REQUEST FOR QUOTATION (RFQ)

HSHQDC-17-Q-00231 Amendment 00002

for

ELECTRONIC CONTRACT FILING SYSTEM

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

U.S. Department of Homeland Security
Washington, DC 20528

August 2, 2017

Dear GSA Contractors:

The Department of Homeland Security (DHS) is pleased to present this Amended Request for Quote (RFQ) 00002 for the Electronic Contract File System (ECFS) for the Office of the Chief Procurement Officer (OCPO) and the DHS community. This competition is being conducted under Federal Acquisition Regulation Part 8.4 Federal Supply Schedules using GSA Information Technology Schedule 70, SIN 132 33 Perpetual Software Licenses, and will result in a single-award Blanket Purchase Agreement.

Questions shall be submitted via email to Contract Specialist Michael Lipperini and Contracting Officer Randy Dreyer utilizing email address: DHS.ECFS@hq.dhs.gov. Questions are due no later than 1:00 PM, Eastern Time, Wednesday, July 5, 2017.

The Government is utilizing a three-phased approach for this RFQ. Phase 1 Quotes in response to this RFQ shall be submitted via email to Contract Specialist Michael Lipperini and Contracting Officer Randy Dreyer utilizing email address: DHS.ECFS@hq.dhs.gov. Phase 1 Quote submissions are due by 1:00 PM, Eastern Time, Tuesday, July 11, 2017. Subsequent quote procedures are in Section 4: Instructions to Quoters.

Sincerely,

/s/

Randy Dreyer
Contracting Officer
Information Technology Acquisition Center
Office of Procurement Operations

RFQ Appendix A – Requirements Identification Matrix
RFQ Appendix B – Contract Checklists
RFQ Attachment 1 – Capability Confirmation Checklist
RFQ Attachment 2 – Past Performance Information Form
RFQ Attachment 3 – Labor Category Descriptions and Qualifications
RFQ Attachment 4 – Pricing Workbook
RFQ Attachment 5 – ECFS Quoter Questions and Responses

1. BLANKET PURCHASE AGREEMENT (BPA)

1.1 Blanket Purchase Agreement

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) to support the U.S. Department of Homeland Security (DHS) Office of the Chief Procurement Officer (OCPO). The intent is to acquire an Electronic Contract Filing System (ECFS) utilizing a Software as a Service (SaaS) licensing and delivery model through the General Services Administration (GSA) Federal Supply Schedule (FSS) 70, Information Technology. The following Special Item Number (SIN) applicable to the Contractor's GSA FSS contract shall be included in the BPA:

132 33 Perpetual Software Licenses

Note: The terms Quoter, Contractor, and BPA Holder are used interchangeably in this agreement.

Signatures:

DHS Office of Procurement Operations (OPO) BPA Contracting Officer

Printed Name	OPO Title	Signature	Date

Contractor

Printed Name	Company Title	Signature	Date

2. BPA TERMS AND CONDITIONS

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 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. The BPA Pricing Schedule shall include all supplies and services included in the scope of this BPA, with the proposed discounts applied. With the exception of labor hour rates, prices shall not escalate and are not subject to upward adjustment during the term of the BPA. All Orders are subject to the terms and conditions of the underlying GSA contract and to the additional terms and conditions provided within this Blanket Purchase Agreement.

2.1 Scope of Services

The following supplies and services can be ordered under this BPA:

Perpetual Software Licenses, Program Management, System Design and Configuration, Testing, Certification and Accreditation, Training, Help Desk Support, Cloud Hosting, and Operations and Maintenance.

2.2 Types of Orders

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

2.3 BPA Volume

The Government estimates, but does not guarantee that the volume of purchases under the BPA will be approximately $9.7 million over base and four one-year options. The Government is obligated only to the extent of authorized purchases actually made under this BPA. There is no minimum order guarantee.

2.4 Obligation

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

2.5 Referenced Federal Acquisition Regulation (FAR) and Homeland Security Acquisition Regulation (HSAR) Clauses/Provisions

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

A. CONTRACT CLAUSES INCORPORATED BY REFERENCE

52.252-2 Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):
FAR: http://farsite.hill.af.mil/vffara.htm
HSAR: 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
52.204-2	Security Requirements	Aug 1996
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.209-10	Prohibition on Contracting With Inverted Domestic Corporations	Nov 2015
52.212-4	Contract Terms and Conditions—Commercial Items—Alternate I	Jan 2017
52.222-50	Combating Trafficking in Persons	Mar 2015
52.224-2	Privacy Act	Apr 1984
Homeland Security Acquisition Regulation (HSAR) Clauses / Provisions		
Clause	**Title**	**Date**
3052-205-70	Advertisements, Publicizing Awards, And Releases	Sep 2012
3052.242-72	Contracting Officer's Technical Representative	Dec 2003

B. FAR CLAUSES INCORPORATED IN FULL TEXT

52.204-21 Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)

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

"Covered contractor information system" means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

"Federal contract information" means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

"Safeguarding" means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) *Other requirements*. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) *Subcontracts*. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

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

(a) The Government may extend the term of this contract by written notice to the Contractor within **thirty (30) days**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **sixty (60) days** before the contract expires. The preliminary notice does not commit the Government to an extension.

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed **60 months**.

(End of Clause)

C. HSAR CLAUSES INCORPORATED IN FULL TEXT

HSAR 3052-204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

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

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

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

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

(End of clause)

HSAR 3052.209-70 Prohibition on Contracts with Corporate Expatriates (Jun 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section

1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan deemed in certain cases*. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain transfers disregarded*. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special rule for related partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that [Check one]:

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(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 is **unequal access to information (potential access and visibility of DHS OCPO contract records). Offerors may gain access to non-public Government information that would provide an unfair competitive advantage under DHS solicitation(s).**

(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.

(End of provision)

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 is **unequal access to information (potential access and visibility of DHS OCPO contract records). Offerors may gain access to non-public Government information that would provide an unfair competitive advantage under DHS solicitation(s).**.

(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, 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.

Key Personnel or Facilities under this BPA:

- Project Manager (BPA Level)
- 1102 Subject Matter Expert
- Other Key Personnel as specified at the individual Order(s)

(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)

2.6 BPA Term

This BPA shall consist of one (1) base period and four (4) option periods as shown below. Orders may have a Period of Performance of twelve (12) months from the last day of Option Period Four of this BPA.

BPA Period	Ordering Period
Base Period	12 months
Option Period One	12 months
Option Period Two	12 months
Option Period Three	12 months
Option Period Four	12 months

This BPA expires at the end of Option Period Four 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 sixty (60) months. Orders may be placed against this BPA on or before the last day of Option Period Four if the option is exercised.

The BPA Holder is to possess a period of performance sufficient to provide the Government with a continuous sixty (60) month period of performance for the BPA. Quoters may be awarded BPAs that extend beyond the current term of their GSA Schedule contract, so long as there are option periods in their GSA Schedule contract that, if exercised, will cover the BPA's period of performance. 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.

2.7 Ordering Officers

DHS Warranted Contracting Officers.

2.8 Orders

Orders will be placed against this BPA by DHS Contracting Activities in accordance with the Ordering Procedures in Section 2.19.

2.9 Award of Orders under the BPA

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

1. BPA and 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, contract type, quantity, unit price and extended price;
8. The security requirements;
9. The payment schedule; and
10. Accounting and appropriation data.

2.10 Order Period of Performance

The period of performance will be designated at the Order level. Orders may be issued at any time during the period of performance. Orders for supplies and services shall be priced using the pricing table specified in the BPA applicable to the Order’s anticipated period of performance. Periods of Performance for orders for supplies or services issued in the final year of the BPA shall not extend beyond 12 months after the BPA’s ordering period end date. The period of performance for each order shall be consistent with the funding appropriation being obligated.

2.11 Invoicing

Invoicing procedures will be specified in each individual Order. The "remit to" address to which payment must be sent is applicable at the 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 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 supplies or services;
(v) Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.

2.12 Order of Precedence

The terms and conditions apply to all 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 GSA FSS contract, the federal supply schedule contract shall take precedence.

2.13 Place of Performance

The primary place of performance will be the Contractor's facilities with frequent visits to Department of Homeland Security in Washington, DC. The place of performance will be specified at the Order level.

2.14 Travel

Contractor travel may be required to support this requirement. All travel required by the Government outside the local commuting area(s) will be reimbursed to the Contractor in accordance with FAR 31.205-46 -- Travel Costs. The Contractor shall be responsible for obtaining COR approval (electronic mail is acceptable) for all reimbursable travel in advance of each travel event. Travel requirements will be specified at the Order level.

2.15 Security Considerations

Contractor access to unclassified, but Security Sensitive Information may be required under this BPA. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination. Security requirements will be specified at the Order level.

2.16 Hours of Operation

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

2.17 Post Award Conference

The Contractor shall attend a Post-Award Conference with the BPA Contracting Officer and the Contracting Officer's Representative (COR) no later than ten (10) business days after the date of award. The purpose of the Post-Award Conference, which will be chaired by the Contracting Officer, 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 Contracting Officer.

Post award conferences at the Order level shall be held at the discretion of the Order Contracting Officer (OCO) awarding the Order if that OCO determines one to be necessary.

2.18 Past Performance

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

2.19 Ordering Procedures

2.19.1 General

The DHS Order Contracting Officer (OCO) will award and administer Orders in accordance with the ordering procedures set forth in the BPA and the procedures outlined in FAR 8.405-3(c) -- Ordering from BPAs.

2.19.2 Order Request for Quotation (RFQ)

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

The Order Request for Quote (RFQ) will be in writing (via mail, e-mail, or fax) and include a description of the required supplies or services, the evaluation or review criteria, and the evaluation or review procedure. The evaluation or review will be based on technical factors such as, but not limited to, technical capabilities, management approach, past performance, and price.

The BPA Holder shall submit a quotation in accordance with the OCO's RFQ instructions. The information that the OCO 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 an Order quote.

2.20 Commencing Work

The BPA Holder shall not commence work until authorized by the OCO. This BPA does not obligate any funds. The Government is obligated only to the extent of authorized purchases by orders issued under this BPA.

2.21 Annual Review of the BPA

In accordance with FAR 8.405-3(e), the Department of Homeland Security, Office of Procurement Operations which has established this BPA will conduct an annual review to determine whether the schedule contract, upon which the BPA was established, is still in effect, the BPA still represents the best value, and 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.

2.22 BPA Administration

The Contracting Officer (CO) for this BPA is identified below:

Name:	Randy Dreyer
Agency:	Office of Procurement Operations (OPO) Department of Homeland Security (DHS)
Address:	
Voice:	
Email:	

The Contract Specialist (CS) for this BPA is identified below:

Name:	Michael Lipperini
Agency:	Office of Procurement Operations (OPO) Department of Homeland Security (DHS)
Address:	
Voice:	
Email:	

Contracting Officer's Representative (COR):

Name:	Brian Wilson
Agency:	Office of Chief Procurement Officer (OCPO) Department of Homeland Security (DHS)
Address:	
Voice:	
Email:	

3. STATEMENT OF WORK
ELECTRONIC CONTRACT FILING SYSTEM (ECFS)
July 7, 2017

3.1 BACKGROUND

The Department of Homeland Security (DHS) seeks to implement an Electronic Contract Filing System (ECFS) utilizing Software as a Service (SaaS) on an authorized FedRAMP cloud hosted environment on an unclassified network. DHS requires an electronic Commercial-Off-The-Shelf (COTS) solution to support electronic contract file storage, workflow, document management, and records management. The Office of the Chief Procurement Officer (OCPO) Oversight and Strategic Support (OSS) Acquisition Systems Branch (ASB) is overseeing the ECFS effort.

DHS OCPO supports eight Heads of Contracting Activity (HCA) located within the Components of DHS. These HCAs are located within Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), Immigration Customs Enforcement (ICE), Office of Procurement Operations (OPO), Transportation Security Administration (TSA), United States Coast Guard (USCG), and United States Secret Service (USSS). Procurement office locations are dispersed across the United States.

There are approximately 1,321 total contracting officers and contract specialists. In addition, there are approximately 600 support personnel across the contracting activities that may also access an electronic contract filing solution. The total number of personnel fluctuates due to employee turnover. The table below shows the estimated number of contracting officers and contract specialists (also referred to as “1102s”) by component

Contracting Activity	**Estimated Number of 1102s**
CBP	159
FEMA	162
FLETC	46
ICE	144
OPO	263
TSA	129
USCG	390

USSS	28
Total	1,321

DHS estimates that the total number of users on this system could be as high as 2000 once it is implemented to all users. Initially, DHS intends to implement the solution via a Pilot Program for a small group of users with representation from all of the Contracting Activities.

The following chart illustrates the average number of new contracts created each year by contracting activity. This number was derived by taking the average from the total number of new awards, including Interagency Agreements (IAA) and Grants, for the past five years. It is estimated that each contract file will require on average 42 MB of storage space.

Contracting Activity	**Average new procurement actions per year.**
CBP	4,806
FEMA	4,548
FLETC	1,591
ICE	2,021
OPO	3,780
TSA	979
USCG	21,590
USSS	1,013
Total DHS	40,328

DHS currently uses a combination of paper-based and electronic contract files to manage and process contracts throughout their lifecycle. The use of paper based processes hampers the OCPO mission because staff does not have easy access to documents required to perform their work. Furthermore, as the Department embraces remote working trends, disaster preparedness, and improved operations, paper based processes do not allow the contracting staff to fully work on files that cannot be accessed remotely.

3.2 SCOPE OF WORK

The scope of this contract includes planning, requirements definition, configuration, testing, certification and accreditation, training, help desk, implementation, software, cloud hosting, and operations and maintenance of an Electronic Contract Filing System for DHS. The solution shall include at a minimum:

- a configuration/testing environment
- a staging/pre-production environment
- a production environment with disaster recovery capability that complies with DHS standards

The solution shall be implemented using a three (3) phase approach:

- Configuration/Testing/Accreditation
- Pilot
- Full Implementation

3.3 OBJECTIVE

The objective of this Blanket Purchase Agreement (BPA) is to procure, implement, operate, and maintain an Electronic Contract Filing System that will support the DHS acquisition community.

3.4 REQUIREMENTS/TASKS

The Contractor shall provide all supplies and services as set forth in the areas below:

3.4.1 PROJECT MANAGEMENT

CPO requires expert project management skills and abilities to seamlessly manage and oversee tasks and functions involved with delivering the full range of capabilities throughout all phases of the Electronic Contract Filing System.

The Contractor shall:

a) Deliver a Project Management Plan to include but not limited: identification of detailed tasks, task durations, implementation approach (to include Pilot phase), and resource assignments for the effort.
b) Manage the project in close coordination with the Contracting Officer Representative (COR).
c) Have weekly status meetings with the COR.
d) Provide the government with a written Monthly Status Report. The report at a minimum shall address:
    - work accomplished in this period
    - work to be accomplished in the next period
    - schedule variance
    - risks and issues that need to be addressed between the contractor and government
e) Support technical compliance and service in all functional areas.
f) Develop and implement quality control and quality assurance measures for all areas of program performance.
g) Analyze descriptive and inferential data.

h) Provide quantitative and qualitative program evaluation and analysis.
i) Deliver continuous process improvement.
j) Develop and deliver business continuity of operations.
k) Respond promptly to technical questions.
l) Report program status and trending information.
m) Maintain effective internal and external communication processes and systems.
n) Rapidly respond to changing and emerging requirements and mandates.

3.4.1.1 Change Management

The Contractor shall develop a Change Management Plan that addresses how to prepare the end user for this solution. The plan shall cover all phases of the project and shall include vision and goals, stakeholders, resources required to carry out the plan, a schedule, roles and responsibilities, and communication tools and strategy (including key messages).

3.4.2 ELECTRONIC CONTRACT FILING SYSTEM

The Contractor shall:

a) Provide an Electronic Contract Filing System utilizing a Software as a Service (SaaS) licensing and delivery model on an authorized FedRAMP cloud hosted environment.
b) System shall meet the requirements addressed at Appendix A – Requirements Identification Matrix and Appendix B – Contract File Checklists.
c) Provide a license mixture that is appropriate for the phased implementation approach (Testing, Pilot, and Full Implementation).
d) Provide a complete solution that meets the standard required for the DHS Enterprise Architecture (see SOW section 3.5.5, DHS Enterprise Architecture Compliance).
e) Provide a solution that complies with the DHS Management Directive (MD) 4300A Sensitive Systems Policy Handbook.

The Solution shall:

a) Allow for electronic contract storage, workflow, document management, secure digital signature, document extraction and redaction, and records management.
b) Comply with the DHS Technical Reference Model (TRM), Federal Acquisition Regulation, Management Directive 4300, and Section 508, and other documents listed in the requirements located at Appendix A and in SOW section 3.5.5.
c) Support the entire DHS procurement community of users in geographically dispersed locations (roughly 1,400 Contracting Officers/Specialists and 600 support personnel).
d) Support a minimum of 3 Government System Administrators per component in geographically dispersed locations
e) Consist of three logically isolated environments designated as configuration/testing, staging/pre-production and production.
f) Be scalable allowing DHS the flexibility to meet current and future requirements.

3.4.2.1 Configuration/Testing Environment

The development environment shall support all development activities, integration, testing, actor shall provide an effective solution that utilizes industry standards such as, ANSI, IEEE, and ISO as required, and best practices that supports the continued development of the ECFS solution. The solution shall be scalable, maintainable, and

reliable to accommodate any future enhancements.

3.4.2.2 Staging/Pre-Production Environment

The Staging/Pre-production Environment shall support all pre-production activities, training, user acceptance testing, and troubleshooting. This environment must be logically isolated from the end user but representative of the production environment. The Contractor shall provide an effective solution that utilizes industry standards and best practices to allow for testing, training and troubleshooting in a manner that is representative of the production environment. The solution shall be flexible to accommodate any future enhancements.

3.4.2.3 Production Environment

The Production Environment shall support all production activities. The Contractor shall provide an effective solution that utilizes industry standards and best practices. The solution shall be flexible to accommodate any future enhancements.

3.4.2.4 Ad Hoc Workflow

The contractor shall implement workflow to allow any user to route any document to one or more user with the appropriate access rights for review, comment, approval, and electronic signature. The contractor shall conduct all planning, analysis, system design, configuration, testing, training, and help desk necessary to accomplish this task. The contractor shall update any documentation (e.g., RTMX, system design document, system configuration document, training documents, etc.) that is impacted by this task.

3.4.2.5 Secure Digital Signature

The contractor shall implement secure digital signatures for documents that are approved within ECFS. Contractor's digital signature solution shall meet DHS Electronic Signature Policy Guidance as outlined in *"DHS Electronic Signature Policy Guidance, v1.03, October 2, 2015"*. The contractor shall conduct all planning, analysis, system design, configuration, testing, training, and help desk necessary to accomplish this task. The contractor shall update any documentation (e.g., RTMX, system design document, system configuration document, training documents, etc.) that is impacted by this task.

3.4.2.6 Document Extraction and Redaction

The contractor shall implement functionality that will permit the user to select documents from a contract file, extract copies, and redact or support redaction of information for purposes such as responding to an audit, litigation, or Freedom of Information Act (FOIA) request. This capability shall include all related requirements located in Appendix A. The contractor shall conduct all planning, analysis, system design, configuration, testing, training, and help desk necessary to accomplish this task. The contractor shall update any documentation (e.g., RTMX, system design document, system configuration document, training documents, etc.) that is impacted by this task.

3.4.2.7 Reports

The solution shall have the capability to generated standard and configurable reports. . The contractor shall conduct all planning, analysis, system design, configuration, testing, training, and help desk necessary to accomplish this task. The contractor shall update any documentation (e.g., RTMX, system design document, system configuration document,

training documents, etc.) that is impacted by this task.

3.4.3 SYSTEM FUNCTIONAL OVERVIEW

The contractor shall provide a complete functional overview and demonstration on the functional capabilities of the solution to a DHS Government team of no more than 25 members. The overview and demonstration shall be a live demonstration of the solution's available built in capabilities. The purpose of the demonstration is to provide the Government members an in-depth understanding of how the software operates.

3.4.4 REQUIREMENTS REVIEW

The contractor shall work with the Government to conduct an in-depth analysis of functional requirements located in Appendix A Requirements Identification Matrix. The Government team shall consist of representatives from each of the contracting activities. The contractor shall work with the Government to determine how the solution will satisfy the functional requirements in detail. The contractor shall conduct an analysis, with the Government, to study the current approach to managing contract files; review functional requirements; define business rules; review policies and procedures; and determine how they will be accommodated within the solution. The contractor shall deliver a Requirements Traceability Matrix (RTMX) that lists each of the detailed requirements and maps the requirements back to the high level requirements.

3.4.5 SYSTEM DESIGN

The Contractor shall:

a) Incorporate the system level requirements into the System Design Document to accommodate the requirements identified in the Requirements Identification Matrix (RIM).
b) Deliver a System Design Document that is based on IEEE Std 1016 or the latest version, that includes:
    1. A system overview.
    2. Illustration of hardware components and software components.
    3. Documentation on how the system will meet the requirements identified in the RIM.
    4. Documentation on how business processes will be supported by the system.
    5. Data backups, redundancy methodology, and disaster recovery capability to prevent data loss due to hardware or software failure.
    6. Minimum desktop hardware and incorporates system and software requirements.

3.4.6 CONFIGURATION

The Contractor shall:

a) Deliver a System Configuration Document that documents specific configuration settings within the system.
b) Configure the solution in accordance with the System Configuration Document.
c) Include DHS technical representatives in the configuration efforts to incorporate DHS business rules and practices.

d) Provide and implement PIV/CAC functionality so that users must use their DHS PIV cards to gain access to the system.

3.4.6.1 PIV/CAC Implementation

The contractor shall provide and implement PIV/CAC functionality so that users must use their DHS PIV/CAC cards to gain access to the system. The contractor shall conduct all planning, analysis, system design, configuration, testing, training, and help desk necessary to accomplish this task. The contractor shall update any documentation (e.g., RTMX, system design document, system configuration document, training documents, etc.) that is impacted by this task.

3.4.7 TESTING

The Contractor shall:

a) Deliver a System Test Plan that includes tests that will demonstrate and verify the solution successfully satisfies the requirements listed in Appendix A Requirements Identification Matrix (RIM).
b) Test the solution in accordance with the System Test Plan.
c) Deliver User Acceptance Test Procedures.
d) Be available to answer questions and monitor the testing process.
e) Document the results of testing in a Test Report.

3.4.8 INFORMATION SECURITY

The Contractor shall:

a) Meet all security specifications to obtain an Authority to Operate (ATO) that complies with DHS MD4300A.
b) Meet all security requirements for a solution in a FedRAMP cloud hosted environment on an unclassified network.
c) Ensure the cloud hosted environment meets at a minimum, Moderate Security impact level.
d) Submit an IT Security Plan, which details the approach, methods, and safeguards the contractor will utilize to comply with Government and DHS Information Technology security requirements.
e) Assist the ECFS Information System Security Officer (ISSO) in the completion of applicable Security Authorization documentation required in order to obtain an ATO.
f) Make all system configuration changes, software, or Operating System updates, and apply relevant security patches to the system as directed by the Authorizing Official (AO) or his representative.
g) Work with the ISSO to modify or update the appropriate Security Authorization documentation as necessary during the certification testing process to reflect all system changes.
h) Assist the ECFS ISSO to obtain the accreditation approval of the system and Security Authorization documentation from the AO or AO representative.

3.4.9 OPERATION AND MAINTENANCE

The Contractor shall operate and maintain the production, pre-production/staging, and

test/development environments of the system such that:

a) Help Desk support is provided.
b) System is available 24x7.
c) Change control processes are provided to secure the functionality of the environment without hindering the ability of developers, managers to efficiently add new functionality, integration, and or delivery mechanisms.
d) Appropriate patch management and control for operating systems is provided that adheres to FISMA and FedRAMP standards.
e) Application software is maintained including installation of software defect corrections, database scripts and upgrades.
f) The system status (server hardware, software, and database) is monitored to proactively identify issues.
g) Automated monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating systems, applications, etc. is provided.
h) Identified issues are researched and mitigated.
i) Virus Protection is kept current.
j) Performance analysis and tuning, running software/database update scripts, indexing tables is accomplished to optimize system performance.
k) Contingency Plan testing is performed in accordance with security requirements.
l) The solution is reviewed and managed in a manner that ensures the application and associated environment complies with the requirements established in DHS MD4300A.

3.4.10 HELP DESK SUPPORT

The Contractor shall:

a) Provide help desk support in accordance with the Contractor's SaaS licensing and delivery model.

3.4.11 PILOT PROGRAM

The Contractor shall:

a) Implement the Solution in accordance with the Project Management Plan, System Design Document, and System Configuration Document.
b) Implement the Solution for no more than 100 total user's representative of all Contracting Activities.
c) Use surveys and/or meetings with stakeholders to gather the feedback from the Pilot.

3.4.11.1 Post Pilot Implementation Review Report

The Contractor shall compile stakeholder feedback in a Post Implementation Review Report and shall include recommended updates for the system based on stakeholder feedback and other findings.

3.4.12 FULL IMPLEMTATION/ROLLOUT

The Contractor shall:

a) Support the rollout of the solution to the remaining users across DHS in accordance with the Project Management Plan.

b) Update as necessary documentation in support of implementation (to include, but not limited to: project plans, updated user guides, etc.).
c) Perform all necessary tasks to support the implementation (to include, but not limited to: training, change management, etc.).

3.4.13 TRAINING

The Contractor shall:
a) Determine the most effective training methodology for a dispersed end user community.
b) Deliver a Training Plan that addresses at a minimum the functionalities of the system, training objectives, delivery methodology, detailed schedule, and its strategy and approach to ensuring end users are properly trained.
c) Deliver the training in accordance with the Training Plan
d) The contractor shall provide user guides that include DHS processes.
e) Provide User guides that shall cover all topic areas covered in the training. The user guides shall be updated in the event that the system functionality changes. Guides shall be provided in an electronic format and via a context oriented online guide and shall be 508 Compliant.
f) Deliver System Administrator training in accordance with the training plan.
g) Provide a System Administrator Guides for the DHS System Administrators. The Guides shall cover all topic areas covered in training.

3.4.14 RECORDS MANAGEMENT

The Contractor shall:
a) Provide functionality to permit the management of federal records in accordance with DHS retention policies and NARA requirements. NARA regulations affecting Federal agencies and their records management programs are found in Subchapter B of 36 Code of Federal Regulations Chapter XII.
b) Provide a solution IAW with FAR Subpart 4.7: Contractor Records Retention and FAR Subpart 4.8: Government Contract Files.

3.4.15 TRANSITION OUT

The Contractor shall:
a) Provide a Phase Out Transition Plan that illustrates how the Contractor shall provide a seamless transition between the incumbent and the successor. This plan will ensure minimal disruption of the Government's activities.
b) Ensure data is transferable in a non-proprietary format.

3.5 GENERAL

3.5.1 CONTRACTOR PERSONNEL

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW. See Attachment 3 for Labor Category Descriptions and Qualifications.

3.5.1.1 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. If for any reason the Contractor staffing levels are not maintained due to resignations, transfers, vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the appropriate Contracting Officer's Representative (COR). Otherwise, the Contractor shall provide a fully qualified replacement.

3.5.1.2 Key Personnel

3.5.1.2.1 Project Manager

The Contractor shall provide a Project Manager designated as Key Personnel that shall act as the central point of contact for the Government for all program-wide technical issues, and will represent the Contractor at all post-award status meetings. The Project Manager shall be responsible for all issue resolution, program management, and other contract support including providing comprehensive account support for the BPA. The Project Manager shall be a single point of contact for the BPA Contracting Officer and the BPA Contracting Officer's Representative (COR). The Project Manager shall HAVE a minimum of five (5) years of experience. Requirements for this key position are:

- Manage and oversee work performance of one or more Orders
- Plan, manage and oversee the work efforts of team personnel
- Interface with the Government to ensure client satisfaction
- Determine and monitor Order schedules
- Ensure compliance with all BPA and subsequent Order requirements and quality standards
- Provide guidance, direction and Contractor management for the BPA, and reviews all services for conformance to Government requirements

The Project Manager shall be available to the BPA COR via telephone between the hours of 8:00 a.m. and 5:00 p.m. (ET), Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within twenty-four (24) hours of notification.

The name of the Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government. The Project Manager is further designated as *Key* by the Government. During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. Additionally, the Contractor shall not replace the Project Manager without prior approval from the BPA Contracting Officer.

3.5.1.2.2 Subject Matter Expert (SME)

The contractor shall provide an 1102 Subject Matter Expert. "1102" is the Government's Contracting Officer and Contract Specialist job series. The 1102 SME shall have a minimum of five (5) years of experience in the federal procurement operations process. Specifically, the 1102 SME shall have an in-

depth understanding of the contract filing process, the contract file lifecycle, and the documentation that constitutes the contract file. Ideally, the 1102 SME should have a minimum of one year of experience implementing and maintaining document management systems.

Note: Other "Key Personnel" will be identified at the Order level.

3.5.1.2.3 Replacement of Key Personnel
Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the BPA Contracting Officer no less than fifteen (15) business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute. All proposed substitutes shall possess at a minimum the required key personnel labor category qualifications and skill levels as listed in Attachment 4 Labor Category Descriptions and Qualifications. The Contractor shall not replace *Key* Contractor personnel without approval from the BPA Contracting Officer.

3.5.1.3 Employee Identification

3.5.1.3.1 Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

3.5.1.3.2 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

3.5.1.4 Employee Conduct
Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

3.5.1.5 Removing Employees for Misconduct or Security Reasons
The Government may, at its sole discretion (via the Contracting Officer*), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to

continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

3.5.2 IT SECURITY AND PRIVACY

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.

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.

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

shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The email notification shall state the required training has been completed for all Contractor and subcontractor employees.

3.5.2.1 Security Review Terms and Conditions

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

3.5.2.1.1 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.

3.5.2.1.2 Security Operations Terms and Conditions

The Contractor shall operate a Security Operations Center (SOC) to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the Contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The Contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the Contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the Contractor facility SOC shall adhere to the incident response plan.

3.5.2.1.3 Computer Incident Response Services Terms and Conditions

The Contractor shall provide Computer Incident Response Team (CIRT) services. The Contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The Contractor shall conduct Incident Response Exercises to ensure all personnel are

familiar with the plan. The Contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer, 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 with 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.

3.5.2.1.4 Firewall Management and Monitoring Terms and Conditions
The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The Contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the Contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

3.5.2.1.5 Intrusion Detection Systems and Monitoring Terms and Conditions
The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the network intrusion detection system (NIDS) solution. The Contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the Contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

3.5.2.1.6 Physical and Information Security and Monitoring Terms and Conditions
The contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to assets. DHS contracted IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office. The contractor is required to maintain within the 50 states, the District of Columbia, or outlying areas of the United States, all Government data that is not physically located on DoD premises, unless otherwise authorized by the contracting officer in writing.

3.5.2.1.7 Vulnerability Assessments Terms and Conditions
The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

3.5.2.1.8 Anti-malware (e.g., virus, spam) Terms and Conditions
The Contractor shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The Contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the Contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

3.5.2.1.9 Patch Management Terms and Conditions
The Contractor shall provide patch management services. The Contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The Contractor shall be informed by DHS, which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the Contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), NIDS, anti-malware, and Firewall) shall be tested by the Contractor prior to deployment in a test environment.

3.5.2.1.10 Log Retention Terms and Conditions
Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

3.5.2.1.11 Controls
The Contractor shall comply with Department of Homeland Security (DHS) technical, management and operational security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A series security policy documents and are based on the NIST 800-53 Special Publication (SP) standards.

3.5.3 PROTECTION OF INFORMATION

Contractor access to information protected under the Privacy Act is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with the law and Government policy and regulation.

Contractor access to proprietary information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

3.5.4 PERSONALLY IDENTIFIABLE INFORMATION (PII)

The Contractor shall exercise care when handling all PII. The Contractor shall:

a) Only disclose PII within DHS to those who have a need-to-know and only outside of DHS in accordance with the Privacy Act and other applicable federal law and DHS policy. Sensitive PII requires special handling because of the increased risk of harm to an individual if it is compromised.
b) Have a nondisclosure agreement on file with DHS, and complete the mandatory online privacy awareness training course.
c) Handle Sensitive PII in accordance with the Handbook for Handling Sensitive Personally Identifiable Information.
d) Access PII only via DHS-approved laptops, USB flash drives, and external hard drives, all of which must be encrypted as noted in *DHS Sensitive Systems Policy Directive 4300A.*
e) Follow all privacy incident reporting and handling requirements as set forth in the DHS Privacy Incident Handling Guide.

3.5.5 COMPLIANCE AND REFERENCE DOCUMENTS

The Contractor solution shall follow all current versions of Government and DHS policies, procedures, guidelines, and standards. The following documents provide specifications, standards, and/or guidelines that shall be complied with in order to meet the requirements of this BPA:

- Title 5 U.S.C.
- Title 5 CFR Chapter 1, Part 1-1199
- Title 36 CFR Chapter XII, Subpart B
- All applicable Federal laws and regulations
- All applicable guides, policies, guidance, and procedures (e.g., OPM, GAO, DHS, OMB, etc.)
- DHS MD 11042.1 Safeguarding Sensitive but Unclassified (For Official Use Only) Information
- MD 4300A DHS Sensitive Systems Policy and Handbook
- Handbook for Safeguarding Sensitive Personally Identifiable Information, DHS Privacy Office, March 2012
- Privacy Incident Handling Guide, January 2012
- Management Directive 047-01, Privacy Policy Compliance
- DHS IT Security Program Handbook for Sensitive Systems (MD 4300A), V9.0 dated October 11, 2011.
- DHS Security Architecture Appendix: Cloud Computing Implementation V1.0, 11/17/2011
- DHS Management Directive 140-01, Information Technology Security Services
- ITAR Quick Essentials Guide V2.0, dated 12/29/2011

- Federal Cloud Computing Strategy, February 2011
- Security Authorization of Information Systems in Cloud Computing Environments, December 2011
- OMB Memo, subject: Security Authorization of Information Systems in Cloud Computing Environments, dated December 8, 2011
- 25 Point Implementation Plan to Reform Federal Information Technology, December 2010
- NIST Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-30, Risk Management Guide for Information Technology Systems, dated June 2001
- NIST SP 800-34 R1, Contingency Planning Guide for Federal Information Systems, dated May 2010
- NIST SP800-37 R1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, dated February 2010
- NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, dated August 2002
- NIST SP 800-53 R4, Recommended Security Controls for Federal Information Systems and Organizations, dated August 2009
- NIST SP 800-60 R1, Guide for Mapping Types of Information and Information Systems to Security Categories, dated August 2008
- NIST SP 800-63 R1, Electronic Authentication Guideline, dated December 2011
- NIST SP 800-88, Guidelines for Media Sanitization, dated September 2006
- NIST SP 800-116, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS), dated November 2008
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), dated April 2010
- NIST SP 800-125, Guide to Security for Full Virtualization Technologies, dated January 2011
- NIST SP 800-137, Information Continuous Monitoring for Federal Information Systems and Organizations, dated September 2011
- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, dated December 2011
- NIST SP 800-145. A NIST Definition of Cloud Computing, dated September 2011
- NIST SP 800-146, DRAFT Cloud Computing Synopsis and Recommendations, dated May 12, 2011
- NIST SP 500-292, NIST Cloud Computing Reference Architecture
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources
- Public Law 107-347, E-Government Act of 2002, including Title III, Federal Information Security Management Act (FISMA)
- DHS Acquisition Instruction/Guidebook 102-01-001 Appendix B SELC Guide version 2.0
- HSPD-12 Policies for a Common Identification Standard for Federal Employees and Contractors
- OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
- OMB M-06-16 Acquisition of Products and Services for Implementation of HSPD-12
- NIST FIPS 201 Personal Identity Verification (PIV) of Federal Employees and Contractors

- OMB M-10-15 FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
- DHS National Security Systems Policy Directive (PD) 4300B
- DHS 4300B National Security Systems Handbook
- DHS IT Security Architecture Guidance Volumes 1, 2 and 3
- DHS Electronic Signature Policy Guidance, v1.03, October 2, 2015
- DHS System Lifecycle (SELC)

3.5.6 GOVERNMENT-FURNISHED RESOURCES

The Government will provide the workspace, equipment and supplies necessary to perform the on- site portion of Contractor services required in this BPA unless specifically stated otherwise in this work statement. The Contractor shall use Government furnished facilities, property, equipment, systems, and supplies only for the performance of work under this BPA, and shall be responsible for returning all Government-furnished facilities, property, and equipment in good working condition, subject to normal wear and tear. The Government will provide all necessary systems, information, data, and documents to the Contractor for work required under this BPA.

The Contractor shall use Government-furnished systems, information, data, and documents only for the performance of work under this BPA. It is the Contractor's responsibility to return all Government-furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government-furnished information, data, and documents to outside parties without the prior and explicit written consent of the Contracting Officer and only in compliance with the Privacy Act, 5 U.S.C. § 552a, and other applicable federal law and DHS policy.

3.5.7 GOVERNMENT-FURNISHED PROPERTY

The Government shall provide the on-site Contractor's staff with computer workstations, network and system access, cubicles, access to duplicating machines, miscellaneous office supplies, and phones. The phones shall be used for work purposes only or for emergency calls.

The Contractor shall use Government-furnished information, systems, data, and documents only for the performance of work under the BPA, and shall be responsible for returning all Government-furnished information, data, and documents to the Government at the end of the performance period. The Contractor shall not release Government-furnished information, data, and documents to outside parties without the prior and explicit consent of the Contracting Officer and only in compliance with the Privacy Act, 5 U.S.C. § 552a, and other applicable federal law and DHS policy.

The Contractor's employees shall keep the workstations neat and tidy. Personal items in the work area or hung on the cubicle walls must be kept to a minimum and must be in keeping with the professional image and guidelines of the Department of Homeland Security. The Government reserves the right to require an employee to remove any item that violates Equal Employment Opportunity laws, has the actual or the appearance of sexual harassment, or is not of a professional nature.

3.5.8 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this BPA, except for the Government Furnished Resources specified in the SOW.

3.5.9 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

Accessibility Requirements (Section 508)

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

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

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.
36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

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

36 CFR 1194.26 Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed under this work statement.

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

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

Section 508 Applicable Exceptions

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

Section 508 Compliance Requirements

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

3.5.10 GENERAL REPORTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows 7 and Microsoft Office Applications).

3.5.10.1 Project Plan
The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a Final Contractor Project Plan to the COR not later than ten (10) business days after the Post Award Conference.

3.5.10.2 Business Continuity Plan
The Contractor shall prepare and submit a Business Continuity Plan (BCP) to the Government. The BCP Plan shall be due 30 business days after the date of award, and will be updated on an annual basis. The BCP shall document Contractor plans and procedures to maintain support during an emergency, including natural disasters and acts of terrorism. The BCP, at a minimum, shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- How the Contractor will communicate with the Government during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
    - Telephone numbers
    - E-mail addresses

3.5.10.2.1 Individual BCPs shall be activated immediately after determining that an emergency has occurred, shall be operational within 24 hours of activation or as directed by the Government, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with the Contractor Project Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Project Manager and the COR shall promptly open an effective means of communication and verify:

- Key points of contact (Government and contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential Contractor work products expected to be continued, by priority

3.5.10.2.2 The Government and Contractor Project Manager shall make use of the resources and tools available to continue contracted functions to the maximum

extent possible under emergency circumstances. Contractors shall obtain approval from the Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

3.5.10.3 Progress Reports

The Project Manager shall provide a monthly progress report to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

3.5.11 PROGRESS MEETINGS

The Project Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at the Government's facility or via teleconference.

The Project Manager shall meet with the COR on a weekly basis to discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place at the Government's facility or via teleconference.

3.5.12 GOVERNMENT ACCEPTANCE PERIOD

The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

3.5.12.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor’s accepted proposal. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

3.5.12.2 The COR will have ten (10) business days to review deliverables and make comments. The Contractor shall have five (5) business days to make corrections and redeliver.

3.5.12.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

3.5.13 DELIVERABLES

The Contractor shall provide the following BPA deliverables in accordance with the following schedule. Order deliverable's shall be specified at the order level.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	2.17	Post Award Conference	10 business days after Award	N/A
2	3.5.10.1	Draft Contractor Project Plan	At Post Award Conference	COR, Contracting Officer
3	3.5.10.1	Final Contractor Project Plan	10 business days after post award conference	COR, Contracting Officer
4	3.4.8	Draft IT Security Plan	At time of proposal	COR, Contracting Officer
5	3.4.8	Final IT Security Plan	30 business days after Award	COR, Contracting Officer
6	3.5.10.2	Original Business Continuity Plan	30 business days after Award	COR, Contracting Officer
7	3.5.10.2	Updated Business Continuity Plan	Adhoc/Annual	COR, Contracting Officer
8	3.5.10.3	Progress Reports	Second Tuesday of each Month	COR, Contracting Officer

4. INSTRUCTIONS TO QUOTERS
(This section will be removed upon award.)

4.1 Introduction

This Request for Quote will be conducted in a three-phase approach as follows:

Key	
***Phase 1**	Verification of FedRAMP Authorization, Solution Overview, Capability Confirmation Checklist
****Phase 2**	Product Demonstration
*****Phase 3**	Past Performance, Management/Technical Approach, Price

Quoters must pass all aspects of a given Phase in order to receive notification to the next Phase. If a Quoter is found unacceptable during evaluation Phase progression, the Quoter's submission will no longer be considered for BPA award.

Phase 1

The Quoters shall submit the following information as part of Phase 1:

1. Documentation verifying FedRAMP Authorization;

2. Solution Overview: Brief summary of Quoter's solution signifying capabilities for electronic contract storage, document management, workflow, records management, electronic signature, document extraction and redaction, and PIV authentication.
3. Capability Confirmation Checklist.

Phase 1 quotation submissions are due no later than ***1:00 p.m., Eastern Time (ET), Tuesday, July 11, 2017. Quotes shall be submitted electronically to the Contract Specialist and Contracting Officer at:*** DHS.ECFS@hq.dhs.gov.

Phase 2

Upon notification by the Contracting Officer (CO), Quoters shall provide a demonstration of their proposed solution. It is anticipated that demonstrations will start on or about **Monday, *July 24, 2017*.** The CO will confirm the specific date and time with those Quoters invited to participate in Phase 2. Quoters must be prepared to provide a demonstration during the timeframe the CO sets forth. Demonstrations will take place at a Government facility located in the Washington, DC metro area. The specific location will be identified by the CO in the notification to Quoters invited to participate in Phase 2.

The government will not provide any hardware, software, or technical capabilities for these demonstrations. Quoter will be required to bring all necessary equipment needed to conduct the technical demonstrations.

Phase 3

The Quoters shall submit the following information as part of Phase 3:

- Past Performance
- Management/Technical Approach
  - Technical Approach
  - Management Plan
  - Staffing Plan
  - Draft IT Security Plan
  - Categorization of Government Requirements - Requirements Identification Matrix
  - Contractor Teaming Arrangement/Subcontracting (if applicable)
- Price

Phase 3 quotation submissions are due no later than ***1:00 p.m. ET, Tuesday, August 8, 2017***. ***Quotes shall be submitted electronically to the Contract Specialist and Contracting Officer at:*** *DHS.ECFS@hq.dhs.gov*.

Quoters shall submit their Phase 1 and Phase 3 quotations via email under the instructions contained herein. Quoters shall submit their Phase 1 and 3 quotations as "PDF" documents except when specified otherwise.

Each electronic file shall be clearly named in accordance with the RFQ 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) In order to facilitate secure transmission, it is recommended that emailed files are compressed (zipped) into one, ZIP file using WinZip.
(4) The WinZip password shall be submitted under a separate email by the closing date and time of this RFQ.
(5) All submissions shall include HSHQDC-17-Q-00231 in the subject line of the email.

Quotations submitted must be received by the Goverrnment by the cut-off date and time as stipulated in the instructions. Late Quotes will be processed in accordance with FAR Part 15.208—Submission, Modification, Revision, and Withdrawal of Proposals.

4.2 Prospective Quoter's Questions

All questions regarding this RFQ shall be submitted in writing to the Contract Specialist, Michael Lipperini and the Contracting Officer, Randy Dreyer at: DHS.ECFS@hq.dhs.gov.

Questions are due no later than ***1:00 p.m. ET, Wednesday, July 5, 2017***.

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 ensure that questions are written to enable a clear understanding as to the Quoter's issues or concerns with the referenced area of the RFQ. 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. Late questions may be addressed if it's in the Government's interest.

Answers to questions will be provided to all prospective Quoters, giving due regard to the proper protection of proprietary information. In order 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 the DHS will not address hypothetical questions aimed toward receiving a potential "evaluation decision" from the 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.: HSHQDC-17-Q-00231 – Questions Submitted (Contractor Name)

The table below may be included in the email or as a separate attachment but shall be in the below format.

	Reference RFQ Section	Paragraph No.	Page No.(s)	Question
1				
2				

All questions will be answered in an amendment and provided to all Quoters via email. DHS will not attribute any question(s) asked to the submitting Quoter(s).

4.3 General Quotation Preparation

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. The Quoter shall follow the detailed quotation package instructions contained herein, and not include multiple combinations of alternates or extensive options within its quotation package.

Information requested herein shall be furnished in writing fully and completely in compliance with instructions. The information requested and the manner of submittal is essential to permit prompt evaluation of all Quotations on a fair and uniform basis. Simple statements of compliance (i.e., "understood"; "will comply") without the detailed description of how compliance will be met may not be considered sufficient evidence that the proposed services can technically meet the requirements of this RFQ. Accordingly, any Quotation in which material information requested is not furnished, or where indirect or incomplete answers or information is provided may be considered not acceptable for evaluation.

Changes to the Quotation by the Quoter shall be accomplished by amended quote(s). Any changes from the original information (quote) shall be indicated by a vertical line, adjacent to the change, on the outside right margin of the page. The Quoter shall include the date of the amendment on the lower right edge of the page. Quotation amendments will be allowed only prior to the due date for Quotations.

Quoters whose Quotations were not selected for award will be notified. Such notification will state in general terms the basis of non-selection. Pursuant to FAR 8.405-3(b)(3), unsuccessful Quoters may request a brief explanation of the basis for the award decision that was based on factors other than price alone.

The Contracting Officer will retain a copy of each quotation, successful or unsuccessful.

4.3.1 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.

4.3.2 Quotation Validity Period

Quotations shall be valid for a minimum of ninety (90) days.

4.3.3 Quotation Content and Submission Instructions

4.3.3.1 Quotation Content (Phase 1 and Phase 3)

Each Quoter shall submit a quotation, which consists of three (3) electronic volumes and a product demonstration. The electronic volumes are described below:

Naming Convention	Tab Title
Volume I: Technical (Phase 1) (Electronic) (Zip File)	
Tab A (Document)	Quotation Cover/Transmittal Letter (limit 2 pages)
Tab B (Document)	FedRAMP Authorization Documentation (limit 5 pages)
Tab C (Document)	Solution Overview (limit 10 pages)
Tab D (Document)	Capability Confirmation Checklist (1 page)
Volume II: Technical (Phase 3) (Electronic) (Zip File)	
Tab A (Document)	Past Performance (limit 5 pages excluding past performance information form(s))

Tab B (Document)	Management/Technical Approach (limit 20 pages excluding QAP, and resumes (resume limit 3 pages))
Tab C (Document)	Categorization of Government Requirements - Requirements Identification Matrix
Tab D (Document)	Contractor Teaming Arrangement/Subcontracting
Volume III: Business & Pricing (Phase 3) (Electronic) (Zip File)	
Tab A (Document)	Quotation Cover/Transmittal Letter (limit 2 pages); GSA Pricing Schedule; HSAR Clause 3052.209-70 (f) *Disclosure*; and HSAR Provision 3052.209-72 (c) *Disclosure*.
Tab B (Document)	Worksheet 1 Labor Descriptions (Attachment 4)
Tab C (Document)	Worksheet 2 Pricing (Attachment 4)
Tab D (Document)	Worksheet 3 Total Price (Attachment 4)

Information contained in each volume shall be complete to the extent that evaluation of each tab may be accomplished independently of, and concurrently with, evaluation of the other. Your responses must demonstrate that both your firm and personnel can successfully complete this project. Quoters shall strictly adhere to the page limits.

NO PRICE INFORMATION IS TO BE INCLUDED IN VOLUME I AND II

Volume I – Technical (Evaluation Factor 1) (Phase 1)

Tab A: Quotation Cover/Transmittal Letter (limit 2 pages)

Your submission of the Quotation Cover/Transmittal Letter shall include the following information:

1) Dun & Bradstreet Number (DUNS)
2) Authorized Point of Contact
3) Contact Email address
4) Contact telephone and fax number
5) Complete business mailing address
6) GSA schedule contract number and expiration
7) Quote Validity Period

Tab B: FedRAMP Authorization (limit 5 pages)
Quoter shall provide documentation verifying the Cloud Hosting Environment has FedRAMP authorization at the Moderate security impact level at time of proposal.

Tab C: Solution Overview (limit 10 pages)
Quoter shall provide a high-level discussion of the functionalities of the proposed solution that must demonstrate each of the following minimum capabilities:

- Electronic contract storage
- Document Management
- Workflow
- Records Management
- Electronic Signature
- Document Extraction and Redaction
- PIV authentication
- Reports

Tab D. Capability Confirmation Checklist (limit 1 page)
Quoter shall fill out the Capability Confirmation Checklist. Quoter shall have an authorized signee affirm that the proposed solution offers the minimum capabilities as cited in the checklist.

Technical - Product Demonstration (Evaluation Factor 2) (Phase 2)

The location, date, and time of product demonstration will be determined after evaluation of Phase 1. The Quoter will be notified by the Contract Specialist and/or Contracting Officer of the Quoter's status to proceed to Phase 2.

The Quoter shall conduct the following demonstration(s) of the proposed software solution to the Government evaluation team:

- Access the solution using Microsoft Internet Explorer and Mozilla Firefox
- Create a new user account and apply access rights
- Log on using PIV credentials
- Show dashboard or landing page that the user would see once logging in
- Upload file 30GB in size
- Demonstrate how a user can upload a minimum of 3 files simultaneously to a folder Show file structures consisting of groupings and subgroupings of files and folders similar to Appendix B Contract Checklists Enter a contract name that has 100 alphanumeric and symbolic characters
- Search for documents based on key words using a minimum of 3 key words in a single search Demonstrate how a user at a minimum is able to search for a document, make changes to a document, and save the document back in the system with the changesDemonstrate how permissions are applied to folders and individual documents. Permissions at a minimum shall allow for "No Access" "Read Only", "Contribute-No Delete", "Contribute-with Delete ", "Full Access" or comparable permission controls.
- Demonstrate that a user sees only files they have been granted access to
- Demonstrate how to create a standard workflow process to be used to support a document review, approval and signature process. A minimum of 3 users shall be able to be added to the workflow. Show basic ad hoc workflow where one user routes a document to another user for review, comment, approval, and electronic signature. (e.g., contract specialist sends a draft document to contracting officer for contracting officer to review and make comments). A minimum of 3 users shall be able to be added to the workflow. Demonstrate how a user can setup notifications and/or alerts at the folder and document level to alert them when changes to a document have been made and when new

documents have been added to a folder. A minimum of 1 alert per document and 1 alert per folder.Demonstrate how a user digitally signs a document within the solution
- Demonstrate redaction of document contents
- Demonstrate how a user designate files for archiving in accordance with NARA requirements
- Demonstrate how files are disposed once they have been retained for the NARA specified amount of time period
- Demonstrate how government "super users" can reset user passwords, apply permissions, configure workflows, and modify user accounts Demonstrate how a user can generate reports based on the following criteria at a minimum: Purchase Request Number, Solicitation Number, Contract Number, Periods of Performance, Option Periods, Delivery Date, Obligation Amount, and Total Contract Cost. User shall be able to generate a report of the above data using a minimum of 3 key words.

The Government retains the right to ask the Quoter to repeat or clarify steps during the demonstrations. This act does not constitute discussions or exchanges with Quoters.

Volume II – Technical (Phase 3)

Tab A: **Past Performance (Evaluation Factor 3) (limit 5 pages excluding past performance information form(s))**

Demonstrated prior experience successfully delivering a high quality, functioning electronic contract filing system to a Federal agency to support the acquisition or procurement electronic contract filing requirements of the Federal agency. The Government will evaluate relevant past performance of each Quoter. The Quoter who will perform technical work relevant to the SOW shall identify three (3) ongoing or successfully completed projects performed by the Quoter (as a Prime Contractor or Subcontractor) that demonstrate recent and relevant past performance. ***Recent*** is defined as within the last three (3) years. ***Relevant*** is defined as work similar in size and scope to the work identified in the SOW.

Quoters shall also provide the information outlined in Attachment 2, Past Performance Information Form. Attachment 2 will be used to assess the relevancy of past performance and may be used to obtain past performance references. In addition, Past Performance reports may also be accessed and utilized by the Government through the Past Performance Information Retrieval System (PPIRS) at https://www.ppirs.gov.

Tab B: Management/Technical Approach (Evaluation Factor 4) (limit 20 pages excluding QAP and resumes (resume limit 3 pages))

The Quoter's Management/Technical Approach shall describe the Quoter's ability to effectively manage the work and provide the proposed team composition to accomplish the requirements in the SOW. In order to facilitate the evaluation of the Quoter's Management/Technical Approach, the Quoter's Management/Technical Approach shall include a Management Plan, Staffing Plan, and Draft IT Security Plan that is simple, easy to read and clearly describes personnel responsibilities.

1) Technical Approach shall address the following:

- Discussion of the background, objectives, and work requirements of the SOW;
- Discussion of how each aspect of the SOW will be accomplished including proposed methods and techniques for completing each task;
- Discussion which supports how each task will be evaluated for full performance;
- Discussion of any technical barriers/anticipated major difficulties and problem areas, along with potential recommended approaches for their resolution.

2) The Management Plan, at a minimum, shall address the following:

- Understanding of the ability to provide management and reporting support services as outlined in the SOW
- A detailed explanation of how the Quoter intends to resolve technical issues, to include the methodology of providing customer service
- Understanding of the corporate commitment to maintain this BPA as a corporate priority
- A description of the Quoter's communication and coordination plans, meetings, and deliverables
- A copy of the Quoter's Quality Control Plan (Provide as an appendix).

3) The Staffing Plan, at a minimum, shall address the following:

- A detailed description of the Quoter's current personnel resources for this effort, staff retention that addresses the Quoter's capabilities and experience relating to the SOW
- A description of the teaming arrangements, if any. The description shall state all team roles and responsibilities, the services to be performed by each team member. Indicate the team members(s) GSA Schedule Number
- Resumes, at a minimum, shall include a description of the experience and capability for the key personnel proposed. Descriptions shall address such items as the individual's background, work experience, and accomplishments. Show the knowledge that Contractor personnel gained through completed and ongoing efforts that are similar in nature to the requirements of the RFQ. The resumes shall be limited to three (3) pages each.

4) The Draft IT Security Plan, shall address the following:

- Details the approach, methods, and safeguards the contractor will utilize to comply with Government and DHS Information Technology security requirements.

Tab C: Categorization of Government Requirements - Requirements Identification Matrix (Evaluation Factor 4)

Quoters shall categorize their solution capabilities to the Government requirements in the Requirement Identification Matrix. Quoters shall fill in the box under the corresponding heading,

which indicates the solution capabilities. Quoters shall include the completed document in Volume II, Tab C of their quote.

Tab D: Contractor Teaming Arrangement (CTA) or GSA Prime Contractor/Subcontractors (if applicable) (Evaluation Factor 4)

1) Quoters may structure their quotation packages either as 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 the DHS. Further guidance on GSA CTAs may be found at the GSA MAS Desk Reference Section 10: Contractor Team Arrangements (CTAs).

2) 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. Each quotation submitted as a CTA shall describe the Team Leader and Team Member responsibilities in terms of receiving Orders under the BPAs, invoicing, and payment. Each quotation submitted as a CTA must include adequate Technical, and Business & Pricing information for DHS to evaluate the merits of the submission. In preparing their quote, CTA's shall follow the Instruction to Quoters for each phase. Quoters shall include CTA supporting documentation in Volume II, Tab D of their quote.

3) If a GSA Prime Contractor / Subcontractor Arrangement(s) is proposed, only the Prime Contractor must have a GSA Schedule IT 70 contract. The Prime cannot contract to offer services for which it does not hold the proper Schedule contract. GSA authorized subcontractors may fulfill requirements under the Prime Contractor's GSA Contract number and pricing table quoted in Attachment 4.

Volume III - Business & Pricing (Evaluation Factor 5) (Phase 3)

There are no page limits to Volume 3, Price Quote.

The Quoter shall prepare a Price Quotation that contains all information necessary to evaluate the prices and/or discounts (price reductions) proposed by the Quoter. Quoters shall only provide pricing for the supplies and services available on their GSA FSS 70 Information Technology contract. If the service is not available under their respective schedule contract, the Quoter shall not provide pricing for the service. The Government will not evaluate an open market item or service that is not available on the Quoter's GSA FSS 70 IT contract. The Price Quotation shall consist of SaaS subscriptions rates, fully burdened hourly rates and discounts offered. There are NO page limitations for Volume III (i.e., the price Quotation, and supporting narrative information).

Quoters shall complete all yellow highlighted areas in Attachment 4, Worksheet 1 and Worksheet 2. Failure to complete all fields will result in a non-responsive quotation. The Quoter shall not alter the formulas in any cells. The Quoter is to input the requested information in each

yellow highlighted cell. Do not add any rows or columns. Worksheets 3 will automatically populate your total evaluated price quote based on pricing information provided in Worksheet 1 and Worksheet 2.

Tab A: Quotation Cover/Transmittal Letter

Quotation Cover/Transmittal Letter (limit 2 pages); GSA Pricing Schedule; HSAR Clause 3052.209-70 (f) Disclosure; and HSAR Provision 3052.209-72 (c) Disclosure.

Tab B: Worksheet 1 Labor Descriptions (Attachment 4,)

Quoters are to propose labor categories from the Quoter's awarded GSA FSS contract that mirrors (best fit) the Government's Labor Category, Description, and Minimum Qualifications as provided on Attachment 4, Worksheet 1, Labor Descriptions. Quoters shall not change the Government Labor Category, Description, or Minimum Qualifications. Quoters shall include their GSA Schedule Labor Category, GSA Schedule Description, and GSA Schedule Qualifications and shall map all information to the Government provided Labor Descriptions. Quoters shall complete all yellow highlighted areas.

Tab C: Worksheet 2 Pricing Worksheet (Attachment 4,)

The Quoter shall complete the pricing table provided as Attachment 4: Pricing Worksheet. The Quoter shall provide a GSA rate and discount for SaaS subscriptions on the Government specified tier levels. Licensing shall be on a "named user" account basis. Quoters shall also provide fixed hourly rates and percentage discounts for the labor categories indicated in each Ordering Periods (Base and Option Year(s)). Quoters shall complete all yellow highlighted areas.

Tab D: Worksheet 3 Total Price Worksheet (Attachment 4,)

Please provide Worksheet 3. This Worksheet will automatically populate your total evaluated price quote based on the information provided in Worksheet 1 and Worksheet 2.

4.3.4 Quotation Submission

The quotation submitted shall fully comply with any and all requirements in the RFQ. The quotation shall clearly demonstrate the Quoter's understanding of the overall and specific technical requirements of the SOW. The Quoter shall provide the requested past performance and pricing information. Failure of the Quoter to address all requirements of the RFQ in their Quotation may result in the Quotation not being considered for evaluation by the Government. Clarity and completeness of the Quotation is of the utmost importance. The Quotation shall be written in a practical, clear, and concise manner. It shall use quantitative terms whenever possible and shall avoid qualitative adjectives to the maximum extent possible.

DHS requires that the Quoter submit an electronic copy of the Quotation. Electronic copies shall be formatted using Microsoft Office Version 2003 or later. Government will accept PDF files in order to not exceed the standard 5 MB individual file size limitation.

Quotations shall be legible, single-spaced, typewritten, in a font size not smaller than twelve (12) point Times New Roman. No reduction is permitted except for organization charts or other graphic illustrations. In those instances where reduction is allowable, Quoters shall ensure that the print is easily readable. Each page shall have text margins of at least one (1) inch on all sides. Header/footer information (which does not include any information to be evaluated) may be included in the margin space. Pages that exceed the maximum page limitation will not be evaluated.

Documents/materials provided for the RFQ become Government property. Quoters, may at their discretion include proprietary markings on any document/materials provided to the Government. The Government will safeguard the materials in accordance with FAR PART 3.104-4 Disclosure, Protection, and Marking of Contractor Bid or Proposal Information and Source Selection Information.

5. EVALUATION
(This section will be removed upon award.)

5.1 Introduction

This GSA Schedule BPA Request for Quotation seeks to obtain an Electronic Contract Filing System for DHS Office of the Chief Procurement Officer. DHS intends to acquire these supplies and services by establishing a single award competitive BPA to a GSA Federal Supply Schedule 70 IT contract holder. However, DHS reserves the right to increase or decrease the number of BPA awards based upon the results of the evaluation**.**

5.2 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), the Request for Quote, and the Evaluation Plan. A single award will be made to the responsible Quoter submitting an overall quote that is determined best value to the Government, price and non-price factors considered.

5.3 Evaluation Process

The Government intends to use a three (3) phased approach to evaluate Quoters under FAR 8.405-3 as follows:

1) Phase 1: The Government will consider all Quoters using Evaluation Factor 1. All Quoters that achieve a “Pass” rating for Evaluation Factor 1 will proceed to Phase 2. Those Quoters that are notified as “Fail”, shall not proceed to Phase 2.

2) Phase 2: The Government will continue its consideration by evaluating Evaluation Factor 2. All Quoters that achieve a “Pass” rating for Evaluation Factor 2 will proceed to Phase 3. Those Quoters that are notified as “Fail”, shall not proceed to Phase 3.

3) Phase 3: The Government will continue its consideration by evaluating Evaluation Factors 3, 4, and 5. Phase 3 will be rated by use of confidence levels for Factors 3 and 4. The Government intends to select the best value Quoter based on a trade-off of Evaluation Factors, 3, 4, and 5.

DHS will perform an evaluation, based on the Quoter's written Technical Information (Volume I and II), Product Demonstration, and Business & Pricing Information (Volume III), to assess the best value to the Government. The determination of best value will be made by comparing the differences in the value of the Technical Evaluation Factors (Volume II Factors 3 & 4)), with the differences in the Business & Pricing Evaluation Factor (Volume III Factor 5). Factors 3 and 4 are of relatively equal importance, and the non-price evaluation factors (when combined) are significantly more important than the price evaluation factor, Factor 5.
In making this comparison, the Government is more concerned with obtaining performance capability superiority rather than the lowest overall price. However, the Government will not

make an award at a significantly higher overall price to achieve only slightly superior performance capabilities.

As the technical evaluation of quotes approaches equality, greater will be the importance of price in making the award determination. In the event that two or more quotes are determined not to have any substantial technical differences (i.e. are technically equivalent), award may be made to the lower priced quote. It should be noted that award may be made to other than the lowest priced quote if the Government determines that a price premium is warranted due to technical merit. The Government may also award to other than the highest technically rated quotation, if the Government determines that a price premium is not warranted.

5.4 Award on Initial Quotations

The Government may award without conducting exchanges; however, the Contracting Officer (CO) reserves the right to hold exchanges with Quoters based on the content of their individual quotations. Accordingly, each initial quotation should be submitted on the most favorable price and technical terms that the Quoter can submit to the Government.

5.5 Evaluation Factors

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

- Factor 1: Technical (FedRAMP, Solution Overview, Capability Confirmation Checklist) (Volume I) (Phase 1);
- Factor 2: Technical (Product Demonstration) (Phase 2);
- Factor 3: Technical (Past Performance) (Volume II) (Phase 3);
- Factor 4: Technical (Management/Technical Approach, Categorization of Government Requirements, CTA/Subcontracting) (Volume II) (Phase 3);
- Factor 5: Business & Pricing (Volume III) including discount terms (Phase 3). Not rated.

Evaluation Factor 1: FedRAMP, Solution Overview, Capability Confirmation Checklist

The Government will evaluate documentation provided by the Quoter verifying the Cloud Hosting Environment has FedRAMP authorization at the Moderate security impact level at time of proposal.

The Government will evaluate documentation provided by the Quoter detailing the functionalities of the solution, which meets the Government's minimum capabilities: Electronic Contract Storage, Document Management, Workflow, Records Management, PIV authentication capability, Document Extraction and Redaction, and Electronic Signature.

The Government will evaluate the Quoter's Capability Confirmation Checklist ensuring it is filled out in its entirety and contains an authorized signee affirmation that the proposed solution offers the minimum capabilities as cited in the checklist.

Evaluation Factor 2: Product Demonstration

Through the demonstration, the Government intends to understand the Quoter's proposed solution and its capabilities as it relates to the Governments requirements. Further, the product demonstration will be used as an opportunity to assess the viability of an Quoter to successfully deliver the ECFS solution.

The Government will evaluate the Product Demonstration validating the proposed software solution has the capabilities of performing the elements as outlined in Evaluation Factor 2.

The Government retains the right to ask the Quoter to repeat or clarify steps during the demonstrations. This act does not constitute discussions or exchanges with Quoters.

Presenters: The Quoter's presentation team is limited to five (5) employees with no more than two (2) from the Sub-contractors. The Government requires at least one of the persons in the Product Demonstration to have a major functional role in the execution of the technical solution being proposed. Each presenter is required to carry and present a valid Government issued ID (e.g., driver's license, passport, etc.).

Evaluation Factor 3: Past Performance

The Government will assess the Quoter's past performance (as a Prime Contractor or Subcontractor) delivering a high quality, functioning electronic contract filing system to a Federal Agency to support the acquisition or procurement electronic contract filing requirements of the Federal Agency. The past performance evaluation will examine the extent to which the Quoter's past performance demonstrates their capability to deliver high quality service. Only recent (or ongoing) and relevant past performance data regarding work will be evaluated. ***Recent*** is defined as within the last three (3) years. ***Relevant*** is defined as work similar in size and scope to the work identified in the SOW.

Past Performance evaluations will be based on: (a) Quoter's quote submission identifying three (3) projects previously or currently performed; (b) Information obtained in Government past performance reference checks relevant to the project descriptions submitted as well as other inquiries on Quoter's past performance, and (c) Information obtained from Government past performance databases. Past Performance evaluations will be rated using a confidence level. A neutral rating will be provided for this Factor if the Quoter does not have recent/relevant past performance.

Evaluation Factor 4: Management/Technical Approach

The Government will evaluate the Quoters's ability to effectively perform and manage the requirements in the SOW. This assessment will consider the Quoter's use of personnel against the required tasks, management of tasks to be performed and quality control. In addition, the Quoter's ability to identify any technical barriers/difficulties and problem areas that could conceivably be encountered in accomplishing the required work and potential approaches how those barriers could be overcome. The Government will access the Quoter's Technical Approach, Management Plan, Staffing Plan, and Draft IT Security Plan to determine the extent to which it demonstrates a comprehensive, sound, and reasonable method to fulfilling the requirements as described in the SOW. The Government will evaluate the Quoter's capabilities

submission to meeting the Governments capability requirements of the Requirements Identification Matrix. The Government will consider the capabilities of the proposed solution meeting Government requirements and the risk involved of requiring additional work or enhancements to meet Government needs. The Government will evaluate Quoters quotes for CTA and subcontracting, validating documentation and quoted methods of accomplishing the tasks in the SOW.

Evaluation Factor 5: Business & Pricing (Volume III) including Discount Terms (Not Rated)

The Government will evaluate the Quoter's Labor Description, Pricing, and Total Price provided in Attachment 4. The evaluation will assess the accuracy, completeness, GSA schedule pricing, discounts offered (price reduction), and reasonableness. The total evaluated price, including the base and four options, will be used in price analysis to determine reasonableness. This process involves comparison of competitive quotes for supplies and services, verification that prices are included for all RFQ requirements, figures are correctly calculated, and prices are presented in an adequate format. Quoters are encouraged to propose price reductions from their GSA Schedule contract.

Pricing will be used to establish the BPA level evaluated price. The established BPA will include SaaS Subscription tiered level pricing, and fixed hourly labor rates for all services and subsequent orders under the BPA. The Quoter is required to submit pricing data in the formats indicated in Attachment 4, Pricing of the RFQ.

Appendices

Appendix A	Requirements Identification Matrix
Appendix B	Contract Checklists

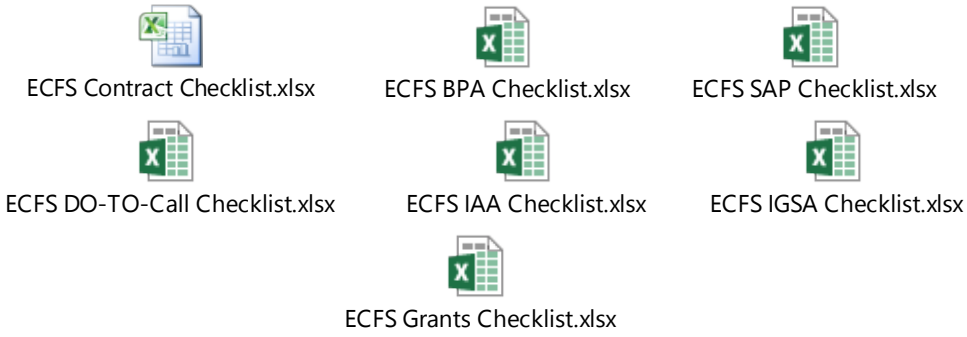
Appendix A – Requirements Identification Matrix

Appendix B – Contract File Checklists

The Checklists in this Appendix represent the checklists most commonly used by DHS 1102s. The checklist entitled "Contract Checklist" encompasses all documents required in a contract file. The other checklists contain a subset of the documents in the Contract Checklist. As described in the requirements listed in Appendix A, the solution shall allow users to select optional documents for the checklist. The solution should not allow them to remove the documents marked as mandatory.

The tab at the top of each worksheet represents the top-tier tab that appears in the contract file. There are six top tier tabs in every contract file (Pre-Solicitation, Solicitation, Pre-Award, Award, Contract Administration, and Contract Closeout). The subtabs are the tabs that appear beneath the top tier tabs (e.g., purchase request documentation, market research, small business review, etc.). There can be multiple documents stored under a subtab. The subtabs can also remain empty until the 1102 has a document that is ready to be stored.

The contractor shall address the seven (7) attachments associated with this Appendix B.



ATTACHMENTS

Attachment 1:	Capability Confirmation Checklist (1 page)
Attachment 2:	Past Performance Information Form (3 pages)
Attachment 3:	Labor Category Descriptions and Qualifications (3 pages)
Attachment 4:	ECFS Pricing Workbook (3 pages)
Attachment 5	ECFS Quoter Questions and Responses

Attachment 1
Capability Confirmation Checklist

Capability
Confirmation Check

Attachment 2
Past Performance Information Form

(Quoters are required to complete this form and shall identify three (3) separate relevant contracts/projects)

Quoter:	
Company Group / Division:	
Program, Project, Or Task	

REFERENCE INFORMATION

1	Customer Name:		
2	Address:		
	Customer Info:	**Contracting Contact**	**Program / Project Manager or COR**
3	Name & Title:		
4	Organization:		
5	Address:		
5	Phone No.:		
6	Fax No.:		
7	E-mail:		
8	Contract Number:		
	Past Performance Information Retrieval System (PPIRS) Record Available?		
9	Contract Type (e.g. contract, BPA, task order) and pricing type (e.g. fixed price, cost reimbursement):		

10	Dollar Value (Not-to Exceed):	
	Cumulative funded amount:	
11	Project Start Date	
	Estimated/Actual Completion Date:	
12	Current status, e.g. completed and/or in progress	
Description of Work Performed and Relevance to Requirements in this RFQ		
Problems Encountered and Resolutions		

Attachment 3
Labor Category Descriptions and Qualifications

Project Manager

Duties: Responsible for project and task management throughout all phases of the Electronic Contract Filing System. Technical and business job functions include but are not limited to; the management of overall project/task schedules, funding vs. cost allocation, tasks completion status, resource allocations, routine oral and written communication regarding project/task status and all other duties typical to the deployment of complex automated systems, developing and implementing sustaining operating procedures in support of knowledge capture and management, and other management information skills. Reports in writing and orally to contractor management and government representatives, including the government contracting officer.

Skill Level:

- A minimum of 5 years of experience managing projects of comparable size and complexity.
- A minimum of two years of experience managing projects to implement the solution proposed.

Minimum Qualifications: Bachelor's degree in a related discipline from an accredited college or university and five (5) years of management and supervisory experience including performance in program management functions.

Contract Subject Matter Expert

Duties: Provide technical, managerial, and administrative direction for problem definition, analysis, requirements development, and implementation of complex solutions by making information technology/information management related recommendations. In-depth understanding of the contract filing process, the contract file lifecycle, and the documentation that constitutes the contract file.

Skill Level:

- A minimum of five years of experience in the federal procurement operations process.
- A minimum of one year of experience implementing and maintaining document management systems.
- In-depth understanding of the contract filing process, the contract file lifecycle, and the documentation that constitutes the contract file.

Attachment 3
Labor Category Descriptions and Qualifications

Minimum Qualifications: Bachelor's degree in a related discipline from an accredited college or university and five (5) years of professional experience in federal procurement operations.

Systems Analyst

Duties: Manage and analyze user needs, determine functional and cross-functional requirements. Perform functional allocation to identify required tasks and their interrelationships. Assist in the development of functional requirements and creation of functional specifications. Assist in the development and documentation of technical system design. Design, and configure Document Management and/or Records Management Systems. Senior level experience in the design, development, implementation, maintenance and operation of technology and business solutions; functional analysis of business and technology customer needs; and providing expert advice regarding integration, testing and troubleshooting solution issues.

Skill Level:

- Extensive experience developing functional requirements and creating functional and technical specifications
- Senior level experience in applying any of the disciplines of planning, analysis, design, development (configure/coding) and implementation of complex system information (infrastructure, network and application) projects.
- Senior level experience in the design, development, implementation, maintenance and operation of technology and business solutions; functional analysis of business and technology customer needs; and providing expert advice regarding integration, testing and troubleshooting solution issues.

Minimum Qualifications: Bachelor's degree in a related discipline from an accredited college or university and three (5) years of professional experience in an information technology/information management or related field.

Database Administrator

Duties: Provides technical expertise and guidance in the logical and physical database design, development, operation, and maintenance of information systems for business processing applications. Ability to formulate specifications for computer programmers to use in coding, testing, and debugging of computer software. Very knowledgeable in both commercially-

Attachment 3
Labor Category Descriptions and Qualifications

available-off-the-shelf (COTS) and custom database software platforms, and develops technical documentation detailing the installation procedures.

Skill Level:

- At least 6 years of experience in database management systems
- Minimum 3 years of relevant programming experience in a batch or online environment
- Ability to formulate specifications for computer programmers to use in coding, testing, and debugging of computer software.
- Very knowledgeable in both commercially available off- the-shelf (COTS) and custom database software platforms; and develops technical documentation detailing the installation procedures.

Minimum Qualifications: Advanced degree or equivalent training and experience in computer science, information systems, engineering, or related areas with specific training in database management systems.

At least 6 years of experience in database management systems.

Technical Writer

Duties: Develop user, reference and procedure manuals. Design and maintain written style guides and templates for various documents. Provide management reports and updates on project status. Ensures technical documentation is accurate, complete, meets editorial and government specifications and adheres to standards for quality, graphics, coverage, format, and style.

Skills:

- 2-5 years of experience as a Technical Writer in a related project
- High level of expertise in word processing packages including Microsoft Word

Minimum Qualifications: Bachelor's degree in related discipline from an accredited college or university and two (2) or more years of technical writing or related experience.

Help Desk Specialist

Duties: Provides telephone support to users for the software application deployed under this contract. Monitor and respond quickly and effectively to requests received through the IT

Attachment 3 *Labor Category Descriptions and Qualifications*
helpdesk. Answers user's calls and records all necessary information. Offers assistance over the phone and follows the problem through to resolution. Assigns problems to the appropriate area for resolution. Logs and reports data on the number and types of calls received. **Skill Level**: • Experience in hardware, software, network troubleshooting, basic operating system functionality or equivalent training and/or education
Minimum Qualifications: Bachelor's Degree or equivalent and 6 years of general experience

Attachment 4
Pricing Workbook

ECFS Pricing Worksheet.xlsx

Attachment 5

ECFS Quoter Questions and Responses

ECFS Quoter
Questions and Respor