portion (Price) of the Phase II submission. The Government recommends Quoters to begin preparation of Phase II quotations only after receipt of the Phase 1 advisory down-select notice.

4 QUESTIONS AND AMENDMENTS

All questions regarding this RFQ shall be submitted uploaded to the GSA eBuy portal and submitted via email to efsi-si@hq.dhs.gov. **Questions are due no later than 12:00 p.m. on November 8, 2019.**

Questions asked via telephone or voicemail will not be accepted and will not be addressed in any amendments to the RFQ.

The Government recommends that the Quoter ensures that questions are written to enable a clear understanding as to the Quoter's issues or concerns with the referenced area of the solicitation. Statements expressing opinions, sentiments, or conjectures are not considered valid inquiries or comments for this purpose and will not receive a response from the Government.

Answers to questions will be provided to all prospective Quoters, giving due regard to the proper protection of proprietary information. To receive responses to questions, Quoters shall cite, at a minimum, the section, paragraph, number, and page number in the format shown below. Further, Quoters are reminded that DHS will not address hypothetical questions aimed toward receiving a potential "evaluation decision" from DHS.

When submitting questions and comments, please refer to the specific text of the RFQ in the following format:

Email "subject line" shall read:

RFQ No.: **70RDAD19Q00000101** – Questions Submitted (Contractor Name)

Questions ***shall be*** submitted in a Microsoft Excel (2003 or later version when available) file in the following format:

	Solicitation or Attachments RFQ Section	Paragraph No.	Page No.(s)	Question Category (Contract or Technical)	Question
1					
2					

If a question reflects a change in a solicitation document, that document may be updated directly; however, any other government response to a question is provided as a courtesy only and does not change or amend anything further. DHS will not attribute any question(s) asked to the submitting Quoter(s).

If Amendments to the solicitation are issued, all Quoters must acknowledge the Amendments by signing the accompanying Standard Form 30 and returning the signed Standard Form 30 for all Amendments issued with the Quoter's Quotation submission. Failure to acknowledge all Amendments issued by the Government may result in the Quotation submitted in response to the solicitation being found non-responsive by the Government.

5 QUOTATION CONTENT AND SUBMISSION INSTRUCTIONS

4.1 Quotation Submission Due Date

Responses for the written Quotation submission of this solicitation shall be received no later than **12:00 p.m. on November 26, 2019** to efsi-si@hq.dhs.gov.

4.2 Quotation Submission Content

Each Quoter shall submit a quotation, which consists of two (2) electronic volumes, as described below:

Naming Convention	Tab Title	Phase
Volume I - Technical		
Tab A	Volume 1 Quotation Cover Letter (limit 3 pages)	1
Tab B	Demonstrated Prior Experience & Reference Checks (10 pages)	1
Tab C	Technical Understanding & Capabilities (15 pages)	1
Tab D	Management Approach (10 pages)	1
Volume II – Business & Pricing		

Tab A	Volume II Quotation Cover letter; SF18 "Request for Quotation"; SF30 "Amendment(s)" if any; GSA Pricing Schedule; FAR Clause 52.209-2 (C) *Disclosure*	2
Tab B	Completed Pricing Template– Attachment 1	2
Tab C	GSA Teaming Arrangement, if applicable	2

Information contained in each volume shall be complete to the extent that evaluation of one volume may be accomplished independently of, and concurrently with, evaluation of the other.

NO PRICE INFORMATION IS TO BE INCLUDED IN VOLUME 1

Volume 1 – Technical Quotation – Phase 1

Tab A: Quotation Cover Letter

Quoters' submission of the Quotation Cover Letter shall include the following information:

a) Dun & Bradstreet Number (DUNS)
b) Contact Name
c) Contact email address
d) Contact Telephone Number
e) Complete business mailing address
f) GSA IT Schedule 70 Contract Number

Tab B: Demonstrated Prior Experience & Reference Checks (Evaluation Criterion 1)

The Quoter shall describe demonstrated prior experience from two (and no more than four) contracts/task orders performed within the last five (5) years, which shall include at least one instance of demonstrated prior experience from the Prime Contractor's Subcontractor (if any) in implementing enterprise-wide information technology systems for financial management, procurement management and contract writing, and asset valuation/management within an organization of a similar scale and complexity as the Department of Homeland Security or one of the Department's components. These experiences must: 1) demonstrate management and coordination of multiple support teams and subcontractor relationships that resulted in achieving quality performance under contracts/orders that were of a comparable size, scope and complexity to the requirement described in this solicitation; 2) demonstrate the Quoter's experience in transitioning Government financial systems comparable in size, scope and complexity to the requirement described in this solicitation, and where different sub-units were transitioned at different times over a multi-year period; and 3) provide evidence of the Quoter's demonstrated prior experience integrating and supporting financial, asset valuation/management, and procurement and contract writing software suites.

Comparability of size, scope and complexity will be in relation to the DHS financial system modernization requirement as documented in Section II.

If demonstrated prior experience of Subcontractors is submitted, the Quoter must clearly identify the owner of the demonstrated prior experience and submit a letter of commitment to team with the Prime Quoter signed by an individual of the Subcontractor's firm authorized to make such a commitment and on the subcontractor's letterhead, that confirms a Subcontracting agreement is in place and that explains the role of the Subcontractor for the current DHS requirement. These letters of commitment from the Subcontractor's shall not count against the page limitation. Additionally, the Government will evaluate most favorably examples of Subcontractor demonstrated prior experience where the Prime Quoter and the Subcontractor performed together/previously teamed.

For each example of prior experience provided, the Quoter shall, at a minimum, document:

- Name of project, duration, and dollar value.
- Government Agency or Company for whom work was performed and a name, title, e-mail and phone number for a representative of that client agency or company that can attest to the work performed.
- Brief description of project (sufficient to establish relevance of experience to the DHS requirement), and role of Prime or Subcontractor which clearly identifies the level and type of services performed under the contract, and the role of the Prime or Subcontractor in performing the work.
- Point of Contact from the Government entity (name, title, current phone number, and current e-mail) familiar with the project and can confirm level and quality of the Quoters referenced prior experience and work. The Government reserves the right to communicate with the Point of Contact provided.
- A discussion of the aspects of the prior experience project that are similar to the DHS need as reflected by this BPA's work scope, as well as aspects that are not similar.

The Quoter is permitted to submit on-going projects as demonstrated prior experience if 12 months of performance, at a minimum, under the on-going contract has been completed and if the Quoter clearly describes the stage that the project is at/what has been completed under performance to date.

The Government may contact the identified representative of the Government agency or company as part of the reference checks to confirm the level and quality of this demonstrated prior experience.

Tab C: Technical Understanding and Capabilities (Evaluation Criterion 2)

The quoter shall 1) demonstrate their knowledge, understanding and capabilities of meeting the requirements in the BPA SOW; and 2) describe their proposed strategy and methods for conducting discovery, systems integration, service transition, operations and maintenance, and training services.

Tab D: Management Approach (Evaluation Criterion 3)

The quoter's Management Approach shall describe the quoter's: 1) qualifications and certifications of the quoter's proposed Key Personnel; 2) proposed use of corporate resources in effective management of the work efforts under the BPA; and 3) comprehensive, sound and reasonable approach to managing the requirements as described in the SOW and the RFQ.

6 ORAL PRESENTATIONS

The order in which Quoters are scheduled for oral presentations will be randomly selected by the Government. The oral presentation will be held in-person in the Washington, DC metropolitan area. Travel costs for the oral presentation will not be reimbursed.

6.1 Oral Presentation Format

The oral presentation is intended to provide the opportunity for the Quoter to detail its proposed approach to meet or exceed the requirements of the solicitation. The oral presentation shall not provide the Quoter any opportunity to revise or change any of the previously provided written Quotation documentation and is therefore not construed to be discussions with the Quoter.

The Government intends for the oral presentation to proceed as follows:

Oral Presentation Portion	Oral Presentation Component	Maximum Time Allotment: 3 Hours (does not include Portion 1)
1	Introduction and Oral Presentation Process and Expectations.	Not specified
2	The Quoter shall present its proposed solution.	Up to 90 minutes
3	The Government shall caucus among themselves prior to interactive dialogue. Quoters shall receive a break.	Up to 30 minutes
4	The Government and Quoter will participate in an interactive dialogue related to the information presented by the Quoter during the oral presentation. The Government may ask a standard set of on-the-spot scenario-based questions of Quoters as well. The Quoter will respond to the Government's questions.	Up to 60 minutes

Exchanges during Oral Presentation: The Government intends for the oral presentation to be an interactive dialogue between the Quoter and the Government. These exchanges are viewed as a component of the oral presentation itself and do not constitute discussions.

Quoters can expect the presentation will be conducted in a conference room with a table of sufficient size to accommodate the participants, including the Government attendees.

The Quoter Participants shall not reach back, by telephone, e-mail or any other means, to any other personnel or persons for assistance during the oral presentation. There will not be internet or WIFI access during the oral presentation.

6.2 Oral Presentation Procedures (Prepared PowerPoint Slide Presentation (30 slides maximum)

The Quoter may submit a .PDF file of up to 15 PowerPoint slides which the Quoter intends to present during its scheduled oral presentation. Presentation slides will be due at 12:00 pm one day prior to the commencement of scheduled Oral Presentations. The due date will be included in the advisory down-select notification. The presentation slides will not be evaluated, as the evaluation will be based on the oral presentation. The presentation slides are intended solely to help the evaluators follow the Quoter's oral presentation. Advance submission of the PowerPoint slides is solely to protect the integrity of maintaining equal submission development time for all Quoters regardless of the scheduled date for oral presentations.

The Government reserves the right to record the oral presentation. Additionally, the Government reserves the right to include aspects of the Quoter's oral presentation as special terms and conditions to any resultant task order.

6.3 Quoter Participants

The Quoter's participants in the oral presentations shall be limited to the Quoters proposed BPA Manager, up to three (3) of the Quoter's additional personnel, and one (1) responsible corporate official. Thus, the Quoter may have no more than 5 participants attend oral presentations. Participants in the oral presentation are limited to personnel of the Prime Quoter and any subcontractors/ teaming partners.

Quoters shall provide the name and e-mail of the Quoter Participants for the oral presentation via email to Contracting Officer and Contract Specialist not less than 24 hours prior to their scheduled date of their Oral Presentation.

6.4 Oral Presentation Content

The Quoter shall prepare and present an oral presentation which shall address the Quoters approach to the task areas identified below. During oral presentations, the Government may also ask Quoters a standard set of on-the-spot technical and management questions.

6.4.1 Technical

The Quoter shall describe the following technical elements:

a) their approach to requirements management with their implementation and verification;

b) approach to configuration management and deployment;

c) approach for business process re-engineering, organizational change management, and training;

d) performing quality management and testing;

e) approach for data migration; and

f) approach for performing: software patching and upgrades; system configuration, testing and deployment; and information technology refreshment

6.4.2 Management

The Quoter shall describe the following management elements:

a) approach timely staffing and management of orders under this BPA addressing the following ensuring sufficient experienced personnel, who have both technical and domain expertise, are recruited, on-boarded, and retained by the Quoter throughout the duration of order period(s) of performance;
b) approach and ability to perform Earned Value Management according to Statement of Work requirements; and
c) approach for risk management and mitigation.

7 Volume II – Price Quotation

There are no page limitations associated with Volume II – Price Quotation

Quoters shall prepare a Price Quotation that contains all information necessary to evaluate the prices and/or discounts proposed by the Quoter. Quoters shall only provide pricing for the Special Item Numbers (SINs) available on their GSA MAS 70 schedule. If the service is not available under their respective schedule contract, the Quoter shall not provide pricing for the service. Alternatively, the Government will not evaluate an open market item or service that is not available on the Quoters MAS 70 schedule. The Price Quotation shall consist of fully burdened hourly rates with discounts.

The Price Volume shall be clearly organized and presented to allow an evaluation by the Government. A Quoter's quotation is presumed to represent the Quoter's best efforts to respond to the RFQ. Furthermore, the services priced in the price volume must be consistent with the services that are described in other volumes of the Quotation. Inconsistency, if unexplained, raises a fundamental issue regarding the Quoter's understanding of the RFQ, as well as of the Quoter's ability to meet the requirements of the RFQ.

Quoters shall follow the Price Template at Attachment 1 for purposes of submitting pricing data. Quoters are to propose labor categories from the Quoter's awarded GSA schedule contract and may substitute if the RFQ labor category position title is different from the Quoter's awarded GSA position title. If a substitute labor category is proposed, Quoters shall map all substitutions

to the RFQ labor category positions. Quoters shall include the following information in the cover letter of its price Quotation:

Tab A: Quotation Cover Letter

Quoters shall include a Quotation Cover Letter, signed copy of the Standard Form (SF) 18 "Request for Quotation"; signed copies of the SF30, if applicable, a copy of the Quoter's GSA MAS 70 schedule/Pricing Schedule in this section, and disclosures.

Tab B: Pricing Template (Attachment 1)

The Quoter is required to submit pricing data in the format indicated in Attachment 1 - Pricing Template of the RFQ. Attachment 1 – Pricing Template shall identify the Quoter's proposed labor categories, labor rates, and provide a total proposed price for the pricing scenario contained within the attachment at worksheet. The pricing scenario is for evaluation purposes only. The labor rates quoted under Labor Rates will be the BPA Award rates.

DHS may choose not to enter into a Blanket Purchase Agreement with Quoters whose prices are not competitive, or which offer no discount or reduction for services off the negotiated GSA schedule rates. Price discounts or reductions must be clearly identified and are strongly encouraged. The Quoter is encouraged to provide discounts to its GSA MAS 70 Schedule labor rates. The discounted labor rates will apply to the BPA and respective task order(s).

Tab C: Contractor Teaming Arrangements (CTAs) or GSA Prime Contractors/Subcontractors

I. Quoters may structure their quotation packages as either a GSA MAS Contractor Team Arrangement (CTA) or as a GSA Prime Contractor/Subcontractor arrangement, whichever approach it believes provides the best value solution to DHS. Further guidance on GSA CTAs may be found at the GSA MAS Desk Reference Section 10, Contractor Team Arrangements (CTAs)

II. If a GSA CTA is proposed, the Quoter is to specifically identify it as such and submit the CTA supporting documentation to DHS as part of its quotation package. The CTA must identify and designate the Team Leader, all Team Members, their corresponding GSA Schedule Contract Number(s), and describe the services to be performed by the Team Leader and each Team Member, along with the associated proposed fixed labor rate. Each quotation submitted as a CTA must include adequate technical/management information for DHS to reasonably evaluate the merits of the submission. Each quotation submitted as a CTA shall describe the Team Leader and Team Member responsibilities in terms of receiving task orders under the BPAs, invoicing and payment. If choosing this approach, please fill in:

- The GSA Contractor Team Leader is:
- The GSA Contractor Team Leader GSA Contract Number is:

- The GSA Team Member is:

- The GSA Team Member 1 GSA Contract Number is:

- The GSA Team Member 2 is:
- The GSA Team Member 2 GSA Contract Number is:

Quoters may add more Team Members if/as necessary.

III. If a GSA Prime Contractor/Subcontractor Arrangement(s) is proposed, only the Prime Contractor must have a GSA MAS 70 Schedule contract. GSA authorized subcontractors may fulfill requirements under the Prime Contractor's GSA schedule and pricing table quoted in Attachment 1. The Prime may not delegate responsibility for performance to subcontractors. The Prime cannot contract to offer services for which it does not hold a Schedule contract.

7.1 Assumptions, Conditions and Exceptions

The Quoter shall submit all assumptions, conditions and exceptions to any of the terms and conditions of this solicitation in the pricing section. If not noted in the Quotation, it will be assumed that the Quoter proposes no assumptions for award and agrees to comply with all the terms and conditions as set forth herein. It is not the responsibility of the Government to seek out and identify assumptions, conditions or exceptions buried within the Quoter's Quotation.

Each assumption, exception or dependency shall be specifically related to a paragraph and/or specific section of the RFQ or associated clearly with an aspect of the pricing proposed. The Quoter shall provide a rationale in support of any noted assumption, exception or dependency, explaining its effect in comparison to the RFQ. This information shall be provided in the format with content as outlined in the table below and is to be included in the price volume.

RFQ Section/Document	Paragraph/Page	Requirement/Portion and Assumption, Condition or Exception	Rationale
RFQ, Schedule, Attachment	Applicable paragraph and/or page number(s)	Identify the requirement or portion to which an assumption, exception or dependency is being taken and detail the assumption, condition or exception	Justify why the requirement will not be met, the rationale for the assumption, condition or exception, and/or discuss reasons why not meeting the Government's terms and conditions might be advantageous to the Government.

Assumptions, exceptions or dependencies do not make a Quotation automatically unacceptable but will be considered as part of the evaluation of the Quoter's price as it relates to the Quoter's overall proposed solution.

SECTION IV - EVALUATION CRITERIA FOR AWARD

(This section will be removed upon award)

1 INTRODUCTION

This GSA Schedule BPA Request for Quotation seeks to obtain system integration support services for DHS Office of the Chief Financial Officer. DHS intends to acquire these services by establishing more than one competitive BPA awards to GSA MAS 70 holders. DHS reserves the right to increase or decrease the number of BPAs it establishes based upon the results of the evaluation**.**

2 BASIS FOR AWARD – BLANKET PURCHASE AGREEMENT

The basis for award will be best value in accordance with FAR 8.405-3. Evaluation will be conducted, and selection will be made in accordance with the guidelines provided in the Federal Acquisition Regulation (FAR), Homeland Security Acquisition Regulation (HSAR), Homeland Security Acquisition Manual (HSAM), and this RFQ. Awards will be made to the responsible Quoters submitting an overall quote that is determined most advantageous to the Government, price and non-price criteria considered. BPA(s) will be established with the firm(s) whose quotation(s) meets the Government's requirements and whose technical evaluation and price represents the best value to the Government, using the tradeoff process.

This method does not use any aspects of FAR subpart 15.3. The use of this process does not obligate the Government to determine a competitive range, conduct discussions with any Quoters, solicit Quotations or revisions thereto, or use any other source selection techniques associated with FAR subpart 15.3.

2.1 Comparative Analysis

Following receipt of responses (including oral presentations), and completion of evaluation of each eligible individual Quoter’s response, the Government may perform a comparative analysis (comparing Quoter responses to one another) to select the Quoter(s) that are best suited to fulfill the requirements, based on the Quoters’ responses to the criteria outlined in this RFQ and their relative importance.

2.2 Award on Initial Responses

The Government anticipates selecting the best-suited Quoters from initial responses, without engaging in exchanges with Quoters. Quoters are strongly encouraged to submit their best technical solutions and price in response to this RFQ.

Once the Government determines the quoter that is the best-suited (i.e., the apparent successful quoter), the Government reserves the right to communicate with only that quoter to address any remaining issues, if necessary, and finalize an agreement with that quoter. These issues may include technical and price. If the parties cannot successfully address any remaining issues, as determined pertinent at the sole discretion of the Government, the Government reserves the right

to communicate with the next best-suited quoter based on the original analysis and address any remaining issues. Once the Government has begun communications with the next best-suited quoter, no further communications with the previous quoter will be entertained until after the task order has been awarded. This process shall continue until an agreement is successfully reached and an agreement is established.

2.3 Evaluation Criteria

The Government will evaluate each quotation using the following evaluation criteria listed below:

- Phase 1
  - Criterion 1: Demonstrated Prior Experience and Reference Checks;
  - Criterion 2: Technical Understanding and Capabilities; and
  - Criterion 3: Management Approach

- Phase 2

  - Criterion 4: Oral Presentation, and
  - Criterion 5: Price (Volume II) including discount terms. (Not rated)

The evaluation criteria are listed in descending order of importance. All non-price evaluation criteria, when combined, are significantly more important than price. As the non-price merits of competing Quoter's Quotations approach equal, Price may become more important in the best value tradeoff decision.

Phase 1 – Criterion 1 – Demonstrated Prior Experience & Reference Checks

The Government will evaluate the Quoter's demonstrated prior experience and reference checks to determine its confidence that the quoter will successfully perform the work.

Phase 1 – Criterion 2 – Technical Understanding and Capabilities

The Government will evaluate the Quoter's technical understanding and capabilities to determine its confidence that the quoter will successfully perform the work.

Phase 1 – Criterion 3 –Management Approach

The Government will evaluate the Quoter's Management Approach to determine its confidence that the quoter will successfully perform the work.

Phase 2 – Criterion 4 – Oral Presentations

Through the Oral Presentations, the Government intends to understand the Offeror's proposed solution and its capabilities as it relates to the Government's requirements. The Government will assess the quality, and based on the levels of quality, a confidence rating will be assigned. Further, the Oral Presentations will be used as an opportunity to assess the viability of an Offeror

to successfully deliver its proposed solution, by evaluating the responses to the advanced questions, on-the-spot questions, and interactive dialogue.

The Government will evaluate the oral presentation, not the slides – the slides are merely an aid to the oral presentation. However, inconsistencies between the oral presentation and the slides will be a basis for a lowered confidence.

2.4 Evaluation Ratings

In its evaluation of the non-price criteria, the Government will consider the benefits and risks associated with the Quoter's proposed approaches to arrive at a confidence assessment of the Quoter's likelihood of successfully performing the work and meeting the requirements of the solicitation. The table below shows the ratings the Government will assign in its evaluation of these criteria.

Ratings for Criteria 1, 2 3 and 4	
Rating	Definition
High Confidence	The Government has high confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with little or no Government intervention.
Some Confidence	The Government has some confidence that the Quoter understands the requirement, proposes a sound approach, and will be successful in performing the contract with some Government intervention.
Low Confidence	The Government has low confidence that the Quoter understands the requirement, proposes a sound approach, or will be successful in performing the contract even with Government intervention.

2.5 Phase 2 – Criterion 5 - Price (Volume II) including Discount Terms (Not Rated)

Each price quotation will be evaluated to include the labor rates the Quoter provides in Attachment 1 – BPA Pricing Template. The evaluation will assess the accuracy, completeness, discounts offered and reasonableness. This process involves verification that prices and/or discounts are included for all RFQ requirements, figures are correctly calculated, and prices are presented in an adequate format.

ATTACHMENTS

Attachment 1:	BPA Pricing Template
Attachment 2:	Glossary of Terms