

From: Fisher, George
To: [Shulman, Stu](#)
Cc: [Rosslyn Murphy](#); [Barnett, Teri](#); [Cash, Marcia](#); [Bowman, Randal](#)
Subject: D17PD00803 Software Licenses and DiscoverText Administrative Support
Date: Tuesday, May 23, 2017 12:26:18 PM
Attachments: [D17PD00803.pdf](#)

Good Afternoon Dr. Shulman,

Attached is the fully executed task order for the software licenses and administrative support.

I will follow up with a Contracting Officers Representative (COR) appointment letter and a Government Representative (GR) appointment letter for your signature and return in a couple of hours.

Rosslyn Murphy will be appointed as the COR; she is cc'd. The COR approves all invoices and has authority over the GR.

Marcia Cash will be appointed as the GR and she is also cc'd. The GR is responsible for the daily task order management and is your primary contact. The GR is responsible for all technical aspects of the task order.

The COR and GR will work together for all invoice approvals with the GR communicating to the COR that the invoiced licenses or labor hours are correct and the invoice is okay to pay.

I have also included Teri Barnett and Ron Bowman in this correspondence so that everyone has a copy of the task order and all are aware of roles assigned.

Once the software licenses are delivered, you may invoice for them through IPP.

The labor hour contract lines (lines 030 and 040) may be invoiced when you feel it is appropriate, though once a month is preferred.

If you have any questions, please do not hesitate to contact me at the numbers below.

Thank you for your support to the Department of the Interior.

George Fisher
Contract Specialist

- Telework every Friday
- Scheduled Leave: 6/5/17 - 6/9/17

Acquisition Services Directorate
Interior Business Center
(703) 964-4815 (Office) Herndon
(571) 328-9671 (Cellphone)
(202) 208-1751 (Office) DC
George_Fisher@ibc.doi.gov
US Department of the Interior
Office of the Secretary

doi.gov/ibc

Your Focus: Your Mission
Our Focus: You

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1

25

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER 05/23/2017		2. CONTRACT NO. (If any) GS 35F 002CA		6. SHIP TO: a. NAME OF CONSIGNEE DOI SECRETARY'S IMMEDIATE OFFICE	
3. ORDER NO. D17PD00803		4. REQUISITION/REFERENCE NO. 0040336889		b. STREET ADDRESS 1849 C St NW MS 6129	
5. ISSUING OFFICE (Address correspondence to) Interior Business Center, AQD Division 1/ Branch 3 381 Elden St Suite 4000 Herndon VA 20170				c. CITY Washington	e. ZIP CODE 20240-0001
7. TO: ATTN GOVERNMENT POC				f. SHIP VIA	
a. NAME OF CONTRACTOR TEXIFTER, LLC				8. TYPE OF ORDER	
b. COMPANY NAME				<input type="checkbox"/> a. PURCHASE REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any including delivery as indicated.	
c. STREET ADDRESS 237 SHUTESBURY RD.				<input checked="" type="checkbox"/> b. DELIVERY Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	
d. CITY AMHERST		e. STATE MA	f. ZIP CODE 01002-1267		
9. ACCOUNTING AND APPROPRIATION DATA See Schedule				10. REQUISITION NG OFFICE DOI SECRETARY'S IMMEDIATE OFFICE	

11. BUSINESS CLASSIFICATION (Check appropriate box(es)) <input checked="" type="checkbox"/> a. SMALL <input type="checkbox"/> b. OTHER THAN SMALL <input type="checkbox"/> c. DISADVANTAGED <input type="checkbox"/> d. WOMEN-OWNED <input type="checkbox"/> e. HUBZone <input type="checkbox"/> f. SERVICE-DISABLED VETERAN-OWNED <input type="checkbox"/> g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM <input type="checkbox"/> h. EDWOSB				12. F.O.B. POINT Destination	
13. PLACE OF a. INSPECTION Destination		b. ACCEPTANCE Destination		14. GOVERNMENT B/L NO.	
				15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) 08/23/2017	
				16. DISCOUNT TERMS ACCP	

7 SCHEDULE (See reverse for Rejection)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	This is a hybrid task order - Invoice Review Required Y Continued					

SEE BILLING INSTRUCTIONS ON REVERSE	18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)		
	21. MAIL INVOICE TO:								
	a. NAME Invoice Processing Platform System						\$13,850.00		
	b. STREET ADDRESS (or P.O. Box) US Department of Treasury http://www.ipp.gov								
c. CITY						d. STATE	e. ZIP CODE	\$13,850.00	17(i) GRAND TOTAL

22. UNITED STATES OF AMERICA BY (Signature)

23. NAME (Typed)
George Fisher
TITLE: CONTRACTING/ORDER NG OFFICER

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
2

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 05/23/2017	CONTRACT NO. GS-35F-002CA	ORDER NO. D17PD00803
-----------------------------	------------------------------	-------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Admin Office: DOI, Interior Business Center, AQD Division 1/Branch 3 381 Elden St Suite 4000 Herndon VA 20170 Period of Performance: 05/24/2017 to 08/23/2017					
00010	1 Enterprise Seat 3 months Accounting Info: 01 Account Assignm: K G/L Account: 6100.233N0 Business Area: D000 Commitment Item: 233N00 Cost Center: DS10100000 Functional Area: DLSN00000.000000 Fund: 178D0102DM Fund Center: DS10100000 Project/WBS: DX.10101 PR Acct Assign: 01 Funded: \$5,640.00				5,640.00	
00020	13 professional Seats 3 months Accounting Info: 01 Account Assignm: K G/L Account: 6100.233N0 Business Area: D000 Commitment Item: 233N00 Cost Center: DS10100000 Functional Area: DLSN00000.000000 Fund: 178D0102DM Fund Center: DS10100000 Project/WBS: DX.10101 PR Acct Assign: 01 Funded: \$2,420.00				2,420.00	
00030	Project Manager 3 months In accordance with SOW entitled DiscoverText Assistance dated 4/16/17 Accounting Info: Continued ...				3,290.00	

TOTAL CARR ED FORWARD TO 1ST PAGE (ITEM 17(H))

\$11,350.00

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 348 (Rev. 4/2006)
Prescribed by GSA FAR (48 CFR) 53.213(f)

DOI-2018-07 01461

ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION

PAGE NO
3

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

DATE OF ORDER 05/23/2017	CONTRACT NO. GS-35F-002CA	ORDER NO. D17PD00803
-----------------------------	------------------------------	-------------------------

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
00040	<p>01 Account Assignm: K G/L Account: 6100.252K0 Business Area: D000 Commitment Item: 252K00 Cost Center: DS10100000 Functional Area: DLSN00000.000000 Fund: 178D0102DM Fund Center: DS10100000 Project/WBS: DX.10101 PR Acct Assign: 01 Funded: \$3,290.00</p> <p>Grad Students Labor Hours 3 months In accordance with SOW entitled DiscoverText Assistance dated 4/16/17.</p> <p>Accounting Info: 01 Account Assignm: K G/L Account: 6100.252K0 Business Area: D000 Commitment Item: 252K00 Cost Center: DS10100000 Functional Area: DLSN00000.000000 Fund: 178D0102DM Fund Center: DS10100000 Project/WBS: DX.10101 PR Acct Assign: 01 Funded: \$2,500.00</p> <p>The total amount of award: \$13,850.00. The obligation for this award is shown in box 17(i).</p>				2,500.00	

TOTAL CARR ED FORWARD TO 1ST PAGE (ITEM 17(H))

\$2,500.00

SECTION 1 GOVERNMENT REPRESENTATIVE & INVOICING

This award D17PD00803 is issued subject to the terms and conditions of the FAR clauses and agency incorporated Clauses, as listed below.

Contract Administration/Government Points of Contact

(a) The Government's Contracting Officer (CO) and Contract Specialist/Administrator (CS/CA) for this project are:

George Fisher
Contracting Officer
U.S. Department of the Interior
Interior Business Center, Acquisition Services Directorate
381 Elden St Ste 4000
Herndon, VA 20170
Phone Number: 703-964-4815
Email: george_fisher@ibc.doi.gov

(b) The Government's Representative (GR) for this project is:

Marcia Cash
Government Technical Representative
U.S. Department of the Interior
U.S. Fish and Wildlife Service
5275 Leesburg Pike, MS: BPHC
Falls Church, VA 22041-3808
Phone: 703-358-2013
Email: marcia_cash@fws.gov

(c) The Contracting Officer Representative (COR) for this project is:

Rosslyn Murphy
Contracting Officer Representative (Invoice Approval Only)
U.S. Department of the Interior
Interior Business Center, Acquisition Services Directorate
381 Elden St Ste 4000
Herndon, VA 20170
Phone: 202-208-6654
Email: rosslyn_murphy@ibc.doi.gov

SECTION 2 – TASK ORDER CLAUSES:

All contractual terms and conditions contained in supplier's GSA Schedule GS-35F-002CA are incorporated herein by reference and made a part of this Task Order by reference herein.

2.1 Additional FAR Clauses Required by Statute:

FAR 52.217-8 OPTION TO EXTEND SERVICES—(NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor 7 days before the contract expires

(End of Clause)

52.224-3 Privacy Training (JAN 2017)

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

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

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

(c)(1) Privacy training shall address the key elements necessary for ensuring the safeguarding of personally identifiable information or a system of records. The training shall be role-based, provide foundational as well as more advanced levels of training, and have measures in place to test the knowledge level of users. At a minimum, the privacy training shall cover—

- (i) The provisions of the Privacy Act of 1974 (5 U.S.C. 552a), including penalties for violations of the Act;
- (ii) The appropriate handling and safeguarding of personally identifiable information;
- (iii) The authorized and official use of a system of records or any other personally identifiable information;
- (iv) The restriction on the use of unauthorized equipment to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise access personally identifiable information;
- (v) The prohibition against the unauthorized use of a system of records or unauthorized disclosure, access, handling, or use of personally identifiable information; and
- (vi) The procedures to be followed in the event of a suspected or confirmed breach of a system of records or the unauthorized disclosure, access, handling, or use of personally identifiable information (see OMB guidance for Preparing for and Responding to a Breach of Personally Identifiable Information).

(2) Completion of an agency-developed or agency-conducted training course shall be deemed to satisfy these elements.

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

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or

otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

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

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

(End of clause)

Alternate I (JAN 2017). As prescribed in 24.302(b), if the agency specifies that only its agency-provided training is acceptable, substitute the following paragraph (c) for paragraph (c) of the basic clause:

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract.

End of Clause

52.239-1 Privacy or Security Safeguards (Aug 1996)

(a) The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government.

(b) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

(c) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

(End of clause)

2.2 Additional Agency Clauses

DIAR 1452.201-70 Authorities and Delegations (Sep 2011)

The Contracting Officer is the only individual authorized to enter into or terminate this contract, modify any term or condition of this contract, waive any requirement of this contract, or accept nonconforming work.

(a) The Contracting Officer will designate a Contracting Officer's Representative (COR) at time of award. The COR will be responsible for technical monitoring of the contractor's performance and deliveries. The COR will be appointed in writing, and a copy of the appointment will be furnished to

the Contractor. Changes to this delegation will be made by written changes to the existing appointment or by issuance of a new appointment.

(b) The COR is not authorized to perform, formally or informally, any of the following actions:

- (1) Promise, award, agree to award, or execute any contract, contract modification, or notice of intent that changes or may change this contract;
- (2) Waive or agree to modification of the delivery schedule;
- (3) Make any final decision on any contract matter subject to the Disputes Clause;
- (4) Terminate, for any reason, the Contractor's right to proceed;
- (5) Obligate in any way, the payment of money by the Government.

(c) The Contractor shall comply with the written or oral direction of the Contracting Officer or authorized representative(s) acting within the scope and authority of the appointment memorandum. The Contractor need not proceed with direction that it considers to have been issued without proper authority. The Contractor shall notify the Contracting Officer in writing, with as much detail as possible, when the COR has taken an action or has issued direction (written or oral) that the Contractor considers to exceed the COR's appointment, within 3 days of the occurrence. Unless otherwise provided in this contract, the Contractor assumes all costs, risks, liabilities, and consequences of performing any work it is directed to perform that falls within any of the categories defined in paragraph prior to receipt of the Contracting Officer's response issued under paragraph (e) of this clause.

(d) The Contracting Officer shall respond in writing within 30 days to any notice made under paragraph (d) of this clause. A failure of the parties to agree upon the nature of a direction, or upon the contract action to be taken with respect thereto, shall be subject to the provisions of the Disputes clause of this contract.

(e) The Contractor shall provide copies of all correspondence to the Contracting Officer and the COR.

(f) Any action(s) taken by the Contractor, in response to any direction given by any person acting on behalf of the Government or any Government official other than the Contracting Officer or the COR acting within his or her appointment, shall be at the Contractor's risk.

(End of clause)

DOI-AAAP-0028, Electronic Invoicing and Payment Requirements - Invoice Processing Platform (IPP) (April 2013) V2

Payment requests must be submitted electronically through the U. S. Department of the Treasury's Invoice Processing Platform System (IPP).

"Payment request" means any request for contract financing payment or invoice payment by the Contractor. To constitute a proper invoice, the payment request must comply with the requirements identified in the applicable Prompt Payment clause included in the contract, or the clause 52.212-4 Contract Terms and Conditions – Commercial Items included in commercial item contracts. The IPP website address is: <https://www.ipp.gov>.

Under this contract, the following documents are required to be submitted as an attachment to the IPP invoice:

The contractor shall submit invoices once per month for Labor Hour or Time-and-Materials Line Items. Copies of the invoice with support documentation shall also be sent through electronic email to the Contracting Officer's Representative (COR) and Contracting Officer(CO).

Additional supporting documentation MAY BE REQUESTED at the discretion of the COR.

Invoices shall be submitted upon completion of the Labor Hour or Time-and-Materials month, and upon completion of the travel, all within the month being invoiced.

Travel invoiced must include the name of the traveler, travel itinerary, purpose of travel (event, exercise, workshop, etc), and any other documentation requested by the COR/CO for Finance/Administration. The contractor will be reimbursed for actual, allowable, allocable, and reasonable travel costs incurred during performance of this requirement in accordance with the Federal Travel Regulations currently in effect on date of travel. Receipts are required for all lodging and any expenditure exceeding \$75.00. A copy of the approved travel request form shall be attached for reference.

The contractor is responsible for ensuring invoices submitted are accurate and complete and are in accordance with federal guidelines, the Federal Travel Regulation (FTR) and other Government mandates and directives.

The contractor agrees to include the following information on each invoice:

1. Name and address of the Contractor
2. Invoice number and date
3. Task Order number and date
4. Period of performance for the billing cycle
5. Payment terms
6. Name, title, phone number, e-mail address, and mailing address of person to be notified in the event of a defective invoice
7. Other substantiating documentation or information as required by the TO
8. Time-and-Materials and/or Labor Hour (LH) Line Items: As a minimum, the following information for each individual:
 - a. Name
 - b. Billing Period Covered for services performed
 - c. Productive Direct Labor Hours
 - d. Labor Category
 - e. Hourly Rate
 - f. Total Dollar Amount
 - g. Security Designation
 - h. On-Site/Off-Site designation
 - i. Cumulative Hours
 - j. Not-to-Exceed Hours
9. Any Travel or Other Direct Costs (ODC's) (including supporting documentation/receipts of all other charges) for the current billing period and cumulative to date. A copy of the approved Travel Authorization Form shall be attached for reference.

FINAL INVOICE:

1. Within sixty calendar days of product acceptance and/or completion of services:

- a. The contractor shall submit a final invoice, designated as such by a clear statement of "FINAL INVOICE" on the face of the invoice document.
- b. The contractor shall provide a certificate of completion which certifies all goods and service have been provided as required by this Order.
- c. The contractor shall provide a release of claims against the government for any further payment under this Order.

The sixty calendar day submission timeframe shall not be extended without written authorization from the contracting officer. In the event items a, b, or c above are not submitted within the authorized timeframe, the contracting officer may make final cost determinations in order to make final payment and close out the contract unilaterally.

The Contractor must use the IPP website to register, access and use IPP for submitting requests for payment. The Contractor Government Business Point of Contact (as listed in SAM) will receive enrollment instructions via email from the Federal Reserve Bank of Boston (FRBB) within 3 – 5 business days of the contract award date. Contractor assistance with enrollment can be obtained by contacting the IPP Production Helpdesk via email ippgroup@bos.frb.org or phone (866) 973-3131.

If the Contractor is unable to comply with the requirement to use IPP for submitting invoices for payment, the Contractor must submit a waiver request in writing to the Contracting Officer with its proposal or quotation.

(End of Local Clause)

INTERNET PROTOCOL Version 6 (June 2012)

- (a) Any system hardware, software, firmware and/or networked component (voice, video or data) developed, procured, or acquired in support and/or performance of this contract shall be capable of transmitting, receiving, processing, forwarding and storing digital information across system boundaries utilizing system packets that are formatted in accordance with commercial standards of Internet Protocol (IP) version 6 (IPv6) as set forth in the USGv6 Profile (NIST Special Publication 500-267) and corresponding declarations of conformance defined in the USGv6 Test Program. In addition, this system shall maintain interoperability with IPv4 systems and provide at least the same level of performance and reliability capabilities of IPv4 products.
- (b) Specifically, any new IP product or system developed, acquired, or produced must:
 - 1) Interoperate with both IPv6 and IPv4 systems and products, and
 - 2) Have available contractor/vendor IPv6 technical support for development and implementation and fielded product management.
- (c) As IPv6 evolves, the Contractor commits to upgrading or providing an appropriate migration path for each item developed, delivered or utilized at no additional cost of the Government. The Contractor shall retrofit all non-IPv6 capable equipment, as defined above, that is fielded under this contract with IPv6 capable equipment, at no additional cost to the Government.
- (d) The contractor shall provide technical support for both IPv4 and IPv6.
- (e) Any system or software must be able to operate on networks supporting IPv4, IPv6, or one that supports both.

(f) Any product whose non-compliance is discovered and made known to the Contractor within one year after acceptance shall be upgraded, modified, or replaced to bring it into compliance at no additional cost to the Government.

(End of Clause)

END OF CLAUSES

ENCLOSURE:

Attachment 1: Statement of Work

ATTACHMENT 1: STATEMENT OF WORK

Office of the Secretary (IOS)
DiscoverText Assistance Services
April 16, 2017

I. INTRODUCTION

The Department of the Interior (DOI) needs assistance with comment management for a Notice published in the Federal Register on May 11, 2017. The Notice has two separate comment periods. The first comment period ends on May 26, 2017, and the second comment period ends on July 10, 2017. The Department of the Interior expects to receive a large number of public comments beginning immediately for both comment periods and requires support organizing and reviewing these comments.

II. OBJECTIVE

DOI needs to purchase licenses for DiscoverText software and program management support to analyze comments to the posting in the Federal Register.

III. REQUIREMENTS

The Department of the Interior (DOI) will utilize DiscoverText contracted licenses and software to analyze the comments, but requires additional contract support to facilitate organizing, reviewing, and analyzing the public comments received. Below is a brief summary of the requirements:

This initiative includes:

- Assisting DOI Subject Matter Experts (SMEs) in the planning and deployment of comment review.
- Providing graduate students to prepare the preliminary data at the vendor's direction and sorting multiple iterations of bulk extract records from the Federal Docket Management System (FDMS).
- Briefing and training DOI Subject Matter Experts on best practice approaches to developing coding protocols to organize the records contained in bulk extracts.
- Ensuring proper and continuous functioning of DiscoverText throughout the project including the following.
 - Upload FDMS Bulk Extracts into DiscoverText.
 - To keep up with the workload, bulk extracts will be provided multiple times per week. The vendor will prepare "buckets" and "datasets" from these extracts making sure there are no omissions or overlaps. Deduplication should be performed on each extract.
 - Vendor will manage DOI user credentials, granting access to DiscoverText as requested by DOI.
 - The vendor will provide guidance on best practices for creating and using "buckets" to achieve the desired analysis ability.
 - The vendor will advise DOI on nomenclature of "buckets" and "datasets", and any other relevant subsets, so SMEs understand where their records can be found.

- The goal of this pre-processing work is that the “starting point” for the SMEs is only to open the dataset assigned to that person and begin coding.
- Vendor will also provide guidance on the most efficient use of DiscoverText, including identifying where “annotations” made by all SMEs can be found, how to add/edit codes, and any other DiscoverText tool that will assist the effort.
- Once the records are coded, Vendor will assist in preparing management reports.

Non Personal Services Contract

This is a “non-personal services Task Order, it is therefore, understood and agreed that the Contractor and/or the Contractor’s employees shall: (1) perform the services specified herein as independent Contractors, not as employees of the Government; (2) be responsible for their own management and administration of the work required and bear sole responsibility for complying with any and all technical, schedule, or financial requirements or constraints attendant to the performance of this Task Order; (3) be free from supervision or control by any Government employee with respect to the manner or method of performance of the services specified; and (4) pursuant to the Government’s right and obligation to inspect, accept or reject the work, comply with such general direction of the Contracting Officer, or the duly authorized representative as is necessary to ensure accomplishment of the Task Order objectives.

The Contractor shall include this provision in all subcontracts for Contractor support services under this Task Order.

CONFLICT OF INTEREST, ORGANIZATIONAL AND CONSULTANT CONFLICTS OF INTEREST

It is the Department of the Interior’s policy to avoid situations in the procurement process where, by virtue of work or services performed for DOI, or as the result of data acquired from DOI, or from industry, a particular company:

- a) Is given unfair competitive advantage over the companies in respect to future DOI business;
- b) Is placed in a position to affect Government actions under circumstances in which there is danger that the company’s judgment may be biased; or
- c) Otherwise finds that a conflict exists between the performance of work or devices for Government in an impartial manner and the company’s self-interest.
- d) If the Contractor has reason to believe that a task assigned by the Contracting Officer or a task being performed by the Contractor violates this policy, the Contractor shall promptly notify the Contracting Officer and state the reasons why a conflict of interests exists, or may appear to exist. After receiving such notice the Contracting Officer shall promptly inform the Contractor whether it should begin, or continue, the assigned task.

ORGANIZATIONAL AND CONSULTANT CONFLICTS OF INTEREST

- a) It is recognized by the parties hereto that the requirement performed by the contractor under this contract is of a nature that it creates a potential organizational conflict of interest as contemplated under FAR Subpart 9.5.

b) In the performance of this contract, the contractor may have access to data which is procurement sensitive or is proprietary to other companies, Government consultants or advisors, or the Government. The contractor agrees that it will not utilize such procurement sensitive or proprietary data in performance of future competitive contracts, for studies in the same field. The contractor further agrees not to act as a subcontractor or consultant to any other prime contractor or subcontractor seeking to utilize such data.

c) The contractor agrees to insert provisions which shall conform substantially to the language of paragraphs a) and b) in every first tier subcontract or consultant agreement for performance of any portion of this requirement.

The Contractor warrants that, to the best of the Contractor's knowledge and belief, there are no relevant facts or circumstances which would give rise to an organizational conflict of interest, as defined in FAR Subpart 9.5, or that the Contractor has disclosed all such relevant information.

The Contractor agrees that if an actual or potential organizational conflict of interest is discovered after award, the Contractor will make a full disclosure in writing to the Contracting Officer. This disclosure shall include a description of actions which the Contractor has taken or proposes to take, after consultation with the Contracting Officer, to avoid, mitigate, or neutralize the actual or potential conflict.

Remedies - The Contracting Officer may terminate this contract action for convenience, in whole or in part, if it deems such termination necessary to avoid an organizational conflict of interest. If the Contractor was aware of a potential organizational conflict of interest prior to award or discovered an actual or potential conflict after award and did not disclose or misrepresented relevant information to the Contracting Officer, the Government may terminate the contract for cause or default, debar the Contractor for Government contracting, or pursue such other remedies as may be permitted by law or this contract.

CONFIDENTIALITY AND NON-DISCLOSURE

All information regarding the work products developed and made available to the contractor under the contract and resulting contracts must be regarded as sensitive information by the contractor and not be disclosed or used in any other way than on the performance of this contract to anyone outside the contractor's organization without the written permission of the Government.

All contractor personnel shall sign a non-disclosure agreement and organizational conflict of interest (OCI) certification. The contractor shall take all reasonable precautions not to divulge information about the requirement and/or use this information for the contractor's gain and shall not divulge any information to any other organization (outside the IBC) without written permission from the Government. Non-Disclosure Statements and Organizational Conflict of Interest (OCI)

Section 508 Applicable Standards

The resources acquired in this investment must meet all applicable standards established by the Access Board in 36 CFR Part 1194, including technical, functional performance, information, documentation, and support standards. The products, services, information and data that are

provided to the Government or the public as a result of this acquisition shall afford individuals with disabilities access comparable to that afforded to individuals without disabilities.

- Standards applicable to this acquisition include:
- Software Applications and Operating Systems 1194.21
- Web-based Intranet and Internet Information and Applications 1194.22
- Telecommunications Products 1194.23
- Video or Multimedia Products 1194.24
- Self-Contained, Closed Products 1194.25
- Desktop and Portable Computers 1194.26
- Functional performance criteria 1194.31
- Information, Documentation, and Support 1194.41

The full text of the above referenced standards can be found at: <http://www.section508.gov>.

IV. REQUIREMENT FOR PROTECTING SENSITIVE INFORMATION

Applicability

This document applies to the Contractor, its subContractors, and Contractor personnel (hereafter referred to collectively as “Contractor”). The Contractor shall insert the substance of the requirements contained in this document in all subcontracts. This document addresses specific Department of the Interior (DOI) requirements in addition to those included in the Federal Acquisition Regulation (FAR), Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. Chapter 35), Privacy Act of 1974 (5 U.S.C. 552a, as amended), Federal Records Act (44 U.S.C. Chapter 31), Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), Health Insurance Portability and Accountability Act of 1996 (HIPAA, Pub. L. 104-191, 110 Stat. 1936), Sarbanes-Oxley Act of 2002 (SOX, Pub. L. 107-204, 116 Stat 745), Office and Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, and other laws, mandates, or executive orders pertaining to the development and operations of information systems and the protection of sensitive information and data. The following should not be construed to alter or diminish civil and/or criminal liabilities provided under various laws or mandates.

Authorization to Use, Store, or Share Sensitive Information

(a) Information created, collected, used, processed, stored, maintained, disclosed, or otherwise disposed of by the Contractor in the performance of this contract shall be accessed, transferred, stored or processed only within the sole jurisdiction of the United States Federal Government. The Contractor shall not host any portion of the information, data, information system, infrastructure, or environment in facilities outside the contiguous United States, Alaska, Hawaii, and other U.S. Territories.

(b) The primary locations shall be the main and backup data centers located within the sole jurisdiction of the United States Federal Government.

(c) In addition, other sites include the location of the Contractor support teams who provide support to the Government in resolving issues involving the task order solution, locations where

backup or archiving facilities may be agreed to by the Government, or sites where antivirus and other security scans are performed.

(d) The Contractor shall comply and agree to at all times to protect the Government's information and data in accordance with the terms of this contract. The data that is processed, maintained, or stored by the Contractor shall be protected against unauthorized access, disclosure or modification, theft, or destruction.

(e) Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Contracting Officer (CO).

(f) The preparation of the deliverables in this contract will be completed at a Controlled Unclassified Information (CUI) level and shall not be shared with any other organization without prior approval from the DOI CO.

(g) The Contractor, and any sub-Contractors, shall not use any Personally Identifiable Information (PII), E-mail Groups, Lists, or contract information for any purpose other than those activities necessary for the performance of this contract.

(h) Written approval by the Chief Information Officer (CIO), or delegate, is required prior to the use or storage of DOI Sensitive Information or sharing of DOI Sensitive Information by the Contractor with any sub-Contractor, person, or entity other than DOI.

(i) The Contractor shall not remove Sensitive Information from approved DOI location(s), electronic device(s), or other container(s), without prior written approval of the DOI CIO, or designate.

(j) Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the terms and conditions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its sub-Contractors shall be under the supervision of the Contractor or the Contractor's responsible employees. The Contractor agrees to assume responsibility for protecting the confidentiality of Government records, which are not public information. Each Contractor or employee of the Contractor to whom information may be made available or disclosed shall be notified in writing by the Contractor that such information may be disclosed only for a purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

The Contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The Service Provider (SP) shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as CUI. It is anticipated that this information will be gathered, created, and stored within the primary work location. If SP personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The use of any

information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act information.

CUI data and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The SP shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*.

The disposition of all information will be at the written direction of the COR. The COR must consult with the POR who in turn must also consult with the appropriate cognizant Records Officer to help ensure appropriate measures have been taken by the SP to ensure that records are preserved and disposed of in accordance with Federal government-wide policy and DOI standards and requirements. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

The data that is processed and stored by the various applications within the network infrastructure may contain financial data as well as personally identifiable information (PII). This data and PII, in addition to all other types of CUI and sensitive information, shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The Contractor shall ensure that the facilities that house the network infrastructure are physically secure.

The data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The SP shall provide requested data at no additional cost to the Government.

Mandatory Requirement for Contractor Return of all DOI and DOI-Activity-Related Information

The disposition of all information will be at the written direction of the COR. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(a) Within thirty (30) days after the end of the contract performance period or after the contract is suspended or terminated by DOI or by the Contractor for any reason, the Contractor must return all original (and at least one duplicate copy of those information types specified by DOI) of all DOI-provided and DOI-Activity-Related Information, (including but not limited to all records, files, and metadata in electronic or hardcopy format); including but not limited to the following:

1. provided by DOI; or
2. obtained by the Contractor while conducting activities in accordance with the contract with DOI; or
3. distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
4. received from the Contractor by any other related organization and/or any other component or separate business entity.

(b) Within forty-five (45) days after the end of the contract performance period or after the contract is suspended or terminated by DOI or the Contractor for any reason, the Contractor must provide DOI with an associated Certification of Verified Return of all original (and at least one duplicate copy of those information types specified by DOI) of all DOI and DOI-Activity-Related Information, (including but not limited to all records, files, and metadata in electronic or hardcopy format); including but not limited to the following:

1. provided by DOI; or
2. obtained by the Contractor while conducting activities in accordance with the contract with DOI; or
3. distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
4. or received from the Contractor by any other related organization and/or any other component or separate business entity.

(c) This certification must be provided by a third party firm approved by DOI in advance. All costs and resource allocations required for this third party service must be the sole responsibility of the Contractor.

Mandatory Requirement for Verified Secure Destruction of All DOI and DOI-Activity-Related Information

The disposition of all information will be at the written direction of the COR. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

(a) Within sixty (60) days after the end of the contract performance period or after the contract is suspended or terminated by DOI or by the Contractor for any reason, BUT ONLY after DOI has accepted and approved the Contractor's compliance with the Certified Verification of Return of Information Requirement, the Contractor must execute secure destruction (either by the Contractor or third party firm approved in advance by DOI) of all existing active and archived originals and/or copies of all DOI and DOI-Activity-Related files and information, including but not limited to all records, files, and metadata in electronic or hardcopy format, by procedures approved by DOI in advance and in accordance with applicable DOI information technology (IT) Security Policy Requirements, including but not limited to the following:

1. provided by DOI; or
2. obtained by the Contractor while conducting activities in accordance with the contract with DOI; or
3. distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
4. received from the Contractor by any other related organization and/or any other component or separate business entity.

(b) Within seventy-five (75) days after the end of the contract performance period or after the contract is suspended or terminated by DOI or the Contractor for any reason, BUT ONLY after DOI has accepted and approved the Contractor's compliance with the Certified Verification of Return of Information Requirement, the Contractor must provide DOI with Certification of Secure Destruction of all existing active and archived originals and/or copies of all DOI -

Activity-Related files and information, including but not limited to all records, files, and metadata in electronic or hardcopy format, by procedures approved by DOI in advance and in accordance with applicable DOI IT Security Policy Requirements, including but not limited to the following:

1. provided by DOI; or
2. obtained by the Contractor while conducting activities in accordance with the contract with DOI; or
3. distributed for any purpose by the Contractor to any other related organization and/or any other component or separate business entity; or
4. received from the Contractor by any other related organization and/or any other component or separate business entity.

(c) This certification must be provided by a third party firm approved by DOI in advance. All costs and resource allocations required for this third party service must be the sole responsibility of the Contractor.

Information/Data Ownership and Access

(a) All documents produced under this contract are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor, even if the contract is revoked by either party for any reason. All appropriate project documentation will be given to the agency during and at the end of this contract in an acceptable and usable format, which may include the original format, at no additional cost to DOI. The Contractor shall not release any information without the written consent of the CO.

(b) The Government retains unrestricted rights to all Government data. DOI retains ownership of any and all user created/loaded data and applications hosted on the Contractor's infrastructure, as well as maintains the right to request full copies of these at any time.

(c) The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the Contractor in the performance of this contract, are the property of the U.S. Government and must be submitted to the COR at the conclusion of the contract in an acceptable and usable format, which may include the original format, at no additional cost to DOI. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-14.

(d) The Contractor acknowledges DOI's exclusive right of ownership of the information and is required to transfer or return (or delete) all agency data collected, processed, stored or maintained by Contractor on behalf of DOI upon termination of services, and shall provide written certification and supporting documentation attesting to the return of agency data collected, processed, maintained, or stored by the Contractor. Contractor shall provide DOI logical and physical access to Contractor's facilities, installations, technical capabilities, operations, records, and databases upon request to verify the Contractor's certification for the return or removal of agency data.

(e) DOI information stored in the Contractor's or Service Provider's (SP) network and computing environments remain the property of DOI, not the Contractor or SP. DOI retains ownership of the information and any media type that stores Government information. The

Contractor or SP do not have rights to the DOI information for any purposes other than those explicitly stated in the contract. The Contractor and SP must protect DOI information from unauthorized access by Contractor and SP personnel, other Contractors, or other SP subscribers. The Contractor and SP must allow DOI full access to DOI information including data schemas, metadata, and other associated data artifacts that are required to ensure DOI can fully and appropriately retrieve DOI information from all of the Contractor or Service Provider environments that have been utilized to store, read, or process DOI's information.

(f) The Contractor shall treat all deliverables under the contract as the property of the U.S. Government for which DOI and any of its designated officials shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable without the express permission of the CO or COR.

(g) The Contractor is required to obtain the CO's approval prior to engaging in any contractual relationship (sub-Contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any sub-Contractor) is required to abide by Government and DOI guidance for protecting sensitive and proprietary information.

(h) At the expiration of the contract, the Contractor shall return all sensitive DOI information and IT resources provided to the Contractor during the contract, and certify to the CO and COR that all DOI information has been sanitized or purged from any Contractor-owned system following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*. DOI reserves the right, and the Contractor shall cooperate with DOI officials, to conduct reviews to ensure that the security and privacy requirements in the contract are implemented and enforced.

(i) The Contractor shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum Federal standards. Contractor must also explain and certify that its subContractor(s) will adhere to the same minimum Federal standards when working with sensitive data.

(j) The Contractor's invoicing, billing, and other financial, administrative records or databases may not store or include any sensitive Government information, such as PII, created, obtained, or provided during the performance of the contract. It is acceptable to list the names, titles and contact information for the CO, or other designated agency official associated with the administration of the contract in the invoices as needed.

Privacy Act Requirements

All DOI contracts and and Requests for Proposals (RFPs) involving Privacy Act information must adhere to the FAR Privacy Act requirements (Subparts 24.1 and 24.2) and include the specified contract clauses (Parts 52.224-1 and 52-224-2), as appropriate, to ensure that personal information by Contractors who work on DOI-owned systems of records and the system data are protected and mandated.

When a DOI contract requires the operation or maintenance of a system of records or a portion of a system of records or requires the performance of any activities associated with maintaining a system of records, including the collection, use, and dissemination of records, the record system

or the portion of the record system affected are considered to be maintained by DOI and are subject to all Federal privacy laws, regulations, and policies.

If the Contractor must use, have access to, or disseminate personally identifiable information subject to the Privacy Act in order to perform any part of a contract on behalf of DOI, these Contractor activities are subject to the Privacy Act and DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

Privacy Breach Reporting Requirements

The Contractor shall provide notice to DOI of any known or suspected breach of PII and meet breach reporting and mitigation requirements as established by DOI. A breach may be in any medium or format, including paper, oral or electronic, and includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. The Contractor shall fully cooperate with all aspects of risk analysis and remedial activities. Failure to cooperate or meet DOI breach reporting requirements may be deemed a material breach and grounds for contract termination.

The reporting of a breach of PII 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.

Upon becoming aware of any breach of PII, the Contractor shall:

(a) Report ALL known or suspected breaches in electronic or physical form to the CO, COR, and the DOI-CIRC via email within one hour of discovery at DOICIRC@ios.doi.gov or (703) 648-5655, regardless of day or time, even if it is believed the breach may be limited, small, or insignificant. If the breach is reported by phone or the CO's email address is not immediately available, the Contractor shall contact the CO immediately after reporting the breach to the DOI-CIRC.

- Contractor shall NOT include any Sensitive Information in the subject or body of any e-mail. Where necessary, Sensitive Information shall be transmitted using encryption methods to protect information in attachments in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules. Passwords shall not be communicated in the same email as the attachment.
- Contractor shall NOT contact individuals impacted by a breach involving PII. All determinations related to response activities, appropriate notifications to individuals and Federal agencies and other organizations, and any remedial actions will be made by the CO in consultation with DOI Privacy Officials.
- If Contractor has questions regarding these procedures, please contact the CO.

(b) Take immediate action to contain or remedy the breach and reduce the impact of the compromise.

(c) Cooperate with DOI officials to investigate and remedy the breach.

(d) Provide full access to the records compromised.

(e) Provide a detailed written analysis with the following data elements that are available at the time of the breach, and any additional information or updates within 24 hours of the initial breach report, that shall address all relevant information concerning the compromise:

- Location(s) of the breach;
- Date and time the breach was discovered;
- Nature of the event (loss, theft, unauthorized access);
- Description or summary of events;
- Description of the PII involved, such as full name, SSN, date of birth, home address, etc.;
- Number of potentially impacted individuals; and
- Estimated number of records exposed or compromised.

Section 508 Requirements

Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), requires Federal agencies to develop, procure, maintain, or use electronic and information technology (EIT) that allows Federal employees and members of the public with disabilities to have access to and use of information and data that is comparable to other Federal employees or individuals without disabilities.

(a) Requirements for accessibility based on Section 508 are determined to be relevant for this acquisition. The following requirements have been determined to apply to this acquisition:

- (1) 36 CFR 1194.21, Software applications and operating systems
- (2) 36 CFR 1194.22, Web-based intranet and Internet information and applications
- (3) 36 CFR 1194.23, Telecommunications Products
- (4) 36 CFR 1194.24, Video and multimedia products
- (5) 36 CFR 1194.25, Self-Contained Closed Products
- (6) 36 CFR 1194.26, Desktop and Portable Computers
- (7) 36 CFR 1194.31, Functional performance criteria
- (8) 36 CFR 1194.41, Information, documentation, and support

(b) The SP shall describe how their proposed outputs/deliverables meet the provisions identified as applicable in the enclosed Government Product/Service Accessibility Template (GPAT).

(c) Responses to this solicitation will only be considered for award after it has been determined that the proposal adequately addresses the requirements for Section 508. Only proposals which contain adequate information to document the responsiveness to the Section 508 requirements (e.g. accessibility capabilities and past performance) will be eligible for any additional merit consideration.

(d) The SP shall test outputs/deliverables relating to software or web applications for accessibility using the Section 508 Compliance Test Process for Applications

(https://www.dhs.gov/sites/default/files/publications/DHS_Section_508_Compliance_Test_Process_for_Applications_0.pdf), and submit documentation demonstrating remediation actions taken to resolve identified deficiencies. Outputs/Deliverables resulting from this solicitation will be accepted based in part on satisfaction of identified Section 508 requirements for accessibility. Outputs/deliverables must include a completed GPAT. Outputs/Deliverables must meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies.

(e) In the event of a dispute between the SP and the agency, the agency's assessment of the Section 508 compliance will control and the SP will make any additional changes needed to conform with the agency's assessment, at no additional charge to the agency.

Records Management Requirements

The Contractor shall ensure compliance with Federal records in accordance with all applicable records management laws and regulations, including but not limited to, the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33); Code of Federal Regulations (CFR) (36 CFR Chapter XII Subchapter B; 36 CFR 1220-1236); National Archives and Records Administration (NARA) Bulletin, direction and guidance; and Departmental policy.

The Contractor shall coordinate with the appropriate Departmental and Bureau Records Management Offices to ensure the identification, storage, retrieval, preservation, access and disposition of records solely using the Department's Email, Enterprise Records and Document Management System (eERDMS). This includes the implementation of all technical aspects to appropriately interconnect and or transfer records to eERDMS. Any exceptions to using this system must be expressly presented by the Contractor in writing to the Departmental and Bureau Records Management Offices and must obtain a waiver from the Departmental Records Officer. Thereafter, each major or minor variance must be expressly presented in writing to as part of the waiver

The official record keeping system for the Department is eERDMS and eERDMS operates on a platform providing cross-system integration through the use of service-oriented architecture (SOA) and Web Service like tools.

The Contractor shall support records management functions through the life of the project and termination of the contract, unless otherwise expressly noted in writing from the Departmental Records Management Office.

The disposition of all data will be at the written direction of the bureau records officer in coordination with the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.

The Contractor shall provide a mechanism for reliably deleting DOI data upon request by DOI as well as providing evidence that the records are managed according to Departmental guidance and deleted in accordance with NARA-approved records schedules. Documents are Federal records regardless of media, such as, but not limited to, paper or electronic.

(a) The purpose of this section is to provide insight into the contract administration aspects of the mechanisms by which the Department conducts records management. Records Management provides a rational basis for making decisions about recorded information, including what should be saved and what should be discarded. These decisions are necessary to support the legal, fiscal, administrative, and other needs of the Government-owned Contractor-operated facilities, the Federal Government, and the general public.

(b) The incorporation of records management provides value to the Department, Federal Government and the public. The availability of complete and accurate documentation under the Records Management Program allows the Department to:

- Protect the legal and financial rights of the Government and of individuals directly affected by Government activities; and
- Preserve institutional memory so that informed decisions are possible and thus facilitate action by DOI Contractor officials.

(c) The Federal Records Act (FRA) of 1950 (44 U.S.C. 31), as amended (e.g., FRA amendments of 2014) requires that the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

(d) When an agency contracts for the design, development, or operation of a system of records on individuals on behalf of the Department to accomplish an agency function, the agency must make and preserve records to sufficiently document all planning, design, development or operation of the system. All DOI contracts must contain requirements, terms and conditions for the processes related to the creation, preservation, ownership and disposition of records. The records management process provides a formal structure for implementing Federal requirements for recorded information, regardless of media.

(e) The Department recognizes the right of the Contractor to retain ownership of certain records. The following categories of records may be considered to be the property of the Contractor. However, it is the responsibility of the CO/COR to identify which of the following categories of records will be included in the contracting clause(s) as Contractor-owned records.

- Employment-related records except for those records described by the contract as being maintained in a Privacy Act systems of records;
- Confidential Contractor financial information and correspondence between the Contractor and other segments of the Contractor outside the DOI facility;
- Records relating to procurement actions by the Contractor, except for records related to actions under the Department of the Interior Acquisition Regulation, 48 CFR 1427.3
- Legal records, including legal opinions, litigation files, and documents covered by the attorney-client and attorney work product privileges; and
- Certain records maintained pursuant to the technology transfer clause of this contract.

(f) Records need to be managed throughout the lifecycle. Records management refers to the planning, budgeting, organizing, directing, training, and control involved in managing the lifecycle of records, in any medium. Contractor maintained records cannot be destroyed without proper authority and must be transferred to the Government. For the Government, the head of the office is responsible for maintaining these records in accordance with NARA-approved records schedules. Any records management questions should be referred to the responsible records officer for that agency. This lifecycle encompasses the interrelated and interdependent phases of records creation or collection, records maintenance and use, and records disposition.

(g) The routine disposition of records created and maintained by DOI and the Contractor may be suspended through coordination of the Departmental Records Officer, Bureau/Office Records Officer, the Records Management Contact, the Program Manager or Site Manager. A records schedule disposition suspension may be required to—

- Suspend the routine disposition of the Department and Contractor records to support an investigation;
- Preserve records for research;
- Identify lessons learned in recovery operations from natural disasters or other emergencies'; and
- Provide evidence for a legal action.

(h) The Contractor should determine if a moratorium exists prior to the disposition of records. The Department and its Bureaus and Offices have an obligation to inform the Contractor when a moratorium is placed or removed from Federal records. Notification of a moratorium will be made formally through the issuance of a letter with a copy maintained in the contracting folder at the Departmental Records Management Program level.

(i) FAR Subpart 4.7 provides the policies and procedures for retention of records by the Contractor to meet the records review requirements of the Government. In FAR Subpart 4.703(a), the Contractor is required to make records generated under contracts available for contract negotiation, administration, and audit requirements of the contracting agencies and the Comptroller General for—

1. Three years after final payment or, for certain records; and
2. The period specified in 4.705 through 4.705-3, whichever of these periods expires first.

Under no circumstances can the Contractor complete disposition of records generated under contract without first turning over a copy (if possible, the original) of these records to the head of office for proper recordkeeping in accordance with a NARA-approved records disposition schedule.

(j) In accordance with the FRA and the CFRs, Federal agencies must ensure that adequate training is provided to all agency personnel on policies, responsibilities and techniques for the implementation of record keeping requirements and the distinction between records and non-record materials, regardless of media. Contractor personnel are considered agency personnel while supporting the operations and assets for the agency. Therefore, Contractor employees are

required to complete DOI mandated training, including information security awareness, privacy, and records management training before accessing any the DOI information systems.

(k) In FAR Subpart 4.8, the contracting office is provided the requirements for establishing, maintaining, and disposing of contract files. Subpart 4.801 states that the head of each office performing contracting, contract administration, or paying functions shall establish files containing the records of all contractual actions. The policies for storing, handling and disposing of contract files are described in Subpart 4.805, including a table with the retention periods for the different types of documents.

(l) Contracted staff with official DOI electronic messaging accounts must comply with all related policies.

Prevention Of Malicious Code

(a) Definitions

Malicious code is a computer code developed for the purpose of causing some form of intentional damage to computer systems or networks. Malicious code may be a complete program or code imbedded in software programs that appear to provide useful functions. The term includes computer viruses and other destructive programs, such as "Trojan Horses" and network "worms."

(b) The contractor must have in place an anti-virus procedure to ensure that media supplied is uncontaminated by malicious code.

(c) The contractor is required to scan all delivered software to insure it is free of malicious code prior to its installation or operation on Government-owned computers or contractor-owned computers connected to Government computer systems or networks. Contractors using diagnostics software disks or connecting to a non-Government computer while performing repairs or upgrades to a Government computer will scan the serviced computer's drive(s) to insure they are free of malicious code upon completion of the service call, or prior to return of serviced equipment, if servicing is performed off-site.