ACITS3 TASK ORDER FORM

PART 1 - TASK ORDER INFORMATION

DATE	TASK TITLE
11/01/2013	NASA Cloud Assessment and Authorization (NCAA) (11/1/13 to 9/30/14).

TASK ORDER NO.	TASK MOD NO.	SERVICE REQUEST NO.	CUSTOMER CODE	SOW REFERENCE
IO2	original		ID	C.3.1.1.7 and C.3.1.6.3

	NAME	PHONE
TASK REQUESTER EMAIL (b) (6)	Susan Jacqulyn Levine	(b) (6)
FINANCIAL MANAGER (b) (6)	Rosatina K Chan	(b) (6)
COMPUTER SECURITY OFFICER (b) (6)	Ernest M Lopez	(b) (6)

TASK PREVIOUSLY COVERED BY ANOTHER CONTRACT OTHER THAN PREDECESSOR TO INCUMBENT? (If YES, provide in SOW) No

DOES THE TASK REQUIRE ACCESS TO GOVERNMENT DATABASES? *(If YES, indicate in SOW)* No

SECTION 508, ELECTRONIC AND INFORMATION TECHNOLOGY ACCESSIBILITY COMPLIANCE (EITAC)

DOES THE TASK INCLUDE EIT ITEMS (Please review the EITAC documentation) No, the task does not include EITAC items.

Upon receipt of this task order request, the contractor shall review the task requirement(s) and inform the Government, as part of its task order/modification response, any discrepancies between standards initially cited and those the contractor proposes to deliver to the Government. Examples of discrepancies include ODCs for which some other standard might be or become applicable and, as a result, require citation in the task order, as well as any cited standards that the contractor believes is not applicable (provide rationale). Note: If, by mistake, the task, including and ODC of the task, should not meet an applicable standard not cited by the requester, it is the requester, not the contractor who is a fault; and the requester must find a way (e.g., by modifying the task request) to bring the task into compliance. In such cases, the requester shall complete a revised ARC form 789 (or equivalent) before the task order/modification is approved

GOVERNMENT FURNISHED EQUIPMENT (GFE)

Government will provide all appropriate equipment and software necessary for the performance of this task unless otherwise noted in this task order. The contractor in accordance with the contract can acquire equipment not presently available as GFE. Equipment identified as task unique will be expensed to the task in accordance with ACITS3 accounting policy, and will be defined as GFE in the Government inventory. All other equipment purchases will be depreciated and be contractor property. The contractor shall follow NASA Ames rules regarding movement and assignment of government owned equipment and ODIN supplied equipment and provide information upon request for the following: Property Assignments, Property Location, and Unused Equipment.

AFFIRMATIVE PROCUREMENT (See http://www.epa.gov/cpg/products.htm)

The item(s) being purchase are NOT on any of the EPA's Comprehensive Procurement Guideline lists. - AND -

They meet the miniumum recycled/recovered content.

TASK DESCRIPTION - STATEMENT OF WORK - REQUIREMENTS
Enter this information on pages 2, 3 and 4.

COTR SIGNATURE: (b) (6) 9/26/13 CO SIGNATURE: (b) (6) 9/26/13

PART 2 - TASK ORDER PLAN PROPOSAL AND APPROVAL SUMMARY

CATEGORIES	CURRENT REQUEST	PRIOR CUMULATIVE ESTIMATE WITHOUT CURRENT REQUEST	TOTAL CUMULATIVE TASK ESTIMATE
Labor Hours:	(b) (4)		
Labor:			
ODC Labor:			
ODC Material:			
ODC Travel:			
ODC Training			
Program Mgt Cost:			
Fee:			
TOTALS:			

PART 3 - APPROVAL SUMMARY - BOTH

APPROVED BY	Signature and Date	EMail Address	Phone
1. TASK REQUESTER:	(b) (6), (b) (4)		
2. DIVISION LEVEL:			
3. TECH AREA MGR.:			
4. BUSINESS MGR.:	(b) (6)		
5. PROGRAM MGR.:			
6. COTR:			
7. CONT. OFFICER:			

ACITS3 TASK ORDER FORM (Continued)				
DATE 11/01/2013	TASK TITLE NASA Cloud Assessment and Authorization (NCAA) (11/1/13 to 9/30/14).			
TASK ORDER NO. IO2	TASK MOD NO. original	SERVICE REQUEST NO.	CUSTOMER CODE ID	SOW REFERENCE C.3.1.1.7 and C.3.1.6.3
PRICING Cost Plus Fixed Price			FUNDING LEVEL: Fund At Task Level	

TASK DESCRIPTION - STATEMENT OF WORK REQUIREMENTS

Work Areas for NASA Cloud Assessment & Authorization Effort

This effort will develop an agency-wide methodology to address the Assessment and Authorization (A&A) and IT Governance of NASA users of cloud computing for the NASA OCIO Computing Services Service Office (CSSO). With OMB mandates like "cloud-first" and the Federal Risk and Authorization Management Program (FedRAMP), NASA data will increasingly move into cloud computing services. Without policies, mechanisms, and procedures to guide NASA users' provisioning and use of cloud computing, NASA faces non-compliance with Federal Information Security Management Act (FISMA), potential loss of control over agency data, and an inability to effectively respond to security incidents involving clouds. The NASA Cloud Assessment and Authorization (NCAA) effort is to understand these emerging requirements, assist in developing policies and processes to address them, and develop a methodology to address FISMA compliance and IT Governance for CSSO users of cloud computing. Specific work areas include:

NASA Cloud Assessment & Authorization

" Refinement of A&A methodology and updating of NCAA processes for CSSO as CSSO progresses towards an operational state.
" Assist standing up CSSO elements and mechanisms for operational readiness with regard to A&A.
" Design and develop A&A package templates for use by CSSO to enable leveraging of NASA-approved Cloud Service Providers (CSPs) by NASA Managed Cloud Environments (MCEs) and for use by MCEs when leveraging NASA-approved CSPs.
" Provide MCE guidance documentation & consultation relevant to A&A.
" Provide subject matter expertise with regards to cloud security and A&A.

CSSO Governance

" Define, develop, and document baseline CSSO Governance constructs & mechanisms.
" Validate and implement CSSO Governance constructs & mechanisms.
" Identify and review NASA and government policies relevant to cloud, providing recommendations for cloud related modifications.
" Provide subject matter expertise with regards to IT Governance.

Cloud Security Assessment Review and other Support

" Assist with security posture reviews of prospective Cloud Service Providers and related activities
" Identify and propose candidate CSSO common controls. Assist with documentation and implementation of selected controls.
" Support CSSO activities & collaborations with NASA OCIO IT Security Division and other IT Governance, A&A, continuous monitoring, and cloud stakeholders.

ACITS3 TASK ORDER FORM (Continued)

DATE	TASK TITLE
11/01/2013	NASA Cloud Assessment and Authorization (NCAA) (11/1/13 to 9/30/14).

TASK ORDER NO.	TASK MOD NO.	SERVICE REQUEST NO.	CUSTOMER CODE	SOW REFERENCE
IO2	original		ID	C.3.1.1.7 and C.3.1.6.3

SPECIFIC DELIVERABLES AND DELIVERABLE DATES

No.	Type of Deliverable	Description of Deliverable	Date Required
1	schedule	Amazon Security Review	1/31/2014
2	schedule	CSP FedRAMP preparation for operational readiness	3/30/2014
3	schedule	Umbrella Package Template	9/30/2014
4	schedule	MCE A&A Package Template	9/30/2014
5	schedule	Cloud/AWS Control Parsing	9/30/2014
6	schedule	MCE Guidance	9/30/2014
7	schedule	Risk Tool Assessment	9/30/2014
8	schedule	Repositories	9/30/2014
9	schedule	CSSO Governance	9/30/2014
10	schedule	CSSO A&A Process Refinement	9/30/2014
11	schedule	Miscellaneous	9/30/2014

TRAVEL, TRAINING AND MATERIALS REQUIREMENTS

No.	Type of Requirement	Description	Date Required

ACITS3 TASK ORDER FORM (Continued)

DATE	TASK TITLE
11/01/2013	NASA Cloud Assessment and Authorization (NCAA) (11/1/13 to 9/30/14).

TASK ORDER NO.	TASK MOD NO.	SERVICE REQUEST NO.	CUSTOMER CODE	SOW REFERENCE
IO2	original		ID	C.3.1.1.7 and C.3.1.6.3

WORK BREAKDOWN STRUCTURE (WBS) CHARGE POINTS

Charge Point	Title
1	NASA Cloud Assessment & Authorization
2	CSSO Governance
3	Cloud Security Assessment Review and other Support

ACITS3 TASK ORDER FORM (Continued)

DATE	TASK TITLE
11/01/2013	NASA Cloud Assessment and Authorization (NCAA) (11/1/13 to 9/30/14).

TASK ORDER NO.	TASK MOD NO.	SERVICE REQUEST NO.	CUSTOMER CODE	SOW REFERENCE
IO2	original		ID	C.3.1.1.7 and C.3.1.6.3

IT SECURITY REQUIREMENTS

Consistent with NPG 2810.1, the specific IT Security requirements to be delegated to the contractor, under this ACITS3 task are as follows:

(Please address the following topics/questions, if applicable, concerning the intended task).

a. This Task's activities HAVE been identified as being covered under an organizational IT Security Plan. This Task DOES NOT support applications that have been designated as a "Special Management Attention" applications.

If "Special Management Attention" applications do exist please describe:

b. Periodic reviews of IT Security measures are necessary. What is the role of the ACITS3 contractor under this ACITS3 Task in areas such as review of user accounts, account management, data backup and restoration, use of warning banner, use of encryption, vulnerability scanning, and security tools? Please describe as appropriate:

user accounts, account management

c. Typically, the Task will not be involved with activities that require compliance with NASA's NPG 2810.1 and Ames' APG 2410.1 that define the requirements for reuse, reassignment or accessing of IT assets and/or their release for repair; if such an activity does occur, the Task Requester will be contacted to identify the civil servant who will have oversight and approval for reuse, reassignment or accessing of IT assets and/or their release for repair associated with this task

d. The Task personnel are trained in NASA's and Ames' policies and procedures relating to IT Security and will participate in the required annually IT security training to maintain proficiency. ThereARE NOT specialized security training requirements associated with this task.

If appropriate, specialized training requirements are described as follows:

e. Is a security clearance needed for any personnel on this task? If so, what level of clearance is required?

NO

f. There ARE NOT other IT Security requirements associated with this ACITS3 Task.

If appropriate they are described as follows:

g. There ARE NOT specific IT Deliverables associated with this ACITS3 Task.

If appropriate, they are as follows:

- ☐ IT Risk Assessment
- ☐ IT Security Plan
- ☐ IT Contingency Plan
- ☐ IT Security Vulnerability Results
- ☐ Results of periodic IT Security Reviews
- ☐ Other documentation as follows: Report of status of IT Security Plan, Contingency Plan, and Risk Assessment of critical services provided by Code I

h. In the event of an IT Security Incident associated with systems and data under this Task, the Ames Chief Information Security Official, the Security Operations Center (SOC), and the Task Requester will be notified immediately by the contractor. In order to ensure full coordination, the following individuals will also be notified in the event of an IT Security Incident:

System Owner (Responsible for the applicable IT Security Plan)	Name:	William Notley	Phone:	
Organizations Computer Security Official	Name:	Ernest Lopez	Phone:	
Alternate System Owner	Name:	Mathew Linton	Phone:	