

Attachment 1

Performance Work Statement

Information Technology Transformation Detailed Planning Follow-on Strategic Deep-dives

For

Office of the Chief Information Officer

Department of the Interior

1. PURPOSE

The purpose of this requirement is for the contractor to provide continued support for the development and refinement of the detailed plan for Information Technology (IT) Transformation through follow-on strategic deep-dives in order to create a modern, consolidated IT Service Delivery organization that will support all Department of the Interior (DOI) bureaus, offices and approximately 80,000 end users. As part of the initial performance work statement, the Department developed numerous deliverables in support of its IT Transformation Plan. In this logical follow-on, deep-dives shall be conducted across a subset of these focus areas to provide additional support for IT Transformation.

2. SCOPE:

DOI has established a strategic goal to fundamentally restructure the way that IT services are delivered to internal and external constituents. The vendor shall review the current detailed IT Transformation Plan, and support the Government in the continued development and refinement of this detailed IT Transformation Plan through additional deep-dives that will achieve this strategic goal by moving DOI to an IT Service Management (ITSM) model for the delivery of IT services.

The ITSM approach that is envisioned will be characterized by:

1. A focus on identifying and serving the customers who are the ultimate consumers of IT services
2. Driving IT service requirements from customer needs rather than from IT wants or desires
3. Creating an IT Service Portfolio that describes IT services in terms of their business value to the customer
4. Using the IT Service Portfolio to provide the high-level organization of an IT Service Catalog into approximately 5-10 Service Areas, for example, "Collaboration Services" or "Geospatial Services"
5. Decoupling the services defined by the Service Portfolio and Service Catalog from the underlying technology and fulfillment processes used to deliver the service

6. Development of unit-based pricing models and establishment of enforceable Service Level Agreements (SLAs) for each service
7. Establishing a process for moving services from initial concept through feasibility analysis, costing, design, implementation and delivery with appropriate decision “gates” that ensure the right IT services are delivered in order to meet customer priorities
8. Utilization of a hybrid delivery model where infrastructure or “utility” services are provided on a consolidated, enterprise-wide basis and mission and program specific applications are provided on a decentralized basis
9. Creation of the following new roles to manage and deliver IT services through the Services Lifecycle:
 - a) Relationship Managers to ensure the satisfaction of specific customer segments across the entire range of services to which those customers subscribe
 - b) Service Managers to ensure that the correct services are offered at the right price and quality levels
 - c) Delivery Managers to manage and execute technology and fulfillment processes in order to optimize delivery across all supported IT services
 - d) Quality Assurance to perform measurement and monitoring of process and service outcome to ensure that SLAs are met and to identify opportunities for process improvement.

DOI will be utilizing services provided by the Office of Personnel Management (OPM) to conduct an assessment and analysis of the existing DOI IT workforce. These services will also include development of recommendations for aligning the DOI IT workforce with the ITSM model described above. Therefore, workforce analysis is out of scope for this requirement. However, the contractor will be required to work collaboratively with the workforce analysis service provider to integrate work-force planning recommendations into the follow-on strategic deep-dives.

3. **OBJECTIVE:**

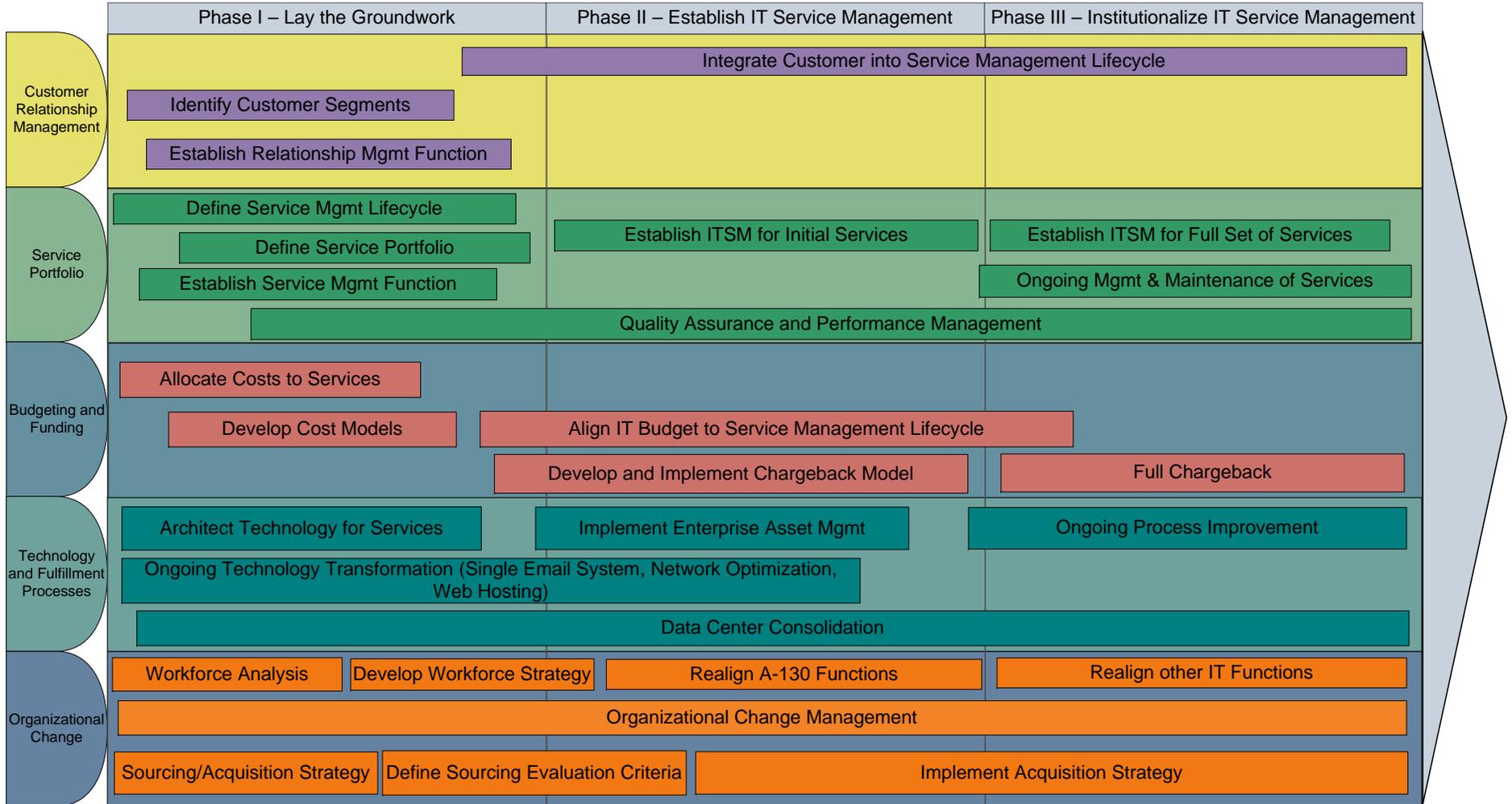
Figure 1 on the following page shows the high-level roadmap that DOI has developed for the IT Transformation Program.

This roadmap shows the *five major functional components* that are envisioned:

1. **Customer Relationship Management:** establishing the processes for identifying and engaging with customers to identify and prioritize service requirements
2. **Service Portfolio:** definition of the Service Portfolio and the processes required for ongoing management and evolution of the portfolio to meet customer needs

3. **Technology and Fulfillment Processes:** aligning the underlying processes with the various services that they support in order to provide customer satisfaction and to meet established service levels
4. **Budget and Funding:** establishing funding models, chargeback processes and other financial elements that must be addressed in order to successfully operate the ITSM model. These models must define methods to correctly allocate costs associated with underlying processes to multiple service offerings in order to establish unit-based pricing models for each service.
5. **Organizational Change:** leading organizational change regarding workforce alignment and strategic sourcing. As noted above, workforce analysis is out of scope for this requirement but incorporating the results of a separate workforce analysis engagement is in scope for this requirement.

Figure 1 - DO IT Transformation Roadmap



The roadmap also shows the *three major phases* that are envisioned:

- **PHASE 1, LAYING THE GROUNDWORK:**

This phase will include the completion of the detailed plan as well as:

- A.** Identification of which services will be provided on a consolidated, enterprise-wide basis and which services will be provided on a decentralized, mission or bureau-specific basis
- B.** Definition of the IT Service Portfolio and IT Service Catalog
- C.** Definition of processes for identifying and prioritizing new elements of the IT Service Catalog
- D.** Refinement of the high level IT Services Lifecycle represented in Figure 2 into a detailed service lifecycle and service governance model
- E.** Definition of financial modeling templates to support unit-based pricing for services including the allocation of the costs of underlying technology and fulfillment processes to each service supported by those processes
- F.** Integration of ongoing DOI technology transformation projects into the IT Transformation Plan, including implementation of a single DOI email system, optimization of network architecture, access control, identity management, web hosting services and data center consolidation
- G.** Planning for the implementation of an Enterprise IT Service Desk
- H.** Planning for the implementation of Enterprise-wide Asset Management
- I.** Development of an IT Transformation communications strategy
- J.** Establishment of Quality Assurance and Performance Management functions
- K.** Utilizing services provided by OPM to conduct a DOI Workforce Analysis
- L.** Development of a data center consolidation strategy to allow DOI to address requirements defined by the Federal Data Center Consolidation Initiative (FDCCI)
- M.** Development of sourcing strategy to include “Cloud First” requirements.

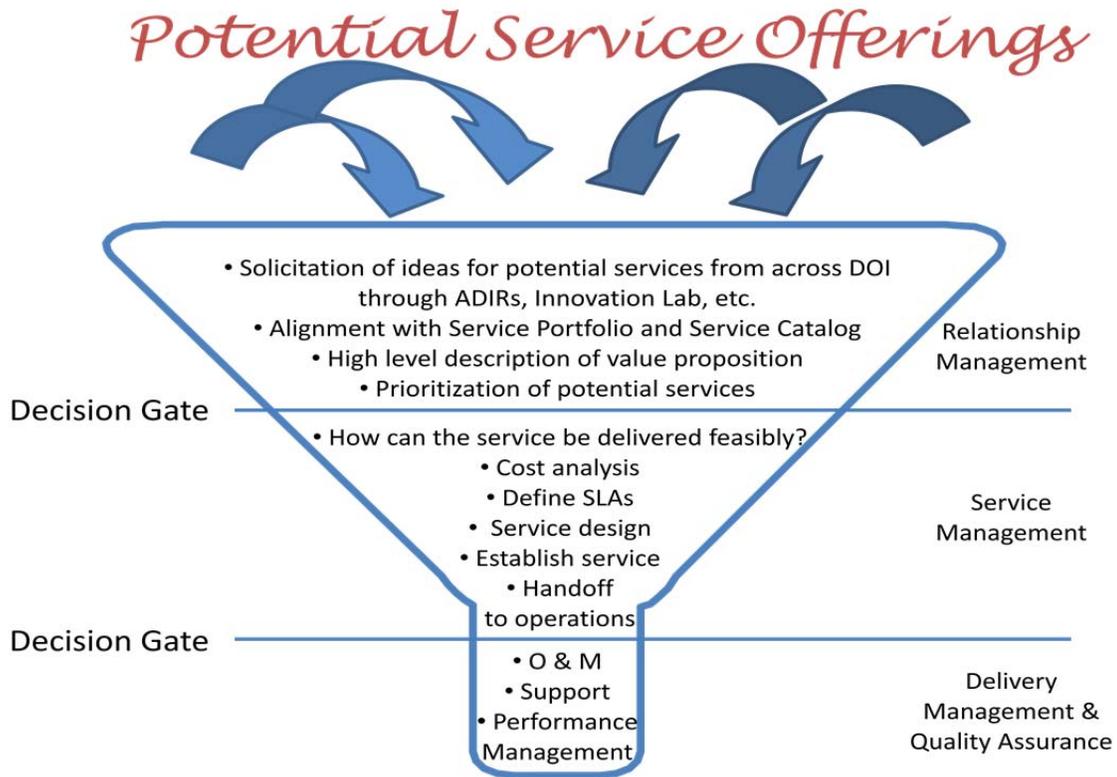


Figure 2 - High Level View of IT Services Lifecycle

- **PHASE 2, ESTABLISHMENT OF IT SERVICE MANAGEMENT:**

In this phase the ITSM model will be established for the initial set of services defined in Phase 1. This phase will also include the implementation of supporting capabilities including:

- A. Implementation of Enterprise-wide Asset Management
- B. Implementation of Enterprise IT Service Desk
- C. Finalization of workforce strategy, in collaboration with services provided by OPM
- D. Establishment of the ITSM model for the initial set of IT services
- E. Implementation of IT acquisition strategy
- F. Realignment of A-130 functions (i.e. Enterprise Architecture, IT Capital Planning, Security, Privacy, etc.) under the DOI CIO.

- **PHASE 3, INSTITUTIONALIZE IT SERVICE MANAGEMENT:**

This phase will complete the transformation to the ITSM model in each of the five major functional components described above. This will include the maturation of DOI's ITSM model to allow for "steady state" operation as well as:

- A. Establishment of the ITSM model for the remainder of the IT Service Portfolio
- B. Full implementation of a chargeback model to provide funding for services and supporting technology and fulfillment processes
- C. Completion of organizational realignment under the DOI CIO
- D. Continued consolidation of data centers.

4. EXCLUSION FROM FUTURE COMPETITION:

The contractor with the successful quote for this requirement and any of its employees, affiliates, and related entities may not propose, bid, subcontract nor consult on the actual implementation of the recommendations as outlined in this requirement which may result in a future solicitation(s).

5. CONTRACTOR QUALIFICATIONS

- 1) The contractor will have an in-depth knowledge, expertise and proven experience in assisting large, complex organizations in the adoption and transition to an ITSM model for the delivery of IT services.
- 2) The contractor will have experience in the planning, execution and management of IT organizational change initiatives for large Federal government organizations utilizing industry best practices for organizational change management.
- 3) The Project Manager identified by the contractor shall have proven and demonstrated experience in managing projects of a similar size
- 4) The contractor will have demonstrated experience and capabilities in high level report writing and oral presentations for executive level management.
- 5) Vendors' quote must demonstrate that both the organization and proposed key personnel can successfully complete this project on time, within budget and within scope.
- 6) Vendor MUST indicate the availability of the key personnel who will be assigned to this requirement. Key personnel are all individuals who will be supporting this requirement in a primary capacity, to include full and part-time personnel.

6. BACKGROUND

The U.S. Department of the Interior (DOI) is a large complex organization that protects America's natural resources and heritage, honors our cultures and tribal communities, and supplies the energy to power our future. The U.S. Department of the Interior is a Cabinet-level agency that manages America's vast natural and cultural resources. Ken Salazar, Secretary of the Interior, heads our Department, which employs 70,000 people, including expert scientists and resource-management professionals, in nine technical bureaus under five Assistant Secretaries ([Attachment 1 & 2](#)). The various Bureaus and offices each possess their own individual Information Technology personnel and infrastructure resulting in significant duplication of effort, lack of common standards and escalating cost in a severely constrained budget climate.

On December 14, 2010, the Secretary of the Interior issued Secretarial Order (SO) 3309, which calls for the centralization of all IT management and operations functions, including IT infrastructure assets, and all Clinger-Cohen functions (e.g. Records Management, Enterprise Architecture, Capital Planning, Privacy, and Cyber (IT) Security) under the Department Chief Information Officer (CIO). Additionally, within 180 days of the date of the Order, each bureau with more than 5,000 employees who currently has a CIO is required to establish one Senior Executive as an Assistant Director for Information Resources (ADIR) who will oversee the orderly migration of assets under the CIO. The primary objective of the new IT organization will be to implement a dynamic new enterprise business model for delivering scalable IT products and services that are transparent and customer and mission focused. The consolidation of IT management, human resources, and Clinger-Cohen functions within the Office of the Secretary will be addressed in the first phase of the transformation process.

In June of 2011, the CIO presented a strategic plan to the Secretary that describes how transition of all IT infrastructures to the organization, management, ownership and control of the CIO will be executed. The strategic plan described the new agency-wide 21st Century IT organization, its concept of operations and a schedule for implementation.

7. PERFORMANCE REQUIREMENTS:

The contractor shall be directly responsible for ensuring the accuracy, timeliness and completion of all deliverables under this effort. Specifically, the contractor shall complete the following deliverables.

8. REFERENCE LISTING:

1. Department of the Interior
Secretary Order 3309
Date 12/14/2010
Information Technology Management Functions and Establishment of Funding Authorities
http://elips.doi.gov/app_so/act_getfiles.cfm?order_number=3309
2. Department of the Interior
Date 01/26/2011
Strategic Plan Provides Blueprint for 21st Century Department
http://www.doi.gov/bpp/data/PPP/DOI_StrategicPlan.pdf
3. Vivek Kundra, U.S. Chief Information Officer
Dated 12/09/2010
25 Point Implementation Plan To Reform Federal Information Technology Management
<http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf>
4. Vivek Kundra, U.S. Chief Information Officer
Dated 02/08/2011
Federal Cloud Computing Strategy
<http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>
5. *Federal Data Center Consolidation Initiative*
<http://www.cio.gov/pages.cfm/page/FDCCI>

9. SPECIFIC DELIVERABLES:

The contractor shall be directly responsible for ensuring the accuracy, timeliness and completion of all deliverables under this effort. Specifically, the contractor shall:

9.1. DEVELOP FOLLOW-ON STRATEGIC DEEP-DIVES FOR DOI'S IT TRANSFORMATION PROGRAM

As part of the initial Performance Work Statement, a set of deliverables across numerous tasks were completed and delivered in support of the Department's effort to develop a detailed IT transformation plan. As part of this follow-on requirement, deep-dives shall be completed for a subset of the previous deliverable focus areas to provide greater detail in support of the IT transformation program. These specific follow-on strategic deep dives shall be developed and delivered by the contractor within the period of performance of this requirement in support of the continued development and refinement of the detailed IT Transformation project plan. The contractor shall coordinate the development of these deliverables with DOI's assigned Contracting Officer's Representative (COR).

Deliverables:

- 1. Management structure including roles and responsibilities:** Additional development and refinement of the next level of roles and responsibilities for Service Delivery, and Support functions
- 2. Sourcing and acquisition strategy:** Build-out of cloud-specific sourcing and acquisition strategy and requirements definition in the context of a refined hosting strategy
- 3. IT Services Lifecycle and Governance:** Strategic deep-dive on performance management strategy, including roles / responsibilities and tools / dashboards
- 4. Financial modeling templates and chargeback model:** Detailed refinement of pricing and roll-out strategies for financial chargeback model including development of simplified intermediate chargeback strategy
- 5. IT Transformation communications strategy:** Development of the next level of communications strategy detail for IT management community and senior Departmental leadership in the context of an updated detailed IT Transformation plan
- 6. Datacenter consolidation strategy:** Detailed strategic recommendations in the context of greater applications and data collection efforts and needs

Due Date: The vendors shall develop a master project schedule which provides the vendors suggested delivery schedule for the deliverables. The schedule will include the development of the deliverable; draft and final review and submission dates for each deliverable.

10. PERFORMANCE MEASURES:

The following performance measures have been established to guide the expected level of service for the required support deliverables to be performed under the resulting task orders. The COR will maintain the method of surveillance on a MONTHLY basis and provide a copy to the CONTRACTOR. The COR will inform the contracting officer in writing of control performance issues. The contracting officer will ensure adequate documentation and corrective action is taken to ensure acceptable performance standards are maintained by the contractor.

Requirement	Performance Standard and Acceptable Quality Level	Method of Surveillance
<ol style="list-style-type: none">1. Management structure including roles and responsibilities: Additional development and refinement of the next level of roles and responsibilities for Service Delivery, and Support functions2. Sourcing and acquisition strategy: Build-out of cloud-specific sourcing and acquisition strategy and requirements definition in the context of a refined hosting strategy3. IT Services Lifecycle and Governance: Strategic deep-dive on performance management strategy, including roles / responsibilities and tools / dashboards4. Financial modeling templates and chargeback model: Detailed refinement of pricing and roll-out strategies for financial chargeback model including development of simplified intermediate chargeback strategy5. IT Transformation communications	Draft and Final deliverable are delivered 100% on time	Periodic Sampling

Requirement	Performance Standard and Acceptable Quality Level	Method of Surveillance
<p>strategy: Development of the next level of communications strategy detail for IT management community and senior Departmental leadership in the context of an updated detailed IT Transformation plan</p> <p>6. Datacenter consolidation strategy: Detailed strategic recommendations in the context of greater applications and data collection efforts and needs</p>		
Bi-Weekly briefings	Delivered within contractual timeframes at least 98% of the time	Customer Feedback

11. DELIVERABLES:

11.1 DELIVERABLE INSPECTION , ACCEPTANCE AND QUALITY:

11.1.1. DELIVERABLE INSPECTION AND ACCEPTANCE CRITERIA

Final inspection and acceptance of all work performed, reports and other deliverables will be performed at the place of delivery by the COR.

11.1.2 DELIVERABLE GENERAL ACCEPTANCE CRITERIA

General quality measures, as set forth below, will be applied to each work product received from the contractor under this statement of work.

1. **Accuracy** - Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
2. **Clarity** - Work Products shall be clear and concise. Any/All diagrams shall be easy to understand and be relevant to the supporting narrative.
3. **Consistency to Requirements** - All work products must satisfy the requirements of this statement of work.
4. **File Editing** - All text and diagrammatic files shall be editable by the Government.

5. **Format** - Work Products shall be submitted in hard copy (where applicable) and in media mutually agreed upon prior to submission. Hard copy formats shall follow any specified Directives or Manuals.
6. **Time-lines** - Work Products shall be submitted on or before the due date specified in this statement of work or submitted in accordance with a later scheduled date determined by the Government.

11.1.3 Deliverable Quality Assurance

The COR will review, for completeness, preliminary or draft documentation that the Contractor submits, and may return it to the Contractor for correction. Absence of any comments by the COR will not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of documentation required herein shall be by **written approval** and acceptance by the COR. The Contractor shall not construe any letter of acknowledgment of receipt material as a waiver of review, or as an acknowledgment that the material is in conformance with this work statement. Any approval given during preparation of the documentation, or approval for shipment shall not guarantee the final acceptance of the completed documentation.

All deliverables or materials associated therewith (“materials”) prepared by the contractor during the course of this contract are hereby deemed the property of the United States Government, including all intellectual property rights associated with any material. Any restrictive or proprietary language included on any material in any media shall deem the product as undelivered.

11.1.4 DELIVERABLE REVIEW:

The **Government** will have a maximum of **five (5) working days** from the day the draft deliverable is received to review the document, provide comments back to the contractor, approve or disapprove the deliverable(s). The **contractor** will also have a maximum of **five (5) working days** from the day comments are received to incorporate all changes and submit the final deliverable to the Government. All days identified below are intended to be workdays unless otherwise specified.

11.2 ADDITIONAL DELIVERABLES:

11.2.1 Project Management Plan

The contractor shall prepare a Project Management Plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements for this effort. The Project Management Plan shall detail the products, methods for developing the products, allocation of staff and other resources necessary to produce the

products and a revised timeline for producing the products, if necessary. The COR shall receive the revised Project Management Plan in both hard copy and electronic form. It is assumed the contractor will build the plan in a scheduling application; however the electronic version shall be sent as a pdf file as not all Government employees have access to a scheduling application. Based on the Project Management Plan, the Contracting Officers Representative (COR) will provide approval to move forward on activities planned. The contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given. The project management plan is expected to be kept up to date, reflecting current work activities and schedules throughout the life of this requirement. (Draft due with proposal / final due 5 days after orientation meeting)

11.2.2 Orientation Briefing

Within **five (5) working days** of award of the contract, the contractor shall conduct an orientation briefing for the Government. The Government does not want an elaborate orientation briefing nor does it expect the contractor to expend significant resources in preparation for this briefing. The intent of the briefing is to initiate the communication process between the Government and contractor by introducing key task participants and explaining their roles, reviewing communication ground rules, and assuring a common understanding of subtask requirements and objectives.

The **Orientation Briefing** will be held at the Government's facility (US Department of the Interior – **Main Interior Building (MIB) 1849 C street, NW, Washington DC 20240**) and the date and time will be mutually agreed upon by both parties, *to be no later than 5 work days after award of contract.*

The completion of this briefing will result in the following:

- a) Introduction of both Contractor and Government personnel performing work under this Contract.
- b) **Final Project Management Plan** with mutually agreed upon dates to be submitted no later than **5 work days** after the orientation meeting.

11.2.3 Bi-weekly Status Reports & Conference Calls & Briefings:

The contractor shall document the efforts performed in the completion of each deliverable in a detailed Bi-Weekly Status Report due every two weeks. The status report shall include, at a minimum:

- Program status, to include objectives met, work completed and work outstanding
- Notable achievements
- Issues or obstacles impeding progress and recommended solutions
- Status of deliverables/milestones
- Issues and resolutions
- Resource planning/status
- Topics or issues identified by the government COR
- Description of work completed and plans for next week(s)
- Summarization of the efforts of each deliverable in the Government PWS

11.3 DELIVERABLE TABLE: Note: specific delivery dates will be mutually discussed and agreed to during the orientation meeting. Dates assume 4 week month.

Item #	Ref	Milestone/Deliverable	Responsibility	Draft (Work Days)	Final (Work Days)	Deliverable Quantity and Distribution
1		Project Management Plan	Contractor	With RFQ	Initial version 5 working days after Orientation Briefing with ongoing updates as required	1 hard copies to the COR 1 electronic copy to the COR 1 electronic copy to the CO
2		Orientation Briefing	Contractor / Government	N/A	Within 5 Days after award	In person meeting
3		Bi-weekly Status Reports & Conference Calls & Briefings:	Contractor	N/A	Bi-Weekly	
4		Non-Disclosure Agreement	Contractor	N/A	2 days after Orientation Briefing	1 electronic copy to the COR 1 electronic copy to the CO
5		Conflict of Interest Statement	Contractor	N/A	2 days after Orientation Briefing	1 electronic copy to the COR 1 electronic copy to the CO
6		Government Furnished Information	Government	N/A	To be provided at the Orientation Briefing if available	The government will provide limited copies to the contractor at the orientation meeting.
7	Deliverables	Follow-on strategic deep-dive deliverables, to include at a	Contractor	As defined in the Vendors'	As defined in the Vendors'	1 electronic copy to the COR

Item #	Ref	Milestone/Deliverable	Responsibility	Draft (Work Days)	Final (Work Days)	Deliverable Quantity and Distribution
		<p>minimum:</p> <ol style="list-style-type: none"> <li data-bbox="470 318 894 613">1. Management structure including roles and responsibilities: Additional development and refinement of the next level of roles and responsibilities for Service Delivery, and Support functions <li data-bbox="470 667 894 927">2. Sourcing and acquisition strategy: Build-out of cloud-specific sourcing and acquisition strategy and requirements definition in the context of a refined hosting strategy <li data-bbox="470 980 894 1240">3. IT Services Lifecycle and Governance: Strategic deep-dive on performance management strategy, including roles / responsibilities and tools / dashboards <li data-bbox="470 1294 894 1391">4. Financial modeling templates and chargeback model: Detailed refinement of pricing 		Project Plan	Project Plan	1 electronic copy to the CO

Item #	Ref	Milestone/Deliverable	Responsibility	Draft (Work Days)	Final (Work Days)	Deliverable Quantity and Distribution
		<p>and roll-out strategies for financial chargeback model including development of simplified intermediate chargeback strategy</p> <p>5. IT Transformation communications strategy: Development of the next level of communications strategy detail for IT management community and senior Departmental leadership in the context of an updated detailed IT Transformation plan</p> <p>6. Datacenter consolidation strategy: Detailed strategic recommendations in the context of greater applications and data collection efforts and needs</p>				
8	Security	<p>Personal Identity Verification Forms – consisting of:</p> <p>A. OPM Standard Form 85 or 85P</p> <p>B. OF 306</p> <p>C. Fingerprint card (local procedures may require that</p>	Contractor	N/A	No later than 5 days after award	COR coordinates the paperwork with the DOI Security Office and other offices to ensure vendor is provided with timely credentials.

Item #	Ref	Milestone/Deliverable	Responsibility	Draft (Work Days)	Final (Work Days)	Deliverable Quantity and Distribution
		<p>the fingerprinting be done at a police station; in this case, any charges are to be borne by the CONTRACTOR.)</p> <p>D. Release to Obtain Credit Information</p> <p>E. PIV card application (web-based)</p>				

12 GOVERNMENT FURNISHED INFORMATION & EQUIPEMENT

12.1 GOVERNMENT FURNISHED INFORMATION:

The government will supply the following information in support of this requirement.

(1) [DOI IT Transformation Strategic Plan \(Reference SO 3309\)](#)

All materials provided by the Government during the course of this contract shall remain the property of the Government and shall be returned immediately upon completion of the contract or as otherwise requested by the COR or Contracting Officer.

12.2 GOVERNMENT FURNISHED EQUIPMENT: None.

When at DOI facilities, the contractor shall be provided with one government furnished laptop, phone, copier and fax service only. The contractor is responsible for providing its staff with their own equipment, (i.e., laptops, cell phone, blackberry, air card, etc) in support of this requirement.

13.0 TYPE OF CONTRACT: FIRM FIXED PRICE

14.0 PERIOD OF PERFORMANCE:

The period of performance for this effort is date of award for a one (1) year period.

15.0 DOI IT System Access: Yes

16.0 ACCESS TO GOVERNMENT PROPERTY OR FACILITIES

The Contractor will be allowed limited access to the Government's facilities. The COR or other Government official as identified by the COR will coordinate and ensure access to the government facilities is provided. The Contractor will be required to check-in at the facility in accordance with the facility procedures and receive a temporary visitor's pass. The Contractor will display this badge at all times while on government premises. The Contractor will comply with all rules and regulations specific to the government facility.

17.0 PLACE OF PERFORMANCE:

The place of performance will be at the contractor site, and DOI facilities, including DC, Reston, Denver.

18.0 HOURS OF WORK

When required to support the Government on-site, the contractor shall adhere to normal business schedules. The core Government business hours are 08:00 AM to 5:00 PM, Monday through Friday. The contractor must be available to the Government during the core business hours.

19.0 OTHER DIRECT COST/TRAVEL

19.1 Other Direct Costs (ODCs): ODC's are **NOT** authorized on this order.

19.2 Travel:

Guidelines for travel are as follows:

- Local Travel, parking and tolls within the DC metropolitan area is not reimbursable.
- Travel will be issued as a not to exceed basis. Travel dollars are included as a place holder as the approximate number of trips required in support of this requirement cannot be determined at this time.
- The Not-To-Exceed place holder for travel is \$25,000 per year.
- Long Distance Travel is anticipated to be to various DOI locations in the United States, primarily west of the Mississippi River.

The Contractor will be reimbursed for travel to provide support at a Government site or other site as may be specified and approved by the COR under this effort. All travel requests will be submitted on a **REQUEST FOR TRAVEL/APPROVAL FORM** ([Attachment 4](#)) and shall be submitted and approved by the COR prior to any travel in support of this contract. The contractor shall be reimbursed for actual allowable, allocable, and reasonable travel costs incurred during performance of this effort in accordance with the Federal Travel Regulations currently in effective on date of travel. [Reference FAR 31.205-46] Travel Costs]

PLEASE NOTE: TRAVEL RECEIPTS ARE REQUIRED TO BE INCLUDED WITH THE INVOICE. Example: airline tickets; parking receipts, hotel, rental car, taxi, etc. Travel is in accordance with the federal travel regulations – FTR per diem and rates are applicable, and charges that exceed the FTR will not be reimbursed. Rental cars are limited to economy – unless more than 2 travelers, and a mid-size car is authorized – rental of larger cars will not be reimbursed. GPS will not be reimbursed. Short term airport parking will not be reimbursed for travel that is more than one business day.

Government Travel References Include:

- 41 Code of Federal Regulations (CFR), Chapters 300 through 304
- FAR 31.205-46 - Travel Costs
- Federal Travel Regulations (FTR) & Per Diem Information – Travel Resources: www.gsa.gov

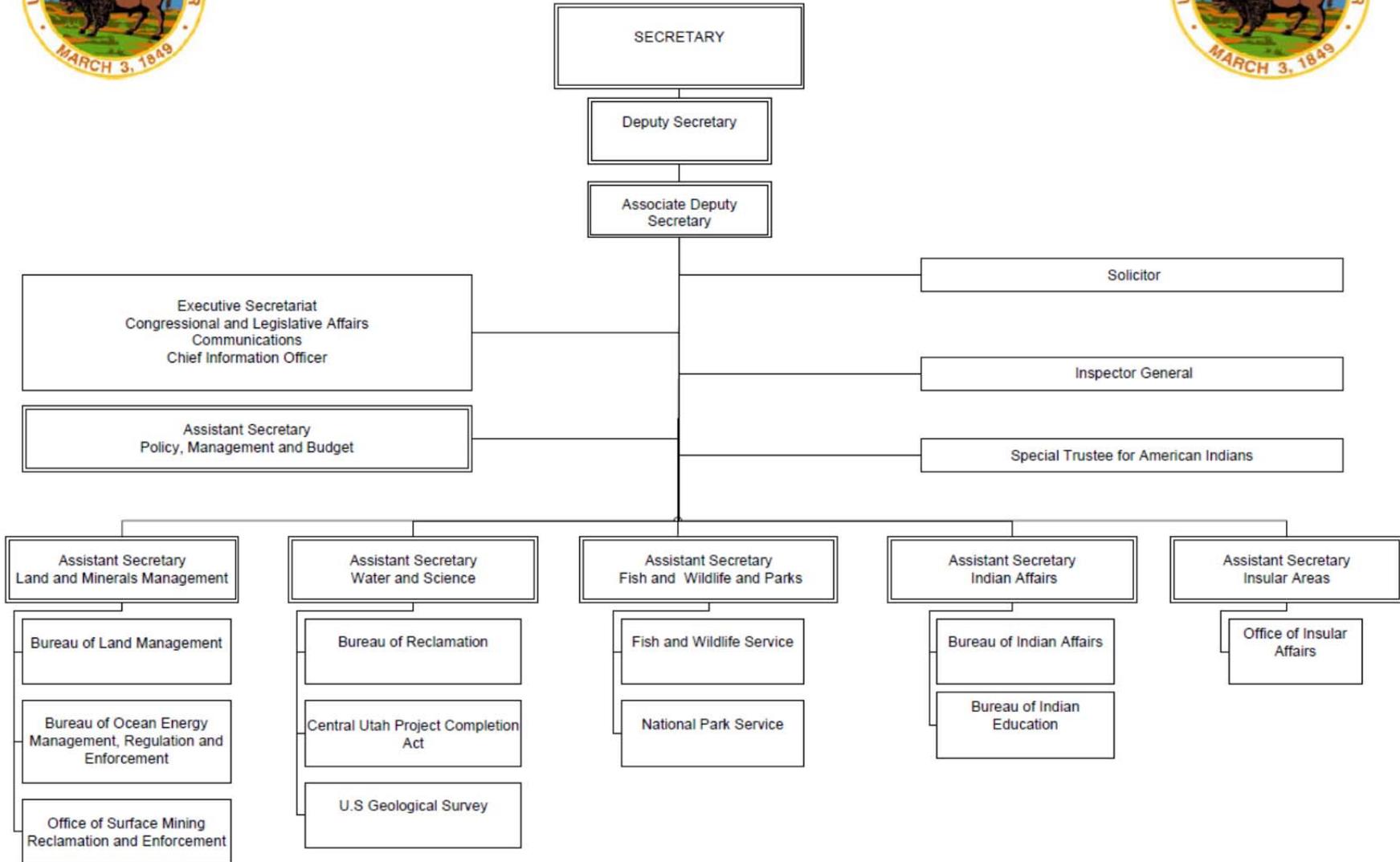
PWS ATTACHMENTS :

1. DOI Organizational Chart #1 – Referenced in PWS
2. DOI Organizational Chart #2 – Referenced in PWS
3. Travel Reconciliation Template – Referenced in PWS
4. Request For Travel/Approval Form – Referenced in PWS
5. Non-Disclosure Agreement – Referenced in RFQ Letter / Terms & Conditions
6. Certificate For Conflict Of Interest – Referenced in RFQ Letter / Terms & Conditions
7. DOI It Security Checklist – Referenced in RFQ Letter / Terms & Conditions



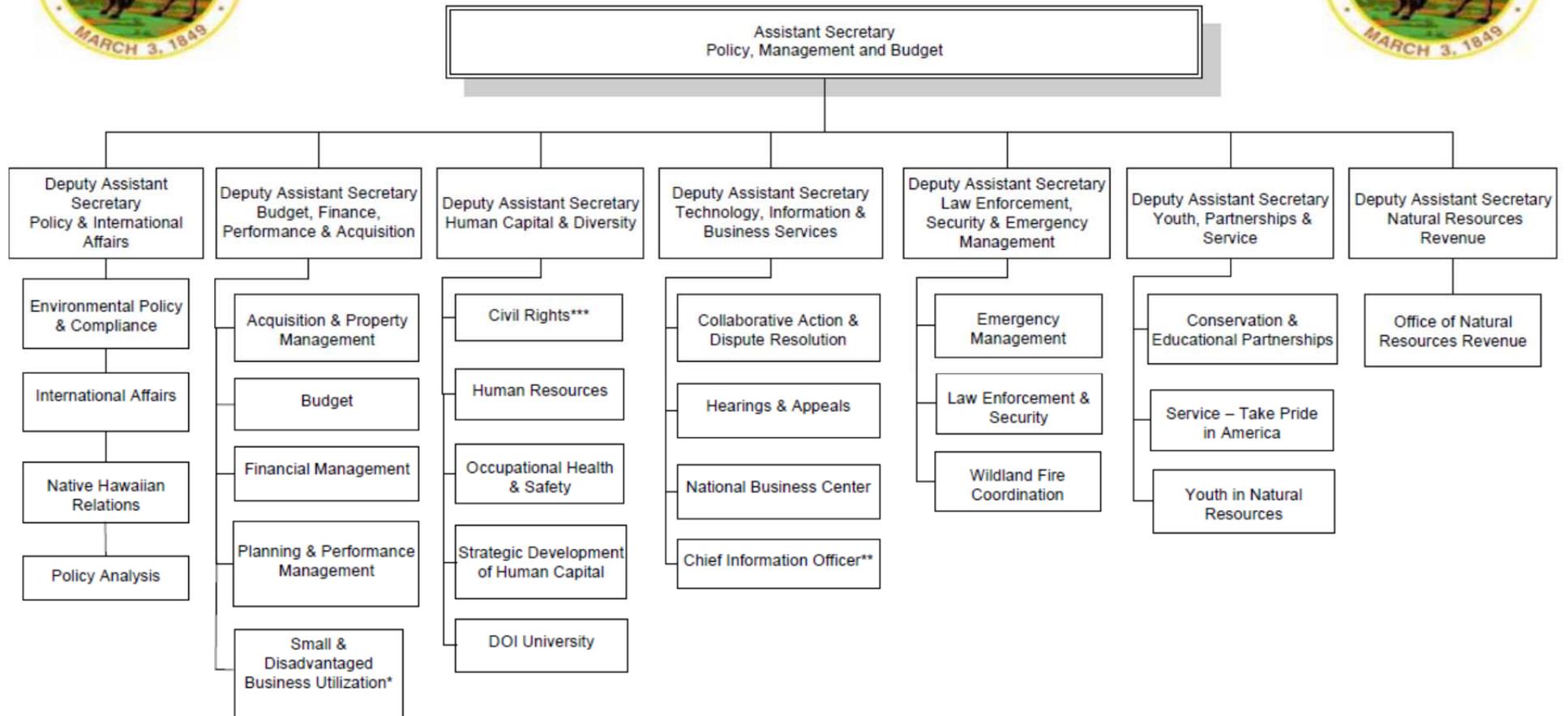
U.S. DEPARTMENT OF THE INTERIOR

ATTACHMENT 1





ASSISTANT SECRETARY- POLICY, MANAGEMENT AND BUDGET



*The Director reports to the Secretary, and receives administrative support and guidance from the A/S – PMB and the DAS – Budget, Finance, Performance & Acquisition.

**These Offices report to the Secretary and receive administrative support and guidance from the A/S – PMB and the DAS – Technology & Business Services.

***The Director reports to the Secretary and receives administrative support and guidance from the A/S – PMB and the DAS – Human Capital & Diversity.

Travel Reconciliation Template

PWS Title: Information Technology Transformation Plan Follow-On for Office of the Chief Information Officer, Department of the Interior

Name of Traveler:

Place of Travel:

Begin Travel Date:

End Travel Date:

	<u>Day</u> <u>1</u>	<u>Day</u> <u>2</u>	<u>Day</u> <u>3</u>	<u>Day</u> <u>4</u>	<u>Day</u> <u>5</u>	<u>Day</u> <u>6</u>	<u>Day</u> <u>7</u>	<u>Day</u> <u>8</u>	<u>Tota</u> <u>l</u>
Airfare	-	-	-	-	-	-	-	-	
Luggage Fee	-	-	-	-	-	-	-	-	
Hotel									
PerDiem									
Rental Car									
Gas for Rental Car									
Parking									
Mileage to Airport									
Mileage from Airport									
Taxi									
Subway									
Total									

Travel is in accordance with Federal Travel Regulations

*First and Last Day of Travel is 75% of Meals and Incidental Expenses (M&IE)

Receipts must be provided

ATTACHMENT 4

REQUEST FOR TRAVEL/APPROVAL FORM

PWS Title: Information Technology Transformation Plan Follow-On for Office of the Chief Information Officer, Department of the Interior

1. Reference Contract Number:
2. Company Name:
3. Individual Requesting Travel: Name / Date:
4. Description of Travel – what will be accomplished / to be supported:
5. Place of Travel [City, State, Facility Name]:
6. Number of Contractor Employee’s traveling:
7. Name of Contractor Employee’s traveling:
8. Total Days Required for travel (includes travel and working days):
9. Indicate number of travel days:
10. Indicate Number of actual work days:
11. Indicate number of overnight stays required:
12. Rental car required: Yes / No
13. Total Estimated Travel Amount:

COR Authorization:

Contact Information/Mailing Address/Phone & email

COR Signature: _____

Date: _____

ATTACHMENT 5

Non-disclosure Agreement between Department of the Interior and Contractor Employee or Other External Entity Granting Conditional Access to Sensitive but Unclassified Information

Task Order Number#: _____

PWS Title: Information Technology Transformation Plan Follow-On for Office of the Chief Information Officer, Department of the Interior

I, _____ (**PRINT FULL NAME**), hereby consent to this agreement in consideration for my being granted conditional access to certain United States Government documents or materials containing sensitive but unclassified information. I understand and agree to the following terms and conditions:

1. *Sensitive but unclassified information* is any information, the loss, misuse, or unauthorized modification of which could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5 U.S.C. paragraph 552a, but which has not been specifically authorized to be kept secret in the interest of national defense or foreign policy.
2. Upon the execution of this agreement, I may be granted conditional access to sensitive but unclassified information. This information concerns the Department of the Interior and other Governmental agencies. Information may be in the form of system data, files and records, contract data, analyses, memos, meeting content, conversations, or any other form. The sole purpose of this access is to assist in the support of this requirement.
3. I will not use, release, or disclose any sensitive but unclassified information or data, in any form whatsoever, to any person or entity except as is necessary to perform the duties under the above-cited contract or except as authorized by the Contracting Officer or the Contracting Officer's Technical Representative. I will not take, alter, or convert such information to any use not specifically authorized under the contract or this agreement.
4. I will not seek access to non-public information beyond what is required for the performance of my duties under the above-cited contract.
5. I will ensure that my status as a contractor employee is known when seeking access to and receiving non-public information.
6. I will protect sensitive but unclassified information in accordance with the provisions of 18 U.S.C. 1905 (Trade Secrets Act), 5 U.S.C. 552 (Privacy Act of 1974), P.L. 104-294 (Economic Espionage Act of 1996), P.L. 103-339 (Counterintelligence and Security Enhancement Act of 1994), and other pertinent laws and regulations governing the confidentiality of privileged information. If I become aware of any improper use, release or disclosure of non-public information, I will advise the Contracting Officer as soon as possible.
7. I will surrender any written or electronic non-public information given to me pursuant to this agreement, including my own notes, upon completion or termination of my duties under the above-cited contract, or upon the request of the Contracting Officer, Contracting

Officer's Technical Representative, or my supervisor.

8. Unless and until I am provided with a written release from this agreement, all conditions and obligations contained herein apply both during my period of conditional access and at all times thereafter.
9. I will submit any book, article, column or other written work for general publication that is based upon any knowledge that I obtained pursuant to this agreement to the Department of the Interior for security review, prior to submission for publication, to ensure that no sensitive but unclassified information is disclosed.
10. I hereby assign to the United States Government all royalties and remuneration that have resulted or will result from any use, release or disclosure that is inconsistent with this agreement.
11. I understand that any unauthorized use, release or disclosure of non-public information in violation of this agreement may subject me and/or my employer to administrative, civil, or criminal remedies as may be authorized by law.

Signed By: _____ Date _____
(Contractor Employee)

Approved By (PRINT NAME) : _____
(Authorized Government Official)

Approved by
Government Official
Signature: _____ Date _____
(Authorized Government Official)

[ATTACHMENT 6](#)

CERTIFICATE FOR CONFLICT OF INTEREST

PWS Title: [Information Technology Transformation Plan Follow-On for Office of the Chief Information Officer, Department of the Interior](#)

TO: _____
Print Name / Contracting Officer

THROUGH: _____
Print Name / Company Project Manager

FROM: _____
Print Name / Contractor Employee

I certify that I am not aware of any matter that might limit my ability to work on contracts and related actions in an objective and unbiased manner or which might place me in a position of a conflict, actual, potential, or apparent, between my responsibilities as a support contractor.

In making this certification, I have considered all my stocks, bonds, and other financial interests, and employment arrangements (past, present, or under consideration) and , to the extent known by me, all the financial interests and employment arrangements of my spouse, my minor children, and other members of my immediate household.

If, after the date of this certification, any person, firm, or other organization with which, to my knowledge, I (including my spouse, minor children, and other members of my immediate household) have a financial interest, or with which I have (or had) an employment arrangement, becomes involved in the acquisition I am responsible for, I will notify the Contracting Officer of this apparent conflict of interest. In such case, until advised to the contrary, I will not participate further in any way (by rendering advice and making recommendations on the applicable contract and/or related action.

(Contractor Employee Signature)

Date

ATTACHMENT 7

Department of Interior ONLY

IT Security Requirements Checklist for All IT-Related Contracts

(Based on the OCIO Directive, "Information Technology Security Requirements for Acquisition", dated August 18, 2004)

Instructions:

In accordance with the referenced Office of the Chief Information Officer OCIO Directive, all Statements of Work, and Performance Work Statement, relating to the acquisition of IT-related services, contract employees, or to the acquisition of computer systems hardware or software, must be accompanied by a completed IT security Requirements Checklist when submitted to Acquisition for processing.

Failure to include a properly signed and approved checklist with all IT-related acquisitions document will result in the return of the document to the preparer. Without exception, no action will be taken on any IT-related acquisition until a properly signed and approved checklist is attached to the acquisition package.

A "properly completed checklist" will consist of a checklist that has

- A "Yes" or an "N/A" entered into every box that is not already pre-filled with "N/A". Entering "Yes" in a box implies that the document preparer (or other appropriate responsible individual) has included all required verbiage in the acquisition documentation for the specific item. Entering "N/A" in a box implies that the acquisition action does not involve the type of acquisition referenced for the heading for that column.
- Copies of additional reference documents attached (where such documents are required by the checklist), to be provided to the acquisition source, OR instructions for accessing the document from a public source such as a website or office.
- Signature and date of the individual completing the checklist (should be the same person as the individual who is submitting the contract request).

Completed IT-Security Requirements Checklists will become part of the contract file for the acquisition, and will remain on file, for the life of the contract.

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
1.	NA	NA	Y	Background Investigation. Contractor employees who will have access to Department of Interior information or will develop custom applications are subject to background investigations. The level/ complexity of background investigations must be the same as for a Federal employee holding a similar position; DM441, Chapter 3, provides guidance for the appropriate

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
				<p>background investigation based on types of access. The solicitation and contract should state the levels required for applicable labor categories or positions. See “Model Statement of Work/Performance Work Statement Language” for Contractor Personnel Security and Suitability Requirements at the end of this Attachment 2.</p> <p>There is not cost to the Contractor for background investigations. Background investigations will be performed by the Office of Personnel Management (OPM) (See Section N of DIAPR 2006-3 for HSPD-12 Implementation for IT Technology Service Contracts, for reference to OPM background investigations requirements).</p>
2.	NA	NA	Y	<p>Non-Disclosure Agreement. Contractor employees who will have access to DOI information or will develop custom applications must sign a non-disclosure agreement prior to gaining access. Each agreement must be tailored to the contract. A draft or sample agreement may be included in solicitations. After award, the COR will develop the final agreements. Copies will be maintained in the contract file.</p>
3.	NA	NA	Y	<p>Training. Contractor employees must take DOI’s end-user computer security awareness training prior to being granted access to DOI data or being issued a user account. Training must be renewed annually.</p>
4.	NA	NA	Y	<p>Personnel Changes. The contractor must notify the COR immediately when an employee working on a DOI system is</p>

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
				reassigned or leaves the contractor's employ, and prior to an unfriendly termination.
5.	NA	NA	NA	Contractor Location. Custom software development and outsource operations must be located in the United States to the maximum extent practical. If such services are proposed to be performed abroad, the contractor must provide an acceptable security plan specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the US may be an evaluation factor.
6.	NA	NA	NA	Applicable Standards. Contractors must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64, and the DOI SDLC Security Integration Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed.
7.	NA	NA	NA	Asset Valuation. The Contractor must use the DOI Asset Valuation Guide for all systems to determine mission impact, data sensitivity, risk level, bureau/departmental/national criticality, and whether the system is a Major Application, Minor Application, or General Support System. Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed.
8.	NA	NA	NA	Property Rights. DOI will own the intellectual property rights to any software developed on its behalf to the maximum

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
				extend practical. Generally, FAR 52.227-14, Rights in Data-General, and its alternates will be used in the contract. However, deviation from this policy may be necessary as circumstances warrant.
9.	NA	NA	NA	IV & V. Software updates must be independently verified and validated prior to being moved into production. The solicitation and contract should be clear as to which party performs this function and is responsible for associated costs.
10.	NA	NA	NA	<p>Certification and Accreditation. Major Applications and General Support Systems must be certified and accredited (C & A) prior to going into production and re-accredited every three years or whenever there is a major change that affects security. C & A documents will be provided to the COR in both hard copy and electronic (specify) forms. The contractor must follow NIST SP 800-37, 800-18, 800-30, 800-60, 800-53, 800-53A, Federal Information Processing Standard (FIPS) 199 and 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST & E) Guide, and the DOI Privacy Impact Assessment. Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed.</p> <p>The government will reserve the right to conduct the ST & E, using either Government personnel or an independent contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any</p>

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
				<p>weaknesses discovered during such testing, generally at no additional cost.</p> <p>The Designated Approving Authority for the system will be the official identified in DOI Secretarial Order No. 3255.</p>
11.	NA	NA	NA	<p>Internet Logon Banner. A Government-approved logon banner must be displayed on the first page of any public access web page.</p>
12.	NA	NA	Y	<p>Incident Reporting. The contractor must report computer security incidents affecting DOI data or systems in accordance with the Department of Interior Computer Incident Response Guide.</p> <p>Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed.</p>
13.	NA	NA	NA	<p>Quality Control. All software products purchased from or developed for the NBC by a vendor or contractor must be certified by the provider to be free of malicious code. The purchase/work order for such software must contain verbiage to the effect that the provider will be held liable for any damage or loss of business as a direct result of malware or malicious code embedded within software licensed to or developed for the NBC under the authority of the purchase/work order.</p>
14.	NA	NA	NA	<p>Self Assessment. The contractor must conduct an annual self assessment in accordance with NIST SP 800-26 on all MAs, GSSs, and outsources applications in production. Solicitations must include either the complete publications or a reference to</p>

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:				Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support		
				<p>public facilities, such as a website of office, where they may be accessed. Both hard copy and electronic copies of the assessment will be provided to the COR.</p> <p>The government will reserve the right to conduct such an assessment using Government personnel or another contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contact) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.</p>
15.	NA	NA	Y	<p>Vulnerability Analysis. All system must be scanned monthly with a vulnerability analysis tool that is compatible with the software in use by the OCIO at the time (specify this in the solicitation). All "safe" or "non-destructive" check must be turned on. An electronic copy of each report and session data will be provide to the COR.</p> <p>At least annually, all high risk systems and systems accessible from the Internet must be independently penetration tested. Electronic and hard copy reports of penetration test results will be provided to the COR.</p> <p>The government will reserve the right to conduct unannounced and prearranged independent vulnerability scans using Government personnel or another contractor.</p> <p>The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.</p>

IT Security Requirements Checklist for All IT-Related Contracts

	If you are ordering:			Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
	COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support	
16.	NA	NA	NA	Logon Banner. Contractor employees who will access Department of Interior data must acknowledge a Government-approved logon warning prior to each logon to the system.
17.	NA	NA	NA	Security Controls. Contractors will be required to ensure compliance with the security control requirements of the current version of NIST SP 800-53 (even if it is in draft) or Federal Information Processing Standard (FIPS) 200 that are appropriate to the sensitivity and criticality of the data or system. FIPS 199 and the DOI Asset Valuation Guide will be used to determine sensitivity and criticality. Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed.
18.	NA	NA	NA	Contingency Plan. The contractor will submit a contingency plan in accordance with NIST SP 800-34 and DOI Contingency Plan Guide. Solicitations must include either the complete publications or a reference to public facilities, such as a website of office, where they may be accessed. The plan must be approved by the COR. A copy of the annual test results will be provided to the COR.
19.	NA	NA	NA	Security Configuration. Has the system(s) being procured been evaluated in accordance with appropriate IT security policies and requirements, including use of common security configurations available from the NIST's website at http://checklists.nist.gov ."

IT Security Requirements Checklist for All IT-Related Contracts

If you are ordering:			Put this requirement in the Statement of Work or Constraint in the Performance Work Statement
COTS Hardware/ Software	Development/ Maintenance of Custom Applications	Outsourced IT Services or On-site Support	

The following shall not be completed and signed by the same individual.

Checklist Completed By:

Printed Name: MARIA E. CLARK

Title: DIRECTOR, IT TRANSFORMATION

Signature: *Maria E Clark* Date: 1/20/12

Checklist Approved By (shall not be the same as the person completing the checklist):

Printed Name: _____

Title: _____

Signature: _____ Date: _____

IT Security Requirements Checklist for All IT-Related Contracts

Model Statement of Work/Performance Work Statement Language

For

Contractor Personnel Security and Suitability Requirements

Performance of this contract requires contractor personnel to have Federal government-issued personal identification card before being allowed unsupervised access to a DOI (facility and/or information system). The Contracting Officer's Representative (COR) will be the sponsoring official, and will make the arrangements for personal identify verification and card issuance.

At least two weeks before start of contract performance, the Contractor will identify all contractor and subcontractor personnel who will require (physical and/or logical) access for performance of work under this contract. The Contractor must make their personnel available at the place and time specified by the COR in order to initiate screening and background investigations. The following forms, or their equivalent, will be used to initiate the credentialing process:

- OPM Standard Form 85 or 85P
- OF 306
- Fingerprint card (local procedures may require the fingerprinting to done at a police station; in this case, any charges are to be borne by the contractor)
- Release to Obtain Credit Information
- PIV card application (web-based)

Contractor employees are required to give, and to authorize others to give, full, frank, and truthful answers to relevant and material questions needed to reach a suitability determination. Refusal or failure to furnish or authorize provision of information may constitute grounds for denial or revocation of credentials. Government personnel may contact the contractor personnel being screened or investigated in person, by telephone or in writing, and the Contractor agrees to make available for such contact.

Alternatively, if an individual has already been credentialed by another agency through OPM, and that credential has not yet expired, further investigation may not be necessary. Provide the COR with documentation that support the individual's status

During performance of the contract, the Contractor will keep the COR apprised of changes in personnel to ensure that performance is not delayed by compliance with credentialing processes. Cards that have been lost, damaged, or stolen must be reported to the COR and Issuing Office within 24 hours. Replacement will be at the contractor's expense. If reissuance of expired credentials is needed, it will be coordinated through the COR.

At the end of contract performance, or when a contractor employee is no longer working under this contract, the Contractor will ensure that all identification cards are returned to the COR.

IT Security Requirements Checklist for All IT-Related Contracts

Before starting work under this contract, a National Agency Check (NAC) will be conducted to verify the identity of the individual applying for clearance. Upon successful completion of the NAC process, an identification card will be issued and access granted

Simultaneously, a NAC with Inquiries (NACI) will be initiated to determine the individual's suitability for the position. If the NACI adjudication is favorable, nothing more needs to be done. If the adjudication is unfavorable, the credentials will be revoked. In the event of a disagreement between the Contractor and the Government concerning the suitability of an individual to perform work under this contract, DOI shall have the right of final determination.

This requirement must be incorporated into any subcontracts that require subcontractor personnel to have regular and routine unsupervised access to a federally controlled facility for more than 180 calendar days or any unsupervised access to a federally controlled Level 3 or 4 information system.
